Міністерство освіти і науки України
Одеська національна академія зв'язку ім. О.С. Попова

Даник Ю.Г., Воробієнко П.П., Чернега В.М.

ОСНОВИ КІБЕРБЕЗПЕКИ ТА КІБЕРОБОРОНИ

Підручник

Видання друге

Одеса
ОНАЗ ім. О.С. Попова
2019

УДК 007.51
Д85
ББК 32.81

Рекомендовано до друку вченою радою
ОНАЗ ім. О.С. Попова
(Протокол № 12 від 27 червня 2019 р.)

Рецензенти:

Шинкарук Олег Миколайович, проф., д.т.н., ректор Національної академії державної прикордонної служби ім. Б. Хмельницького (м. Хмельницький);
Кобозєва Алла Анатоліївна, проф., д.т.н., завідувач кафедри Одеського національного політехнічного університету (м. Одеса), заступник голови підкомісії 125 Кібербезпека НМК 7 сектору вищої оствіти НМР МОН України.

Даник Ю.Г.
Д85 Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.
ISBN 978-617-582-069-8

В підручнику викладено сутність і зміст кібербезпеки. Розглянуто роль і місце кібербезпеки у системі національної безпеки держави. Надано аналіз побудови системи кібербезпеки. Розглянуто широке коло питань зі складових кібербезпеки, їх аналізу і дій для її всебічного забезпечення. Значної уваги приділено технологіям дій у кіберпросторі та питанням організаційних і управлінських заходів забезпечення кібербезпеки.

Підручник підготовлений за матеріалами наукових розробок авторів, вітчизняних й іноземних видань та призначений для підготовки студентів, може бути корисний для науково-педагогічних працівників, докторантів, ад'юнктів та широкого кола військових і цивільних фахівців, що працюють у галузі кібербезпеки.

УДК 007.51
ББК 32.81

ISBN 978-617-582-069-8

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце
АСДУ – автоматизована система диспетчерського управління
АСУ – автоматизована система управління
ВТС ОВТ – високотехнологічні системи озброєння і військової техніки
ЄС – Європейський Союз
ЗМІ – засоби масової інформації
ІС – інформаційна система
ІТС – інформаційно-телекомунікаційна система
КбО – кібероперація
КЗ – кіберзагроза
КС – комп’ютерна система
ОКІ – об’єкти критичної інфраструктури
ООН – організація об’єднаних націй
ПЗП – постійно запам’ятовуючий пристрій
ТВД – театр воєнних дій
COA – course of action
EW – electronic warfare
MDMP – military desion-making process

ВСТУП

У сучасних умовах збройна боротьба ведеться із застосуванням високотехнологічного озброєння і військової техніки, високоефективних засобів розвідки, управління й ураження зі значним збільшенням розмаху і швидкоплинності операцій. Інформаційне забезпечення процесів управління та навантаження органів управління постійно зростають. Забезпечення ефективності управління своїми силами і засобами та порушення його у противника надає вагомі переваги над ним в умовах сучасного протиборства.

Кібервпливи все частіше стають ефективним інструментом для досягнення мети щодо несилового контролю та управління, як об'єктами з критичною інформаційною інфраструктурою держави, що може піддатися такому впливу, так і окремо взятими громадянами, їх об'єднаннями. Вони відкривають можливості досягнення політичних цілей, змін легітимних урядів, а також здійснення деструктивних змін в усіх сферах життєдіяльності суспільства і держави (економічній, енергетичній, духовній тощо), взяття під контроль і навіть поневолення цілих народів і країн практично без застосування військової сили в класичному її розумінні.

Взагалі, на сьогодні, практично всі більш-менш розвинені держави вже зіткнулися з кіберзагрозами та необхідністю формувати системи кібербезпеки та кібероборони. Тенденція перенесення дій у воєнних конфліктах до нового бойового середовища – кіберпростору ще більше загострило ці проблеми. Це спонукало провідні країни світу до запровадження першочергових заходів зі створення спеціальних структур і підрозділів для дій у кіберпросторі.

Спираючись на світовий досвід можна стверджувати, що процес забезпечення кібербезпеки, перш за все, передбачає протидію деструктивним впливам у цій сфері. Для цього потребує створення й організації потужна підсистема кіберзахисту. Не менш важливими складовими системи забезпечення кібербезпеки мають виступати і підсистеми кіберрозвідки та кібервпливу.

Зміст підручника орієнтований на підготовку фахівців з питань забезпечення кібербезпеки та кібероборони держави.

Матеріал підручника поділений на три розділи. В першому розділі розглядаються основні положення забезпечення кібербезпеки на міжнародному, регіональному та національному рівнях. Проблемні питання забезпечення кібербезпеки на кожному з рівнів та шляхи їх вирішення. Особлива увага приділяється загрозам у сфері кібербезпеки та системі кібердій. Розкриваються питання щодо завдань кібероборони держави та шляхів її забезпечення.

Другий та третій розділи присвячені технологічним та практичним аспектам забезпечення кібербезпеки та кібероборони. Викладені технологічні рішення щодо питань захисту інформації в інформаційно-телекомунікаційних системах та управління кібербезпекою. Розглянуто особливості організації, підготовки та проведення навчань з кібербезпеки за досвідом провідних країн

світу. Важливе місце відведено розкриттю питань організації наукових досліджень та підготовки фахівців з кібербезпеки та кібероборони. Запропоновано загальні характеристики планування та проведення кібероперацій за стандартами країн-членів НАТО. Проведено глибокий аналіз щодо сутності, призначення, класифікації та базових принципів побудови кіберзброї.

Розділ 1 ОСНОВНІ ПОЛОЖЕННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

1.1. Особливості трансформації і розвитку воєнного мистецтва та вирішення проблем національної безпеки і оборони в інформаційному та високотехнологічному суспільстві

1.1.1. Особливості війн та збройних конфліктів XXI століття

Аналіз змін геополітичної і геостратегічної обстановки демонструє наявність проявів принципово нових тенденцій у формуванні майбутньої картини світу. На її стан і розвиток істотно впливають нові явища у філософії війни, теорії воєнного мистецтва і практики війн (воєнних конфліктів), в основі яких лежать інноваційні досягнення інформаційних та інших високих технологій, а також модифіковані та трансформовані у зв'язку із вищезазначеним традиційні та кардинально нові методи, форми і способи досягнення цілей конфліктів різної інтенсивності (включно збройні). Збройна боротьба розглядається вже не як зіткнення бойових одиниць, що вражають один одного в ході вогневого протиборства та захоплення території супротивника, а як зіткнення багатофункціональних бойових систем, основною метою якого є позбавлення конфронтуючої системи здатності до дії [1].

Стратегічні аспекти ведення війн були викладені ще 460 р. до н.е. у трактаті Сунь-Цзи "Мистецтво війни" [2], однак реалізація того що він написав проходила поетапно. В епохах розвитку технологій, озброєння та воєнної техніки змінювались форми та способи ведення війни.

На сьогодні "обличчя війни" змінилося повністю, про це сказали ще у 1989 році, у своїй статті Вільям Лінд з групою кадрових офіцерів морської піхоти США [3].

Основним у війнах четвертого покоління, в які "вступило" людство, за їх поглядами є війна культур, ініціація, підтримка і піджившлювання ззовні та організація всередині держави психологічного й інформаційного тиску на її народ і керівництво, взяття їх під зовнішній контроль та управління, створення умов для виникнення та сприяння зростанню в цій країні соціально-економічного хаосу і самовиснаження військових, фінансових та інших ресурсів.

Що ж таке війна? Війна – складне суспільно-політичне явище, пов'язане з розв'язанням суперечностей між державами, народами, національними й соціальними групами з переходом до застосування засобів збройної боротьби, що відбувається у формі бойових дій між їхніми збройними силами. Це специфічна форма вияву соціальних відносин, в якій панує збройна боротьба, як продовження політики, що підпорядковує своїм цілям усі сфери суспільного життя.

Основна причина виникнення війн – зіткнення інтересів, прагнення політичних (а на цей час й інших міжнародних, регіональних, зовнішніх та внутрішніх акторів) сил використати збройну боротьбу для досягнення різних зовнішньо- та внутрішньополітичних й інших цілей.

Наприкінці XX століття вже склалася така ситуація коли можна було дати еволюцію війн, як з позиції форм, способів та мистецтва війни, так і з позиції розвитку озброєння та військової техніки. Отже, на цей час класифікація еволюції війн має два основних різних підходи. Перший підхід був запропонований у 1989 році у статті Вільяма Лінда, другий, що базується на змінах, які відбувалися в озброєнні й військовій техніці, викликаних розвитком технологій, що, у свою чергу, призводило до змін тактики, оперативного мистецтва й стратегії запропонував В. Сліпченко [4, 5] у 2002 році.

Так, *до першого покоління війн* за класифікацією, яка базується на змінах, які відбувалися в озброєнні й військовій техніці, відносять ті, що мали місце на зорі відомої історії людства, в яких застосовувалася в основному холодна та метальна зброя. Це були війни піших і кінних підрозділів, частин. І вже у той час виникло питання оснащення воїнів зброєю різних видів, як масовою (холодна зброя, луки, пращі), так і специфічною, малосерійною (балісти тощо), використання якої, незважаючи на її складність, відносно високу вартість, потребу у висококваліфікованих фахівцях для їх розробки, виробництва та застосування й досить великий час необхідний для її виготовлення, давало змогу дистанційно й дуже ефективно впливати на інфраструктуру, війська й населення сторін конфліктів. Базовим принципом досягнення мети дій в той час було пряме силове протиборство.

Поява і розповсюдження в XII–XIII століттях пороху та гладкоствольної вогнепальної зброї, ознаменувала початок *другого покоління війн*. З'явилися не тільки нові способи збройної боротьби в масштабах тактики підрозділів, частин і з'єднань, але й абсолютно нова, окопна війна, яка проіснувала майже 500 років. За цей час суттєво змінилася технологія виготовлення засобів збройної боротьби, відбувся перехід від одиничних їх зразків до масового виготовлення (формування технології виробництва) та застосування, суттєве збільшення їх ефективності. При цьому вже проявляється стійка тенденція: засоби, які були продуктом нових технологій, з точки зору їх інноваційності, високої, на початковому етапі, вартості та ефективності застосування, протягом певного часу, до появи ефективних засобів захисту від них або протидії ним відігравали ключову роль у досягненні мети стороною, яка їх мала у наявності (за умови готовності особового складу до їх ефективного використання).

Поява в XIX столітті нарізної, багатозарядної стрілецької зброї й нарізної артилерії з набагато більшою ніж у гладкоствольної зброї дальністю, скорострільністю й точністю стрільби й ураження також сприяло переходу до нового покоління війн. З’явилася можливість під час збройного зіткнення суттєвого збільшення дистанції між супротивними сторонами й вогневого впливу на більшу глибину бойових порядків сторін. Відбулося зародження траншейних, окопних війн на суходолі, бойових дій на морях і океанах – *війн*

третього покоління, які вже проводилися в оперативно-тактичних масштабах. Починається масовий серійний випуск уніфікованих зразків озброєння та військової техніки й оснащення ними збройних сил. Змінюється базовий принцип досягнення мети дій. Основою стає економіко-силове протиборство. Тобто економіка держави повинна не тільки забезпечити підготовку до війни, але й витримати та забезпечити силове протиборство протягом певного часу. Створення й прийняття на озброєння автоматичної, ракетної й реактивної зброї, авто- і бронетехніки, авіації, бойових надводних і підводних кораблів, поява нових транспортних засобів та засобів управління й зв'язку, локаційних засобів привело до виникнення нового – *четвертого покоління війн*, які вже мали оперативно-стратегічний масштаб і характеризувалися можливістю нанесення ударів не тільки в зоні безпосереднього зіткнення сторін, але й на значну глибину їх територій за рахунок використання авіаційних і ракетних засобів. Воїн озброєний автоматичною зброєю, захищений бронею бойових машин, знаходячись на борту літального апарату, став за своїми можливостями відповідати цілим підрозділам попередньої епохи. Технології, які використовуються у військовій сфері все більш ускладнювалися, вироби озброєння та військової техніки ставали дедалі більш вартісними й одночасно ефективними. Але продукти високих на свій час технологій ще не були превалюючими порівняно із іншими засобами, які використовувалися у воєнній справі.

Із появою ракетно-ядерної зброї пов’язують виникнення *війн п'ятого покоління*. На той момент багато кому здавалося, що за рівнем технології та з точки зору її ефективності ракетно-ядерна зброя є апогеєм людських досягнень у сфері озброєння та військової техніки. Але зброя, практичне застосування якої еквівалентно завершенню історії людства не могла не спонукати до подальшого удосконалення технологій у воєнній справі та пошуку засобів не менш ефективних, але більш безпечних для існування земної цивілізації.

В період четвертого й п’ятого поколінь особливого значення починає набувати інформаційна складова. Ефективність розвідки, дезінформації, психологічних впливів тощо стають вирішальними. Виникає феномен “холодної війни”, коли перемога, яка полягає у руйнуванні та зміні політичного устрою здобувається через руйнування економіки шляхом здійснення, здебільшого, деструктивних інформаційно-психологічних та когнітивних впливів, які спрямовані на зміни світогляду та світосприйняття людей та просування хибних концепцій, стратегій розвитку, наукових поглядів, технологій тощо. Практика її ведення показала, що у результаті впливу на об’єкти соціуму, інфо- та кіберсфер протилежної сторони можуть бути “запущені” могутні матеріально-енергетичні процеси, що значною мірою забезпечують можливість досягнення кінцевої мети протиборства. Тобто, не будучи засобом фізичного знищення збройних сил, військово-економічного потенціалу протиборчої сторони, деструктивні когнітивні, інформаційно-психологічні та кібервпливи починають ставати засобом насильства, що може привести до досягнення перемоги над ворогом: руйнування економічного та

воєнно-промислового потенціалу держави, деморалізації збройних сил, населення тощо. Відбувається чергова зміна базового принципу досягнення мети дій. Він перетворюється на принцип інформаційно-економіко-силового протиборства.

Шосте покоління війн пов’язують із розробкою та масовим застосуванням високотехнологічних засобів, систем та комплексів: систем високоточної (неядерної) зброї різного базування, зброї на нових фізичних принципах, кіберзброї, сил і засобів радіоелектронної боротьби, розвідувально-ударних систем і комплексів тощо, які створюють найрозвиненіші країни, що надає їм якісної військово-технічної та стратегічної переваги під час ведення воєнних дій без необхідності застосування значних угрупувань військ (сил). Це і подальші покоління війн вже відносяться до виду високотехнологічних.

Інший підхід, запропонований Вільямом Ліндом (William S. Lind) і групою авторів [3], полягає у тому, що переходу між поколіннями воєн (Generation Warfare, GW) сприяють два ключових елементи: ідеї та технології. Відповідно до цього була запропонована така класифікація війн.

Перше покоління війн (1GW) склали “класичні” війни, які досягли своєї найвищої точки в епоху наполеонівських війн. Характеризувалися вони лінійною тактикою, застосуванням холодної, вогнепальної зброї.

До другого покоління (2GW) віднесені “війни індустріальної епохи”, до Першої світової війни включно. Тактика ґрунтувалася на застосуванні вогню і пересування, при цьому вона залишалася лінійною у своїй основі.

Третє покоління війн (3GW) – від закінчення Першої світової війни й донині. Характеризувалися вони як маневрені, “механізовані” при потужному вогневому впливі на противника. Пізніше додалася високоточна зброя, яка принципово не змінила, хоча і розширила можливості її ведення. Тактика ґрунтувалася на широких маневрах, оточеннях і прориві ліній оборони на велику глибину, з використанням великих загальновійськових з'єднань і авіації (практична реалізація поглядів генерала Дуе).

Ідея “*війн четвертого покоління*” *(4GW)* зародилася в часи “холодної війни”, коли наддержавам в ході боротьби за свою присутність у різних точках світу стало зрозуміло, що широкомасштабне застосування танків, авіації і ракет малоефективне, а роль партизанських і різних політичних, економічних, фінансових, інформаційних та психологічних підривних операцій кардинально зросла. Такий підхід не був чимось новим. Ще у V столітті до н.е. відомий китайський філософ і теоретик Сунь-Цзи у трактаті «Про військове мистецтво» писав: «Мистецтво війни полягає у тому, щоб знищити противника зсередини. Той, хто майстерно веде війну, впокорює чуже військо не б'ючись, захоплює чужі фортеці без облоги, руйнує чужі держави без тривалих кампаній. Сто разів битися та перемогти не краще з кращих. Краще з кращих це підкорити чужу армію без битви». Ці питання до речі фундаментально розглянув у книзі "Заколот - ім'я третьої всесвітньої", виданої в Буенос-Айресі в 1960 році Євген Месснер. В ній він описав, який характер придбають війни до кінця XX століття. Що в них основні зусилля будуть спрямовуватися на деструкцію

всього хорошого, що є в країні супротивника; залучення видних представників противника в злочинні підприємства; підрив репутації і престижу, виставлення в потрібний момент на ганьбу громадськості дійсно цінних, професійних і порядних осіб; використання співпраці з самими підлими і мерзенними людьми; розпалення сварок і зіткнення серед громадян країни – цілі деструктивних дій; підбурення молоді проти старих; заважання всіма засобами діяльності уряду у разі його ефективності і професійності; перешкоджання усіма способами оснащенню, забезпечення і наведення порядку в армії, особливо у сфері її підготовки, військової освіти і науки; сковування волі воїнів супротивника безглуздими і хибними ідеями; знецінення всіх традицій і богів ворогів; щедрі пропозиції та подарунки для придбання інформації і спільників тощо." Він також передбачив розгул міжнародного тероризму і неготовність державних силових структур протистояти цій новій загрозі. Вже у вступній частині від звернув увагу на те, що: "... створилася нова форма збройних конфліктів, яку назвемо мятежвійною, в якій воїнами є не тільки війська і не стільки війська, скільки народні рухи. Цей новий феномен підлягає розгляду з різних точок зору, і в першу чергу з психологічної: якщо у війнах класичного типу психологія постійних армій мала значення, то в нинішню епоху всенародних військ і народних воюючих рухів психологічні фактори стали домінуючими. Народне військо-психологічний організм, народний рух - суто психологічне явище. Війна військ і народних рухів – мятежвійна – психологічна війна". Ієрархію цілей мятежвійни Месснер вибудовує в такому порядку: "1) розвал моралі ворожого народу; 2) розгром його активної частини; 3) захоплення або знищення об'єктів психологічної цінності; 4) захоплення або знищення об'єктів матеріальної цінності; 5) ефекти зовнішнього порядку заради придбання нових союзників, потрясіння духу союзників ворога ". Війни цього покоління характеризується змішанням усіх рівнів взаємодії, на всіх рівнях – тактичному, оперативному, стратегічному; стиранням кордонів між фронтом і тилом, військовими і цивільним населенням, війною і миром. Тобто основні аспекти і положення війн (воєнних конфліктів) сучасності і майбутнього та розуміння ефективності саме таких підходів формувалися протягом всієї історії людства, але були відсутні технології – комп'ютери, високоточна зброя, цифрові інформаційно-комунікаційні та робототехнічні засоби (безпілотники тощо), високоефективні технічні засоби розвідки, лазери; інтернет, електронні ЗМІ, комплекси електронних впливів та протидії тощо, які забезпечують їх практичну реалізацію.

Отже, розглянуті існуючі підходи щодо еволюції війн, не суперечать, а доповнюють один одного. А спільним в них є те, що зараз збройне протиборство трансформується у війну "технологій" або високотехнологічні війни.

Взагалі, усі епохи становлення людської цивілізації супроводжувалися зіткненнями інтересів у різних сферах – політичній, воєнній, економічній та інших. Проте аналіз тенденцій та особливостей розвитку людства від індустріального до високотехнологічного суспільства свідчить, що сучасне

суспільство пройшовши етап коли перехід до нової формації було обумовлено розвитком інформаційних та електронних технологій, вийшло на новий, у якому цю роль відіграють високі технології в усьому своєму спектрі.

Для того щоб зрозуміти, що таке є високі технології взагалі і які особливості їх впливу на забезпечення національної безпеки та обороноздатності держави слід згадати, що таке є технологія як коренева основа високих технологій.

Із безлічі існуючих визначень (остаточно визнаного та прийнятого ще й досі не існує, а в міру розвитку науки і техніки з'являються все нові) скористаємося таким.

Технологія (від грецьк. *techne* – мистецтво, майстерність, уміння і грецьк. *logos* – вивчення) – сукупність методів й інструментів для досягнення бажаного результату; метод перетворення даного в необхідне; спосіб виробництва [6, 7].

В наукове використання термін "технологія" увів Іоганн Бекман (1739–1811). Так він назвав наукову дисципліну, що викладалася ним в університеті в Геттінгені з 1772 р. А у 1777 р. він опублікував роботу "Введення в технологію", де писав: "Огляд винаходів, їх розвитку й успіхів у мистецтвах і ремеслах може називатися історією технічних мистецтв; технологія, яка пояснює в цілому, методично і безумовно всі види праці з їх наслідками і причинами, являє собою набагато більше" [7].

Метою технології взагалі є знаходження такого розкладання на елементи процесу досягнення будь-якого результату, яке забезпечує його найбільш просте й ефективне отримання.

Термін "високі технології", який увійшов в обігу у другій половині XX століття, як і термін "технології" також ще не набув остаточного визначення. Найбільш визнаними та розповсюдженими визначеннями, такими що найбільш повно охоплюють принципово важливі сторони явища, що розглядається, є такі [8-10]:

високі технології – наукоємні, універсальні, багатофункціональні, багатоцільові технології, що мають широку сферу застосування, здатні викликати ланцюгову реакцію нововведень, що забезпечують більш оптимальне, порівнянно з попередніми технологіями, співвідношення витрат і результатів;

висока технологія – сукупність інформації, знань, досвіду, матеріальних засобів при розробці, створенні і виробництві нової продукції і процесів у будь-якій галузі економіки, що мають найкращі характеристики за критерієм "ефективність – вартість".

Взагалі під високими технологіями багато хто розуміє будь-які складні за виконанням, але при цьому, прості у використанні технології в чистому вигляді, методи і техніку виробництва виробів і послуг або втілені технології, що охоплюють машини, обладнання, споруди, виробничі та інші системи в цілому і продукцію з високими техніко-економічними параметрами, застосування яких дозволяє найефективніше добитися необхідних результатів.

Зрозуміло, що на кожному етапі розвитку людства існували свої технології, які на той час також можна було назвати високими за існуючими сьогодні поглядами. Основними відмінностями сучасних високих технологій від високих технологій попередніх періодів суспільного розвитку є суттєво і принципово вищі наукоємність, швидкість впровадження і ротації, вплив на структурні перебудови економіки та системи управління, зміна процесів організації виробництва і методів управління та низка інших.

У розвинених країнах існуючі суспільні відносини вже сьогодні багато в чому визначаються саме цією обставиною. Тобто фактично відбулося формування наступної суспільно-політичної формації – високотехнологічного суспільства.

Високотехнологічне суспільство – суспільство, в якому:

− основним предметом праці переважної більшості людей є високі технології;

− знаряддям праці є продукти високих технологій;

− засобами праці – високотехнологічна техніка;

− основою його функціонування є високоорганізоване, високотехнологічне управління;

− основним видом діяльності переважної більшості людей відповідно, також є високоорганізоване, високотехнологічне управління.

Тим самим високотехнологічне суспільство предстає як ширша соціальна категорія, що включає “інформаційне суспільство” як одну зі своїх стадій розвитку при переході від індустріального суспільства.

На цей час побудова високотехнологічного суспільства є стратегічною метою всіх провідних держав світу – США, Японії, Канади, Німеччини, Франції, Великої Британії, Туреччини, Китаю, Південної Кореї, Ізраїлю, а також переважної більшості країн-членів Європейського Союзу та НАТО [7].

Розуміючи актуальність та важливість розвитку високих та інноваційних технологій, які є запорукою конкурентоспроможності, все більше країн обирають аналогічну стратегію, зокрема й Україна [11].

Слід зазначити, що розвиток та впровадження високих технологій проявляють себе дуально. З одного боку, очевидно, що без них ефективно забезпечити необхідний рівень національної і міжнародної безпеки у сучасному світі важко, а в скрутних економічних умовах обумовлених всесвітньою економічною кризою – майже неможливо. З іншого – революційний розвиток високих технологій породжує нову систему загроз.

Відкриття, які надали можливість контролю матеріальних структур на мікро-, нано-, піко- і молекулярному рівні, досягнення у сфері генетики, біо- та квантових технологій, роботі з великими масивами даних, штучному інтелекті тощо також несуть певні, цілком реальні загрози. Відповідно до висновків експертів ці розробки, ймовірно, приведуть до значних, навіть принципових змін, практично в усіх галузях промисловості – від машинобудування до легкої промисловості. Створення новітніх матеріалів, вакцин і комп'ютерів суттєво (але не завжди безпечно для людства) трансформує весь світ.

Зазначені досягнення, як правило, знаходять своє використання, в першу чергу, у воєнній сфері. В цілому, формування високотехнологічного суспільства, масоване впровадження у воєнній сфері високотехнологічного озброєння та військової техніки ведуть до суттєвих і навіть кардинальних змін у теорії і практиці підготовки і ведення воєнних дій на суші, морі і в навколоземному просторі.

В цілому, сформувалася нова група загроз, які полягають у:

− можливості глобального контролю державних і світових інформаційних та телекомунікаційних мереж, систем управління, мереж енергопостачання, транспортування та їх руйнування;

− розповсюдженні небезпечних технологій;

− масовій безконтрольній нелегальній, а також керованій міграції;

− появі та поширенню міжнародного тероризму тощо.

Основоположними тенденціями у воєнній справі на теперішній час та на стратегічну перспективу, є такі, як:

1) глобальна інформатизація та початок роботизації військових формувань і створення високоінтегрованих систем управління, які, у свою чергу, стають об'єктами кібервпливу і вимагають розвитку форм і способів ведення кібер-протиборства;

2) зростання інтенсивності конфліктів в інформаційному та кіберпросторі за участі спеціально створених для цього спеціалізованих структур та формувань. Ведення терористичних дій через інформаційний та кібер-простори та безпосередньо в них;

3) домінування більш розвинутих країн у веденні деструктивних дій саме через інформаційний та кіберпростори, з одного боку, та з іншого – зростання уразливості держав при зростанні рівня їх високотехнологічного розвитку;

4) використання світових інформаційних мереж та електронних засобів масової інформації для маніпулювання свідомістю і досягнення когнітивних трансформацій, як окремих спільнот і населення окремих країн, так і світової громади;

5) виділення інформаційного та інформаційно-аналітичного забезпечення в самостійний вид забезпечення військ (сил) і формування відповідних структур для його здійснення;

6) постійне зростання кількості та можливостей комп’ютерних та електронних засобів, що задіяні в зберіганні, обміні й обробці інформації і під час прийняття управлінських рішень, у тому числі на всіх етапах планування операцій та у ході бойових дій. Зростання ролі імітаційного моделювання при плануванні операцій і в процесі ведення бойових дій. Подальша інтеграція засобів штучного інтелекту в системи воєнного призначення;

7) інтеграція на основі продуктів високих технологій систем розвідки, управління та ураження від підрозділу (одиниці бойової техніки) до командування всіх ланок управління. Мініатюризація комп’ютерних та електронних засобів, їх використання практично в усіх зразках озброєння та бойової техніки (від високоточної зброї до особистої зброї та спорядження).

Таким чином, стрімкий розвиток та масове впровадження досягнень електроніки і радіотехніки, криптології, обчислювальної техніки й інформатики, елементів штучного інтелекту, хмарних технологій, інтернету речей, можливостей зберігання обробки та передачі великих масивів даних та інформації (Big Data), сучасних інформаційних, кібер- та інших високих технологій призвело до формування нового спектра ризиків і загроз у сфері національної безпеки й оборони держави, які реалізуються у кіберпросторі та (або) через кіберпростір. Відбувається експоненціальне зростання інформатизації та автоматизації всіх сфер людської діяльності, кількості інформації, що зберігається, обробляється і передається, швидкості її передачі й обробки, ускладнення систем управління взаємодії між ними та зв'язків між процесами управління. Кіберзагрози охоплюють всі базові сфери суспільної діяльності (політичну, воєнну, правову, економічну, енергетичну, інфраструктурну, соціальну, духовну, технологічну тощо), деструктивно впливаючи на національну безпеку в цілому.

Це, у свою чергу, вимагає подальшого розвитку теорії воєнного мистецтва особливо в частині стратегії, забезпечення раціонального застосування воєнних знань і досвіду при підготовці і веденні операцій і бойових дій, визначення воєнної політики держави, чисельності наявних та потрібних мобілізаційних ресурсів, напрямів розвитку науки і техніки, об'ємів і рівня суспільного, перш за все, промислового виробництва, напрямів та рівня розвитку засобів збройної боротьби – озброєння та військової техніки, потреб у стратегічній сировині, а також визначення кількості й якості складу збройних сил та їх підготовки [12].

Ера класичних війн, які велися за участю багаточисельних лінійних армій, певною мірою завершилась війною в зоні Перської затоки в 1991 році. Ставши переломною і перехідною, вона знаменувала відкриття ери високотехнологічних воєнних конфліктів у нових сферах – кібер-, електронній інформаційній та високотехнологічній в цілому. Чисельність збройних формувань в таких воєнних конфліктах може бути суттєво зменшеною порівнянно з традиційними масовими арміями. Кількість компенсується якістю – високою ефективністю управління, озброєння та професійним його використанням.

Протиборство усучасних умовах переміщується у багатовимірний простір в якому головними сферами, у яких відбувається зіткнення, стають кібер-, інформаційна, психологічна та когнітивна.

Визначальний вплив технологій на воєнну справу протягом всієї історії людства є безумовним. Воєнні конфлікти (війни) за засобами збройної боротьби, які в них застосовувалися або могли бути застосованими, можуть бути поділені на наступні види:

− звичайні (або традиційні);

− війни, які ведуться із масованим застосуванням засобів масового ураження;

− високотехнологічні війни (рис. 1.1.).

Поряд із високоточними засобами вогневого ураження й іншими сучасними компонентами озброєння й військової техніки, в них особливе значення має перевага в когнітивному, інформаційному та кіберпросторах над супротивником у зборі, обробці, аналізі, визначенні замислу, формулюванні рішення й передачі інформації споживачам та здійсненні ефективного управління і впливів у реальному масштабі часу.

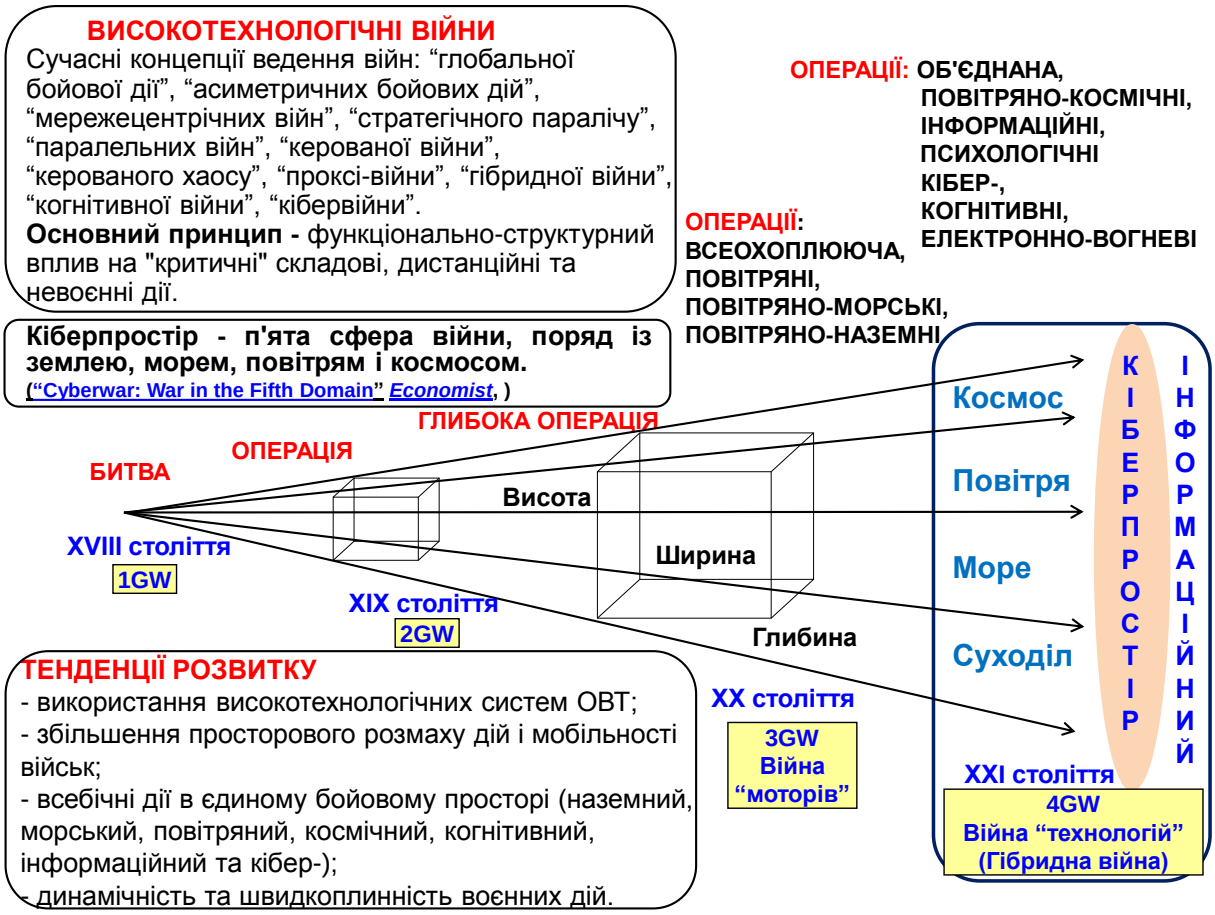

Рис. 1.1. Еволюція основних концепцій ведення війн

У воєнних конфліктах сучасності спостерігається стійка тенденція застосування їх учасниками (одним, декількома або всіма) у суттєвих обсягах або у масовому порядку високотехнологічних зразків озброєння та військової техніки (які переважають за ефективністю існуючі зразки масового виробництва) та що особливо важливо і є відрізнюваною ознакою сучасності і майбутнього – інноваційних технологій управління ними [1, 14].

При цьому, як правило, такі засоби навіть при немасовому їх використанні, забезпечують вирішальний вплив на хід і результати конфлікту. Нові можливості, які отримали засоби збройної боротьби завдячуючи інноваційним технологіям, спонукали розвиток у провідних країнах світу, впровадження та практичне використання нових стратегічних концепцій: “глобальної бойової дії”, “глобальної присутності”, “глобального охоплення”, “мережецентричних війн”, ”стратегічного паралічу”, “паралельних війн”, “керованої війни”,

“керованого хаосу”, “проксівійни”, “гібридної війни”, “когнітивної війни”, “кібервійни” тощо. Усі ці концепції передбачають бойовий вплив на ймовірних противників дистанційно перш за все в когнітивній, інформаційній, кібер-сферах з використанням всеосяжного розвідувально-інформаційного забезпечення, кібер- й високоточної ракетної та іншої зброї, робототехнічних (безпілотні літальні апарати (БпЛА), безекіпажні сухопутні й морські засоби), інноваційних електронних, спрямованої енергії та інших бойових засобів.

Прогрес у технологіях взагалі завжди був рушійним фактором розвитку воєнного мистецтва. Він привів на цей час до трансформації понять філософії війни у більш прагматичні і зрозумілі категорії, які дозволяють визначати нові тенденції еволюції такого складного явища, як збройна боротьба. Тому, провідні фахівці й дослідники, визначаючи сутність воєнних дій сучасності й майбутнього цілком справедливо ведуть мову про “високотехнологічні” війни, воєнні конфлікти й бойові дії. Це воєнні конфлікти, в яких їх учасники у масовому порядку використовують високотехнологічні зразки озброєння та військової техніки, об’єднані інноваційними технологіями управління, і саме такі засоби забезпечують вирішальний вплив на хід і результати конфлікту [15].

Слід зазначити, що з погляду на сутність парадигми високотехнологічних збройних конфліктів та з урахуванням усіх аспектів, які впливають на формування поняття високотехнологічних систем ОВТ, а саме:

− технологію виробництва та супроводження зразків ОВТ упродовж їх експлуатації;

− організацію застосування високотехнологічних зразків ОВТ;

− управління збройною боротьбою або військами (силами) в цих умовах;

− рівень ефективності застосування самих зразків ОВТ;

− можливо стверджувати, що високотехнологічними системами озброєння і військової техніки (ВТС ОВТ) є системи, створені на основі інноваційних технологій, застосування яких дає суттєве збільшення бойового потенціалу і можливість здобуття переваги над противником, а нейтралізація таких систем або ефекту від їх застосування потребує від противника значних, як наукових досягнень, так і витрат ресурсів звичайних засобів озброєння.

При цьому, високотехнологічні воєнні конфлікти – це воєнні конфлікти, в яких превалююча частина або вирішальні воєнні дії є високотехнологічними.

Високотехнологічні воєнні дії – це організоване, на основі використання інноваційних технологій управління, застосування сил і високотехнологічних систем ОВТ для досягнення політичних і військових цілей, новітня форма технологічно-економіко-силового протиборства у війні.

Мета, форми та способи ведення такого протиборства суттєво залежать від інтенсивності та ефективності інтегрального застосування високотехнологічних систем озброєння і військової техніки (для комплексної розвідки, ураження (подавлення), інформаційного забезпечення, навігації, зв’язку та передачі даних, управління тощо), рівня розвитку та впровадження інноваційних соціо-технічних технологій планування та управління збройною боротьбою.

Основними рисами високотехнологічних воєнних дій є:

− перенесення основних зусиль у повітряно-космічний, інформаційний, когнітивний та кіберпростори;

− відповідне ситуаціям (адаптивне) застосування технічних засобів розвідки, повітряно-космічних розвідувальних, інформаційно-телекомунікаційних, навігаційних та ударних систем;

− широкомасштабне застосування роботизованої техніки та бойових систем зі штучним інтелектом;

− зростання масштабів інформаційних, кібер-, психологічних і когнітивних дій та радіоелектронної боротьби в усіх сферах;

− застосування зброї на нових фізичних принципах, поява кібернетичної зброї, інформаційної та когнітивної зброї, здатної необхідним чином впливати на людину;

− набуття операціями високоманеврового характеру при широкому просторовому розмаху дій без чітко визначених їх головних та інших напрямків, з застосуванням об'єднаних оперативних угруповань та перехід до адаптивних форм воєнних дій;

− можливість ведення дій одночасно на всій території країн їх учасників із нанесенням ударів одночасно з усіх можливих напрямків.

Для високотехнологічних війн є характерним поєднання управління військами і зброєю із управлінням збройною боротьбою, сутність якого зводиться до:

− трьох головних положень - розвідати, прийняти рішення, уразити, а у подальшому до повної реалізації концепції "керованої війни";

− постійні активні дії в інформаційному, когнітивному та кібер- просторах;

− роботизації засобів збройної боротьби, виведення людини з поля бою, ведення воєнних дій дистанційно;

− формування та застосування ситуативних розвідувально-ударних комплексів і систем;

− широкомасштабного застосування "нелетальної" зброї;

− зростання кількості і впливу на хід та результати воєнних дій іррегулярних збройних формувань;

− зростання асиметричності в характері воєнних дій;

− збільшення ролі сил спеціальних операцій;

− зростання ролі інформаційного, психологічного впливу та ведення кібернетичних дій;

− перехід до адаптивних форм і способів ведення воєнних дій.

Закономірностями збройної боротьби у високотехнологічних війнах є залежність її ходу і результатів від:

− якості підготовки військових керівників;

− рівня розвитку воєнної науки та технологій і їх впровадження у системах озброєння та військової техніки;

− захищеності інформаційного, когнітивного і кіберпростору та панування у інформаційній, когнітивній і кібернетичній сферах;

− кількості та якості високотехнологічних сил і засобів, що можуть бути зосередженими та застосованими в певному місці, в одиницю часу;

− високоорганізованого управління.

У високотехнологічних війнах досить швидко і кардинально змінюється багато звичних положень не тільки стратегії, але також і оперативного мистецтва та тактики [4, 5]. Такими є тенденції та закономірності в розвитку збройної боротьби у високотехнологічному суспільстві.

При цьому, найбільш ефективне досягнення мети забезпечується впливами на управління в усіх його проявах.

Слід зазначити, що реалізація потенціалу високих технологій забезпечує стратегічну перевагу стороні, у якої рівень застосування інноваційних технологій вищий, лише протягом певного часу. У свою чергу, перевага технологій однієї зі сторін конфлікту і ступінь їх інновації визначається затратами часу і ресурсів, які необхідні протилежній стороні для досягнення подібних можливостей. Поза сумнівом, що досягнення переваги в технологіях залежить від розвитку фундаментальної та прикладної науки, рівня технологій виробництва, освіти та управління в державі.

Значний розрив у рівні технологій може призвести до ресурсного виснаження противника у разі переходу конфлікту у фазу збройного протистояння, коли для досягнення рівноваги стороні з низьким рівнем технологій доведеться компенсувати відставання за рахунок суттєвого збільшення кількості звичайних ОВТ, а також інших, в тому числі людських, ресурсів.

Особливого значення високі технології набувають у забезпеченні ефективності та успішності превентивних дій, які є сукупністю упереджувальних заходів, спрямованих на недопущення ескалації небезпек у загрози національним інтересам держави та їх реалізації у подальшому, і примушення суб’єктів загроз до відмови від своїх намірів у разі виникнення кризової ситуації будь-якої природи. У сучасних умовах превентивні дії розглядаються провідними фахівцями, які працюють у сфері оборони, як найбільш прийнятні і доцільні з точки зору забезпечення воєнної безпеки держави і національної безпеки в цілому.

Особливості превентивної оборони та превентивної кібероборони.

Можливість превентивних дій в тому числі і в кіберпросторі для забезпечення національної безпеки вже стало офіційною позицією багатьох провідних країн світу.

Роботи з обґрунтування та ведення превентивних дій в інтересах забезпечення національної безпеки та оборони проводяться в провідних країнах світу та Європейського Союзу. Так, в «Директиві з оборонної політики у сфері компетенції федерального міністра оборони» закріплено саме широке поняття оборони, яке включає і зазначені питання. В документі визначено, що сучасна оборона не може бути зведена лише до відсічі збройної агресії по периметру кордонів держави або блоку НАТО. У відповідності з директивою “оборона

включає у себе запобігання конфліктів і криз, подолання криз сумісними міжнародними зусиллями". При цьому, оборона повинна забезпечити адекватне реагування на загрози, в тому числі терористичного й асиметричного характеру. Відповідно до директиви, асиметричні загрози можуть виникнути в будь-який час, в будь-якій точці світу і можуть бути спрямовані проти кожного. Безпека Німеччини у сучасних умовах повинна забезпечуватися в будь-якій точці планети, в тому числі із застосуванням Бундесверу, й оборону неправомірно обмежувати будь-якими географічними рамками [17].

Взагалі слід зазначити, що поняття превентивних дій, превентивних ударів, превентивної оборони превентивної війни не є новими. Превентивна війна (від лат. *praevenio* – випереджую) ведеться для випередження противника у разі явної загрози нападу з його боку. На думку А. Свечина, "превентивними війнами – є війни, які розпочинає одна держава з урахуванням зростання сили сусіда, що загрожує в майбутньому війною, яку прийдеться вести в умовах гірших, чим ті, які склалися на даний момент" [18, 19].

В 1996 році Міністр оборони США Ф. Карлуччі надав нового змісту поняттю "превентивна оборона". За його поглядами в ній передбачалось використання можливостей збройних сил для вирішення задач підвищення рівня національної безпеки за рахунок їх більш широкої участі в міжнародних заходах. Зокрема, він звернув увагу на активне залучення збройних сил до заходів реалізації договорів з контролю за озброєннями, розповсюдженням ЗМУ, а також налагодження двосторонніх відношень з воєнними відомствами інших держав по всьому світу. Пізніше ці ідеї втілилися в нові задачі американських збройних сил, в яких передбачалася їх участь у формуванні сприятливих для інтересів США умов міжнародної обстановки [20].

Подальший розвиток ідей превентивної оборони найшов своє відображення в підписаному Президентом США Дж. Бушем 17 вересня 2002 року документі "Стратегія національної безпеки США", а також прийнятій 16 березня 2006 року новій редакції Стратегії національної безпеки США, яка стала логічним продовженням попереднього документу. В "Стратегії…" 2002 сформульована, а в "Стратегії…" 2006 закріплена доктрина превентивної війни. "Стратегія…" 2002 визначила ворогом США "тероризм – навмисне політично мотивоване насилля, яке спрямоване проти невинних жертв".

"Стратегія…" 2002 визначала: "Враховуючі цілі злочинних режимів і терористів Сполучені Штати більше не можуть покладатися тільки на реактивну поведінку, як це було раніше. Нездатність зупинити потенційного агресора, швидкоплинність реалізації сучасних загроз, розміри потенціальних втрат, які можуть бути нанесені арсеналом засобів, які знаходяться у розпорядженні наших противників, не дають такої можливості. Ми не можемо дозволити нашим ворогам вдарити першими".

Відповідно до "Стратегії…" 2006 керівництво США бере на себе зобов'язання знищувати терористичні організації для «захисту Сполучених Штатів Америки й американського народу їх внутрішніх і зовнішніх інтересів через виявлення і знищення загроз до того, як вони досягнуть кордонів США".

Хоча Сполучені Штати постійно намагаються заручитися підтримкою міжнародної спільноти, вони заявили, що не зупиняться перед односторонніми діями, які вживаються для реалізації їх права на самооборону шляхом здійснення превентивних заходів проти терористів з метою попередження нанесення ними шкоди народу і державі.

Концепція стримування більше не працює проти нового ворога – тероризму.

Прийоми стримування шляхом санкцій та залякування безумовно також є не чимось іншим як одним із елементів превентивної оборони. Вони повинні забезпечити досягнення зовнішньополітичних цілей шляхом залучення воєнної сили та формування у потенційного противника думки про надто небезпечні для нього наслідки або невиправдано високі втрати в результаті воєнного зіткнення.

У разі недосягнення мети зазначеним шляхом оборона полягає вже у прямому використанні воєнної сили. У такому випадку, збройні сили можуть бути застосовані для досягнення цілей національної безпеки, якщо того вимагають обставини, що склалися.

Контроль над озброєннями спрямований на своєчасне викриття і випередження намірів будь-яких країн з порушення прийнятих обмежень щодо складу та структур військових формувань, кількості озброєнь та розробки нових зразків зброї.

Найбільш повно і системно питання теорії і практики превентивної оборони знайшли своє відображення в монографії Уільяма Дж. Перри “Превентивна оборона: Нова стратегія безпеки США”. В ній превентивна оборона характеризується як політика, що не дає небезпеці перерости в загрозу: “Превентивна оборона – це оборонна стратегія Сполучених Штатів у двадцять першому столітті, яка орієнтована на небезпеки, які за недостатньої уваги до них можуть перерости в реальну загрозу виживанню США. Ці небезпеки поки не є загрозами, які потрібно стримувати або з якими потрібно боротися, поки ці загрози можуть бути відвернуті до того, як виникла необхідність в крайніх заходах. … Ця стратегія розглядає фактори, які несуть загрозу безпеці США, і можливості їх відвернення…. Такий підхід до відвернення небезпек передбачає використання для вирішення задач превентивної оборони політичних, економічних, інформаційних та військових засобів”. “Поступове зміщення акценту від цілей оборони території до захисту інтересів за межами НАТО – є стратегічним імперативом НАТО після закінчення холодної війни”.

Таким чином, проведений аналіз поглядів військових фахівців передових держав світу підтвердив актуальність превентивних дій та превентивної оборони в цілому для забезпечення національної безпеки держави, яскраво демонструє не тільки їх актуальність, але й наявність гострого протиріччя між необхідністю превентивних дій і легітимності таких дій з точки зору норм міжнародного права [21].

Так, глава VII Статуту ООН передбачає тільки дві підстави застосування сили суб’єктами міжнародного права. Одна з них – повноваження Ради Безпеки

ООН “здійснювати такі дії повітряними, морськими чи сухопутними силами, які є необхідними для підтримки або відновлення міжнародного миру і безпеки”. Друга підстава – закріплена статтею 51 Статуту ООН – право держави на “індивідуальну або колективну самооборону в разі збройного нападу на Члена ООН до тих пір, поки Рада Безпеки ООН не вжиє заходів, необхідних для підтримки міжнародного миру і безпеки”.

Розв’язанням вказаного протиріччя може стати подальший розвиток і надання нового змісту та трактування сутності поняття превентивної оборони з урахуванням тенденцій розвитку теорії і практики забезпечення національної безпеки у сучасному світі і в перспективі.

Як вже було показано, на цей час існує багато поглядів щодо сутності та принципів здійснення превентивної оборони. Але всі вони в частині застосування збройних сил зводяться до нанесення превентивних ударів по потенційних агресорах, результатом яких повинна бути їх відмова від досягнення поставленої мети або неможливість її досягнення.

Взагалі вся історія людства сповнена прикладами спроб досягти мети забезпечення безпеки шляхом нанесення випереджувальних ударів. Найбільш сучасною та досконалою формою є такий вплив на усі сфери життя країни, яка потенційно може нести загрозу, який знищує умови виникнення і можливості реалізації загроз і намірів досягти своєї мети силовим шляхом. У рамках цього нового змісту і наповнення превентивна оборона отримала в кіберсфері і стратегічних комунікаціях.

Саме це відображається у її визначеннях всіх представників сучасної теорії превентивної оборони. Але в цих поглядах та визначеннях є протиріччя між тим, що, з одного боку, найбільш ефективним методом забезпечення національної безпеки є здійснення превентивних впливів, а з іншого – існуючі міжнародні норми спрямовані саме на обмеження застосування воєнної сили в тому числі і кіберпросторі, яке само по собі може стати причиною порушення стратегічної стабільності, виникнення й ескалації конфліктів.

У той самий час, зважаючи на постійні динамічні швидкоплинні зміни міжнародної обстановки, системи глобальних проблем людства та поглядів на застосування воєнної сили і несилових впливів привело до необхідності формулювання нових поглядів і підходів до проблеми забезпечення національної безпеки. Це, у свою чергу, вимагає зміни сутності поняття превентивної оборони. Зважаючи на розглянуте, превентивна оборона повинна поєднувати усі можливі шляхи та засоби, які заздалегідь (до розвитку їх небезпечних меж) зупинять наміри суб’єкта загрози без порушення норм міжнародного права. При цьому, необхідно забезпечувати таку оперативність реагування, щоб незважаючи на те, що суб’єкт загрози розпочав діяти першим, результати активного впливу у відповіді повинні випереджувати наслідки його дій.

Розглянемо основні елементи організації та здійснення превентивних дій. Превентивні дії є функцією держави, яка комплексно здійснюється усіма суб’єктами національної безпеки й оборони. Ці дії і можна визначити як превентивну оборону.

Превентивна оборона (превентивні дії в інтересах оборони) – сукупність упереджувальних заходів та дій, спрямованих на недопущення ескалації небезпек в загрози та реалізації загроз національній безпеці держави у воєнній сфері і примушення суб'єктів загроз до відмови від реалізації своїх намірів у разі виникнення безпосередньої воєнної загрози будь-якої природи.

Аналізуючи досвід реалізації елементів превентивної оборони в провідних країнах світу та виходячи із сутності дій з її реалізації, неважко дійти висновку, що дії з її здійснення за своєю сутністю є стратегічними діями. Стратегічний характер підтверджується й органічною єдністю її основних ознак з ознаками існуючих видів стратегічних дій: стратегічного розгортання, протиповітряної оборони держави, територіальної оборони.

Всі існуючі види стратегічних дій мають спільні ознаки: масштабність; узгодженість за єдиним замислом та планом для досягнення стратегічних цілей держави; для їх забезпечення та здійснення залучається потенціал всієї держави.

В існуючому визначенні стратегічних дій збройних сил [9, 10] вони трактуються наступним чином: "Стратегічні дії збройних сил – військові дії стратегічного масштабу, що різняться за своєю метою, характером, змістом задач, які виконуються, і способам дій стратегічних угруповань збройних сил". Інше відоме визначення трактує стратегічні дії збройних сил, як сукупність операцій, бойових дій, специфічних форм збройної боротьби і заходів, що проводяться за єдиним замислом і планом збройними силами для досягнення стратегічної мети війни.

Зважаючи на це, превентивну оборону, як вид стратегічних дій, можна охарактеризувати як адаптивне до обстановки комплексне поєднання несилових та силових заходів, спрямованих на недопущення переростання небезпек в загрози та їх подальшої ескалації.

Тому превентивна оборона (в тому числі превентивна кібероборона), як вид стратегічних дій, це здійснення комплексу заходів щодо запобігання, стримування, сковування, упередження та реагування у відповідь з безумовним випередженням сторони, яка здійснює напад, в настанні для неї неприйнятних наслідків шляхом забезпечення необхідних впливів на критичні елементи політичної, воєнної, економічної та інших сфер життєдіяльності держави, яка є джерелом загроз або ворожих дій.

Вона передбачає випередження, адекватність, рішучість, узгодженість, перевагу в інформаційному, часовому і просторовому розподілі впливів (інформаційних, кібер-, когнітивних, вогневих (кінетичних), невогневих (електромагнітних і т.п.) тощо) для запобігання кризових ситуацій або розв'язання їх на власну користь.

Превентивна оборона (в тому числі превентивна кібероборона) може здійснюватися поетапно: від запобігання, стримування, упередження, сковування до силового реагування у відповідь. В залежності від протікання кризи та рівня реалізації загроз превентивна оборона може здійснюватися послідовно за етапами або переходити до будь-якого етапу, більш високого

порядку минаючи попередні. Реалізація етапів за напрямами дій також може відрізнятися (на різних напрямах можуть одночасно реалізовуватися етапи нижчого або вищого рівнів, послідовно або паралельно, та змішані форми при одночасній реалізації форм більш високого або меншого рівнів).

Основні аспекти стратегії превентивної оборони та її реалізації

Одним із найскладніших понять, що перебуває в постійній трансформації, з яким треба визначатися для практичної реалізації превентивної оборони, є стратегія. І не тільки стратегія взагалі, як основоположне, базове поняття та вища форма воєнного мистецтва, але і як визначений напрям певних дій щодо підготовки держави до оборони та збройних сил до застосування.

Важливою складовою стратегії національної безпеки України, як і будь-якої іншої держави, безперечно є національна воєнна стратегія. Зміст поняття воєнної стратегії та її принципи постійно доповнюються і розширюються. Це було відомо з давніх часів. Ще Сунь-Цзи зазначав, що принципи стратегії постійно розвиваються, і хто не знає цієї істини, той не знає про війну нічого [2, 22]. Особливо яскраво еволюція поняття воєнної стратегії простежується в його визначеннях, наданих відомими воєнними теоретиками і практиками.

В теорії воєнного мистецтва термін strategos походить від грецьких слів – stratos (військо) і ago (веду). Взагалі стратегія – найвища сфера воєнного мистецтва, яка включає теорію і практику підготовки держави до оборони, збройних сил до застосування і масштабних воєнних операцій [9, 19, 23].

Фельдмаршал Август фон Гнейзенау (1761–1831), характеризуючи воєнну стратегію, звертав увагу переважно на просторово-часові особливості ведення війни, що вже і на той час було цілком слушним з точки зору досягнення її мети, а також досить чітко вказував параметр, на який слід впливати, та обмеження, що є критичними з точки зору вирішення стратегічних задач. Так, він наголошував, що стратегія – це наука використання простору і часу. При цьому, майже завжди можна відвоювати втрачену територію, але повернути втрачений час неможливо.

Воєнні теоретики передових країн світу, у свою чергу, зазначають, що стратегія – це планування, координація і концентроване використання різноманітних засобів і ресурсів, які є в коаліції, держави, політичної групи або командувача для досягнення переваги над супротивником. Такий підхід, у свою чергу, чітко вказує на нагальну потребу в наявності теоретичних та практичних аспектів знаходження раціонального співвідношення між метою і ресурсами, які необхідні та є у наявності. Найбільш загальне визначення для будь-якої сфери діяльності трактує стратегію таким чином: стратегія – це теорія і практика, яка спрямована на досягнення головної мети (місії) певної соціальної структури шляхом досягнення часткових стратегічних завдань. Це необхідний елемент організації діяльності у будь-якій сфері.

Ряд дослідників визначають стратегію й як:

− загальний план якої-небудь діяльності, що охоплює тривалий період часу, спосіб досягнення складної мети, що є, головною для управлінця на даний

момент, надалі коректованої під умови, що змінюються;

– інтегровану модель дій, призначених для досягнення цілей суб'єкта, змістом якої служить набір правил ухвалення рішень, використовуваний для визначення основних напрямів діяльності;

– специфічний управлінський план дій, спрямованих на досягнення встановлених цілей.

У цілому, основним, що є загальним в усіх відомих дефініціях стратегії та існуючих успішних стратегіях, є поєднання мети та визначення шляху її досягнення в умовах ресурсних обмежень.

Звідси вкрай важливого значення набуває управлінська діяльність щодо практичної реалізації стратегії – стратегічний менеджмент, як процес управління організацією, що орієнтує її на досягнення (реалізації) своєї головної мети (місії) і досягнення стратегічних цілей через раціональне використання людських і матеріальних ресурсів та розвиток конкурентних стратегічних переваг [24].

Враховуючи вищевикладене, стає можливим обґрунтувати визначення стратегії превентивної оборони. Для цього застосуємо підхід формування поняття від загального до часткового, визначимо мету її здійснення, теоретичні та практичні аспекти досягнення за головними елементами:

1. Стратегія – теорія і практика дій, спрямованих на досягнення головної мети.

2. Головна мета (місія) – максимально унеможливити переростання викликів і небезпек у воєнній сфері в загрози національним інтересам держави та їх подальшої реалізації, і примушення суб'єктів загроз до відмови від своїх агресивних намірів [16].

3. Стратегічні цілі – не допустити загострення воєнно-політичної обстановки (нарощування воєнного потенціалу агресора) до граничних меж, перевищення яких зумовлює неминучість вирішення протиріч силовими методами, на основі здійснення заходів запобігання і стримування, упередження та реагування у відповідь з безумовним випередженням сторони, яка здійснює напад, в настанні для неї неприйнятних наслідків [16].

4. Сутність стратегії – це визначення пріоритетів, важливості та раціонального співвідношення між стратегічними цілями і ресурсами, необхідними для досягнення головної мети.

При цьому, одним із ключових понять, яке використовується та визначається як необхідна умова досягнення стратегічних цілей, є забезпечення стратегічної переваги над протилежною стороною. У зв'язку з цим, закономірно постає питання, по-перше, про визначення самого сенсу стратегічної переваги, а по-друге, стосовно чого визначати таку перевагу. У воєнному мистецтві поняття переваги над противником зазвичай розглядається або через кількісно-якісне співвідношення сил та засобів, або через зіставлення інтенсивності втрат протиборчих сторін протягом певного часу. Водночас, поняття переваги має також трактування за сферами, в яких відбувається зіткнення сторін (повітряній, наземній, морській, космічній, інформаційній,

кібер-, когнітивній тощо). Через те виникає необхідність розглядати забезпечення переваги в них, як у кожній окремо, так і в усіх разом.

Таким чином, стає можливим стверджувати, що стратегічна перевага – це спроможність однієї зі сторін конфлікту реалізувати такі можливості, які суттєво збільшать імовірність досягнення своєї воєнно-політичної мети, і водночас мінімізувати здійснення ефективної протидії противником у воєнному конфлікті.

Відповідно до цього, спроможність у певному місці в певний час створити необхідний потенціал, який забезпечить перевагу над потенціалом противника, зумовлює неможливість ефективної реалізації противником його власного потенціалу, створює умови, в яких потенціал противника на основі використання можливостей високотехнологічних систем ОВТ та інноваційних технологій управління стане деструктивним і перетвориться в загрозу для нього самого, визначає стратегічну перевагу під час здійснення превентивної оборони.

Наповнення загального поняття стратегічної переваги необхідним змістом стосовного умов превентивної оборони забезпечує його трансформацію у поняття "стратегія превентивної оборони" та "превентивної кібероборони". Сутність стратегії превентивної оборони полягає у визначенні стратегічних цілей і ресурсів для здійснення практичних дій з метою недопущення переростання викликів і небезпек у загрози національним інтересам держави у воєнній сфері та їх подальшої реалізації і примушенні суб'єктів загроз до відмови від своїх агресивних намірів з безумовним випередженням держави, яка є джерелом загроз або ворожих дій в настанні для неї неприйнятних наслідків на основі забезпечення необхідних впливів на критичні елементи її політичної, воєнної, економічної та інших сфер життєдіяльності.

Таким чином, стає можливим стверджувати, що **стратегія превентивної оборони** – це теорія і практика діяльності держави щодо недопущення переростання викликів і небезпек у загрози її національним інтересам у воєнній сфері та їх реалізації, примушення суб'єктів загроз до відмови від своїх намірів шляхом збалансованого, на основі високих та інноваційних технологій, застосування всього наявного воєнного потенціалу держави з мінімальним навантаженням на економіку.

Для розкриття змісту ролі і місця високих технологій в реалізації мети превентивної оборони виникає необхідність розгляду процесу її досягнення в контексті розвитку конфлікту від його зародження до переростання у збройну фазу.

Етапи реалізації дій щодо здійснення заходів превентивної оборони переходять один в інший відповідно до ймовірності переростання конфліктної ситуації у збройне протистояння (рис. 1.2).

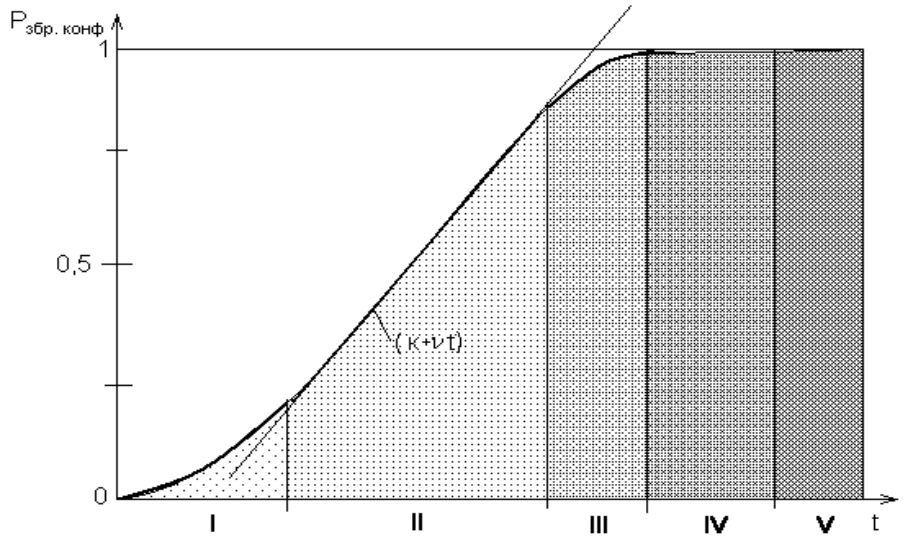

Рис. 1.2. Графік здійснення заходів превентивної оборони залежно від зростання ймовірності виникнення збройного конфлікту

I етап – запобігання виникненню конфлікту;
II етап – стримування розвитку конфлікту;
III етап – сковування конфлікту;
IV етап – упередження (випередження) противника;
V етап – реагування у відповідь.

Відповідно до рівня розвитку конфлікту роль кожної складової превентивної оборони та їх зміст розкритий в [16]. Зауважимо, що при цьому дуже важливо своєчасно здійснювати перехід від однієї фрази до наступної, якщо попередні заходи не досягли своєї мети.

Перший етап превентивної оборони – запобігання. Основна мета цього етапу полягає в недопущенні формування критичної маси протиріч, які виникають на основі конфронтації інтересів протилежних сторін, та переростанні сукупності протиріч у конфлікт за умови готовності сторони-агресора вирішити конфлікт за допомогою зброї.

Другий етап превентивної оборони – стримування. Розвиток цієї фази конфлікту розглянемо в рамках лінійної моделі. За цієї умови динаміку зростання ймовірності виникнення збройного конфлікту на цьому етапі можна описати функцією:

$$S(t) = k + vt, \tag{1.1}$$

де $S(t)$ – лінійна функція зростання ймовірності виникнення збройного конфлікту;

v – нормована швидкість змін імовірності виникнення збройного конфлікту;

t – час розвитку конфлікту;

k – початковий рівень розвитку конфліктної ситуації у разі відсутності чи низької ефективності заходів запобігання або запізнення з початком дій зі стримування розвитку конфлікту.

Основна мета цього етапу стримати (параметр – нормована швидкість розвитку конфлікту $v \to 0$) або зупинити розвиток конфлікту ($v = 0$), а в подальшому повністю його розв'язати.

Третій етап превентивної оборони – сковування. Цей етап починається, коли сформувалася загроза реального застосування зброї (ймовірність виникнення збройного конфлікту як достатньо високу відповідно до правила Парето можна визначити при $P_{\text{збр конф}} > 0{,}8$). Мета сковування полягає у формуванні обмежень стосовно масштабів застосування військової сили, видів зброї, сприяння порушенню процесів державного управління концентрації, необхідної для початку збройного конфлікту кількості матеріальних і людських ресурсів у потрібному місці та в потрібний час.

Четвертий і п'ятий етапи превентивної оборони – упередження і дії у відповідь починаються з моменту застосування зброї стороною, яка здійснює агресію. Зміст і мета цих етапів розкриті в [16], але виникає питання, яким чином реалізувати стратегію превентивної оборони та забезпечити вирішення задач випередження противника у завданні йому неприйнятних збитків та здійснити ефективні дії у відповідь.

Для цього в основу реалізації стратегії превентивної оборони доцільно покласти концепцію раціонального (оптимального) використання наявних ресурсів у процесі досягнення стратегічних цілей. З цією метою стає можливим застосувати теорію розподілу енерго-інформаційного потенціалу П у просторі і часі, яка відображає взаємозв'язок між сукупним енергетичним потенціалом сил і засобів, здатних завдати ураження противнику, та інформаційних ресурсів у системі управління реалізацією енергетичного потенціалу [25].

Потенціал визначається функціоналом:

$$\Pi = \Im(E, I), \tag{1.2}$$

де E – сукупний енергетичний потенціал сил і засобів, здатних завдати ураження противнику;

I – інформаційний ресурс у системі управління реалізацією енергетичного потенціалу.

У широкому значенні функціонал визначення енерго-інформаційного потенціалу потребує урахування додаткових параметрів: параметра часу, який характеризує процес накопичення і використання енерго-інформаційних ресурсів, визначення простору, в якому здійснюються превентивні дії, а також множину задіяних ключових об'єктів і має вигляд:

$$\Pi = \Im(E, I, V, T, M), \tag{1.3}$$

де T – параметр часу, який характеризує процес накопичення і використання потенціалу;

V – n-мірний простір превентивних дій;

M – множина ключових об'єктів.

У процесі розподілу потенціалу в часі та просторі на ключові об'єкти і зони (райони) формується потрібний рівень потенціалу, який може бути реалізований для завдання ураження противнику в даній точці простору, а мистецтво стратега буде полягати в раціональному розподілі наявного потенціалу у часі за цілями і формування такого рівня потенціалу, який забезпечить досягнення стратегічних цілей.

Взагалі створення воєнного потенціалу – це комплексне складне питання не простого сумування, а системного акумулювання певних воєнних проявів усіх основних потенціалів держави: економічного, наукового, політичного, соціального, духовного для підготовки держави до оборони. Кожна держава визначає власний підхід до його створення. При правильному здійсненні акумулювання має місце прояв синергетичного ефекту, а ступінь його прояву визначає, наскільки вірно було здійснено це акумулювання. У сучасних умовах найбільш прийнятним шляхом трансформації оборонних структур держави для забезпечення воєнного потенціалу, який дозволить адекватно реагувати на виклики і загрози, є впровадження інноваційних технологій та високотехнологічних систем озброєння і військової техніки (далі ВТС ОВТ). Провідні держави світу орієнтують свої збройні сили на підготовку до збройних конфліктів, під час яких передбачається широке використання високотехнологічного озброєння.

Практика воєнних конфліктів останніх десятиліть не без підстав свідчить, що нині у війні перемагає той, хто швидше сприймає нові технології та втілює їх у життя, бере на озброєння нові воєнні доктрини і концепції, що відповідають духу часу, і, зрештою, в кого командири не лише самі використовують нові технології та ідеї, але й добре знають, які з них і коли може використовувати противник.

Як вже зазначалося, коли одна, декілька або усі сторони конфлікту застосовують засоби збройної боротьби, які переважають за ефективністю існуючі зразки масового виробництва, збройне протиборство трансформується у протиборство технологій, а сам процес ведення війни теж підпорядкований технології її ведення. Здобуття переваги у конфлікті, при цьому, можна формалізувати аналітичним виразом, наведеним у [26] для обчислення рівноваги збройних угруповань сторін конфлікту:

$$\sum_{t=0}^{T}\sum_{i=1}^{m}(N_i^B(t)-k_i(t)N_i^A(t))^{\eta_i(t)}=0, \qquad (1.4)$$

де T – тривалість планування застосування ВТС ОВТ;

i – тип ОВТ;

N^B_i – кількість зразків озброєння i-го типу сторони B на момент часу t;

N^A_i – кількість зразків озброєння i-го типу сторони A на момент часу t;

$k_i\,(t)$ – коефіцієнт технологічної переваги зразка озброєння i-го типу сторони A над зразком озброєння i-го типу сторони B на момент часу t;

$\eta_i(t)$ – значимість i-го типу зразка озброєння в загальній системі озброєння;

m – кількість типів зразків озброєння.

Врахування умов, які забезпечують перевагу над противником за рахунок нарощування кількості ОВТ або високотехнологічності, забезпечується наданням виразу (1.4) у виді такої нерівності:

$$\sum_{t=0}^{T}\sum_{i=1}^{m}(N_i^B(t))^{\eta_i(t)} < \sum_{t=0}^{T}\sum_{j=1}^{m}(k\ (t)N_j^A(t))^{\eta_i(t)}; \qquad (1.5)$$

$$N_i^B < kN_j^A;$$

$$\frac{N_i^B}{N_j^A} < k,$$

де j – тип ОВТ.

Досягнення переваги можна пояснити прикладом на основі співвідношення потенціалів, що дозволить порівняти різнорідні засоби ОВТ у можливому їх взаємному бойовому зіткненні:

$$E_{\text{втс}} = N \cdot E_{\text{нтс}}\ , \qquad (1.6)$$

де $E_{\text{втс}}$ – потенціал високотехнологічних систем ОВТ;

$E_{\text{нтс}}$ – потенціал низькотехнологічних систем ОВТ;

N – кількість низькотехнологічних систем ОВТ, яка необхідна для досягнення рівності потенціалів.

Тому, за аналітичним виразом (1.5) коефіцієнт технологічної переваги k зразка озброєння j-го типу сторони A над зразком озброєння i-го типу сторони B на момент часу t дорівнює N.

Таким чином, коли протистояння у конфлікті переходить у площину боротьби технологій, до уваги береться технологічна перевага в різних сферах (управлінні, ОВТ тощо).

Аналіз досвіду впровадження і використання високотехнологічних систем в локальних війнах і збройних конфліктах XX та XXI століть показує стійку залежність між ефективністю досягнення мети збройної боротьби та концентрацією високотехнологічних систем і засобів у розпорядженні найвищої ланки управління (і використанням їх органами оперативного ситуативного функціонального управління при переході від превентивних до регулярних дій) для досягнення стратегічних цілей шляхом впливу на ключові (критичні) елементи держави противника та його збройних сил. Але, в умовах високої динаміки розвитку високих технологій подвійного призначення та ОВТ, між розвитком високих технологій та економічними можливостями держави щодо масового переозброєння збройних сил часто виникає протиріччя. Вихід із вказаного протиріччя – це концентрація високотехнологічних систем і засобів у підпорядкуванні структури, яка спроможна: забезпечувати високу ефективність використання наявних зразків в інтересах національної безпеки; визначати необхідну потребу у високотехнологічних системах ОВТ, виявляти

напрямки розвитку високих технологій; здійснювати необхідне доукомплектування звичайних зразків ОВТ високотехнологічними системами та їх високотехнологічну модернізацію, управляти цими процесами в умовах підготовки до високотехнологічних воєнних конфліктів та їх ведення.

Створення такої системи забезпечить максимально повну реалізацію таких переваг високотехнологічних систем і засобів, як мінімальний час готовності до застосування; завдання непоправних втрат противнику за мінімальний проміжок часу; висока маневреність зусиль для концентрації в декількох місцях одночасно; зменшення ефективності протидії з боку противника.

Зважаючи на те, що основою превентивної оборони є органічне поєднання військ (сил), оснащених високотехнологічними ОВТ, інтегрованих в єдиний інформаційний простір, та ефективних технологій управління їх застосуванням, можна методологічно визначити основні елементи реалізації стратегії превентивної оборони на основі використання високих технологій.

Так, процес застосування високотехнологічних систем і засобів можна поділити на дві фази:

1) на початковій фазі воєнного конфлікту вони застосовуються для зниження воєнного потенціалу держави противника;

2) під час організації та здійснення оборони держави високотехнологічні системи і засоби застосовуються для виконання стратегічних задач, збільшення бойового потенціалу збройних сил на напрямах зосередження основних зусиль в інтересах вирішення найбільш важливих задач.

Оцінка можливої побудови будь-якого із варіантів комплексної структури для організації застосування високотехнологічних систем ОВТ та досягнення акумулювання за єдиним задумом зусиль усіх складових розвідки (космічні системи, РЕР, БПЛА тощо); дій ССО; сил і засобів інформаційної боротьби; вогневого та невогневого ураження і подавлення (ВТЗ, РЕБ, високоточна зброя, реактивні системи залпового вогню) може бути здійснено на основі аналізу бойового потенціалу, який можна описати функціоналом:

$$\text{БП}(t) = K_{\text{у}} \sum_{i=1}^{N_{\min}} g_i \text{БП}_i(t), \qquad (1.7)$$

де $\text{БП}_i(t)$ – бойовий потенціал ВТС ОВТ;

$K_{\text{у}}$ – коефіцієнт якості управління реалізацією бойового потенціалу комплексної структури ВТС ОВТ;

i – тип окремого зразка ВТС ОВТ;

g_i – коефіцієнт ваги;

$N_{\min}$ – мінімально необхідна кількість зразків ВТС ОВТ.

Динамічне управління ресурсами у системі превентивної оборони повинно бути адаптивним до змін оперативної обстановки і створювати сприятливі умови на стратегічному рівні для ефективного проведення операцій. За таких умов стратегічна мета превентивної оборони – максимальне зниження воєнного

потенціалу противника до початку проведення операцій збройними силами. Для цього бойовий потенціал високотехнологічних систем і засобів повинен бути достатнім, щоб після його реалізації противнику були завдані такі втрати, після яких він відмовився б від подальшої агресії. Для цього необхідно виявляти критичні елементи системи воєнної організації держави противника і розподіляти ресурси таким чином, щоб досягати максимальної ефективності застосування високотехнологічних систем ОВТ.

У сучасних умовах, час реакції на загрозу повинен бути меншим за час, необхідний противнику, щоб зробити небоєздатними ключові елементи і насамперед високотехнологічну складову системи превентивної оборони. Тому тривалість початкової фази збройного конфлікту скорочується до відрізка часу (t – реалізації бойового потенціалу високотехнологічною системою або засобом), необхідного для застосування «найшвидшого» засобу завдання непоправного збитку, який робить подальші дії агресора недоцільними.

Інтенсивність реалізації бойового потенціалу, нарощування до потрібного рівня й утримування його протягом часу, необхідного для завдання непоправних втрат противнику, показано на рис. 1.3. Необхідний результат може бути досягнутий на будь-якій фазі застосування сил та засобів на етапах випередження противника та дій у відповідь. Якщо мета превентивних дій на зазначених етапах не була досягнута на попередній фазі, необхідно передбачити логічний розвиток процесу застосування сил і засобів на наступній фазі таким чином, щоб інтенсивність впливу, яка забезпечить відмову противника від своїх намірів, не зменшилася нижче рівня, на якому розвиток досягнутого успіху попередньої фази може бути втраченим. Тобто нарощування зусиль на наступній фазі повинно вийти на рівень, з якого можна ефективно продовжити у разі потреби вплив на противника без втрати досягнутих переваг. Аналітично це можна описати таким чином:

$$W(t) = \frac{d}{dt}\text{БП}(t), \tag{1.8}$$

$$\text{БП}(t) = \sum_{i=1}^{N}\text{БП}_i(t=0) + B(t), \tag{1.9}$$

$$B(t) = \int_0^{t_{\max}} (\sum_{i=1}^{N} b_i(t))dt, \tag{1.10}$$

де $W(t)$ – інтенсивність реалізації бойового потенціалу;

БП_i – бойовий потенціал зразка ОВТ;

i – тип окремого зразка ВТС ОВТ;

N – кількість зразків ВТС ОВТ;

$b_i(t)$ – функція відновлення або нарощування бойового потенціалу i-го зразка ВТС ОВТ;

B(t) – інтегрована функція відновлення або нарощування бойового потенціалу.

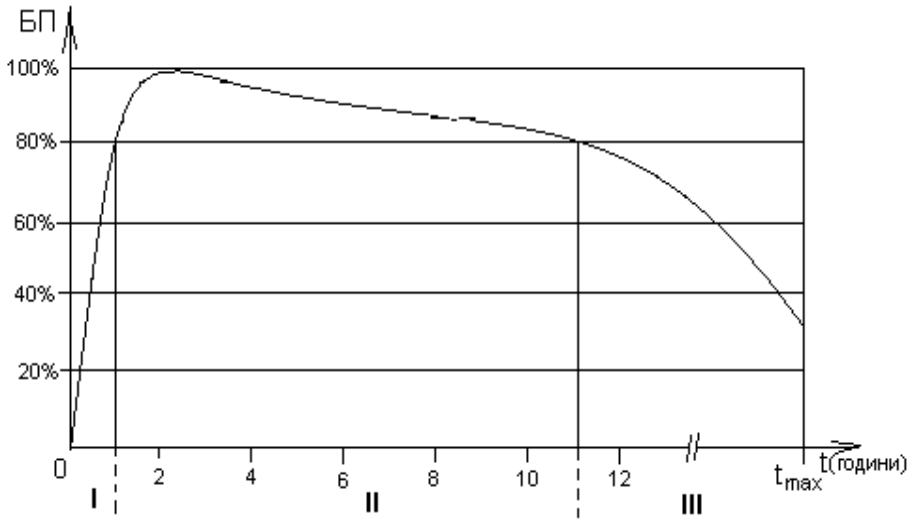

Рис. 1.3 Графік інтенсивності реалізації бойового потенціалу:

I – фаза нарощування інтенсивності реалізації бойового потенціалу до необхідного рівня;

II – фаза утримування інтенсивності реалізації бойового потенціалу протягом певного часу, необхідного для завдання непоправних збитків агресору, що примусить його відмовитися від подальших дій;

III – фаза динамічного зменшення інтенсивності реалізації бойового потенціалу пропорційно досягненню мети превентивних дій.

Усі сили та засоби, які залучені до здійснення превентивних дій, за своїми можливостями щодо оперативності застосування та потужності можуть бути віднесені до таких категорій: 1) сили та засоби негайного реагування стратегічного, оперативного та, в окремих випадках, оперативно-тактичного рівня (час реалізації бойового потенціалу упродовж хвилин); 2) сили та засоби швидкого реагування оперативного та оперативно-тактичного рівня (час реалізації бойового потенціалу упродовж годин); 3) сили та засоби оперативно-тактичного і тактичного рівня високої боєготовності здатні ефективно вплинути на хід подій та розвинути досягнутий успіх (час реалізації бойового потенціалу упродовж доби і більше). Вимоги до тривалості реалізації бойового потенціалу високотехнологічних систем і засобів залежать від задач, які необхідно вирішити в конкретній ситуації, та технологічного рівня озброєння противника і його стану.

Залежно від динаміки ескалації конфлікту високотехнологічні системи і засоби можуть переходити з категорії засобів швидкого реагування до категорії засобів негайного реагування і навпаки, зважаючи на готовність сил і засобів та системи управління противника (рис. 1.4).

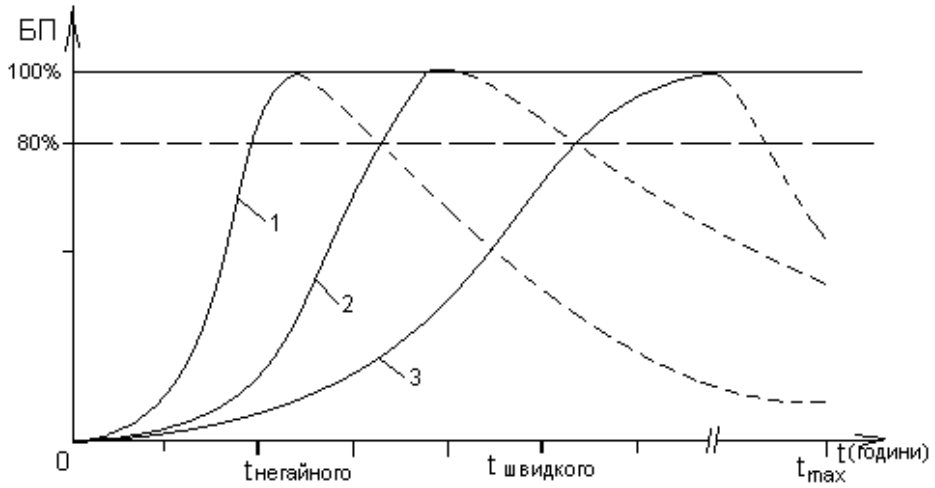

Рис. 1.4. Графіки реалізації бойових потенціалів різних засобів ВТС ОВТ:

1 – сили негайного реагування стратегічного, оперативного та оперативно-тактичного рівня;

2 – сили швидкого реагування оперативного, оперативно-тактичного та тактичного рівня за необхідністю;

3 – сили та засоби оперативно-тактичного та тактичного рівня високої боєготовності.

Слід зазначити, що процес розвитку збройних сил має циклічний характер. Спочатку їх розвиток відбувався від окремих збройних формувань до масових армій, на сучасному етапі тенденція змінилась: від масових армій до нечисленних збройних сил, побудованих за функціональними ознаками, зменшення кількості особового складу на полі бою за рахунок заміни його високотехнологічними системами і засобами та широкомасштабного застосування роботизованих систем.

На рис. 1.5 показані два підходи до забезпечення потрібного потенціалу збройних сил.

У разі розвитку високотехнологічних систем ОВТ за визначений проміжок часу (t_{opt}) та при необхідному рівні фінансування розробки озброєння час досягнення мінімально достатнього потенціалу скорочується на декілька (3-4) років, порівнянно з варіантом нарощування потенціалу збройних сил за рахунок збільшення кількості звичайних зразків ОВТ, та дозволяє отримати резерв часу на переозброєння збройних сил в цілому.

Доцільно в ході вирішення питань переходу Збройних Сил України до впровадження інноваційних технологій, як у системі військового менеджменту, так і в питаннях застосування інноваційних способів та засобів ведення збройної боротьби обрати одну із альтернативних концепцій:

1) отримання нових якостей від існуючих зразків ОВТ за рахунок використання високотехнологічних систем та інноваційних підходів щодо їх застосування та подальшого системного розвитку нових високотехнологічних систем ОВТ;

2) здійснення модернізації (переозброєння) Збройних Сил України

заміною існуючих зразків ОВТ сучасними і найбільш ефективними на даний час, пошуком можливостей постачання нових видів ОВТ, що за сучасних економічних можливостей держави стає проблематичним;

3) здійснення структурної перебудови Збройних Сил України, продовження термінів експлуатації існуючих зразків ОВТ, нарощування обсягів виробництва існуючих зразків.

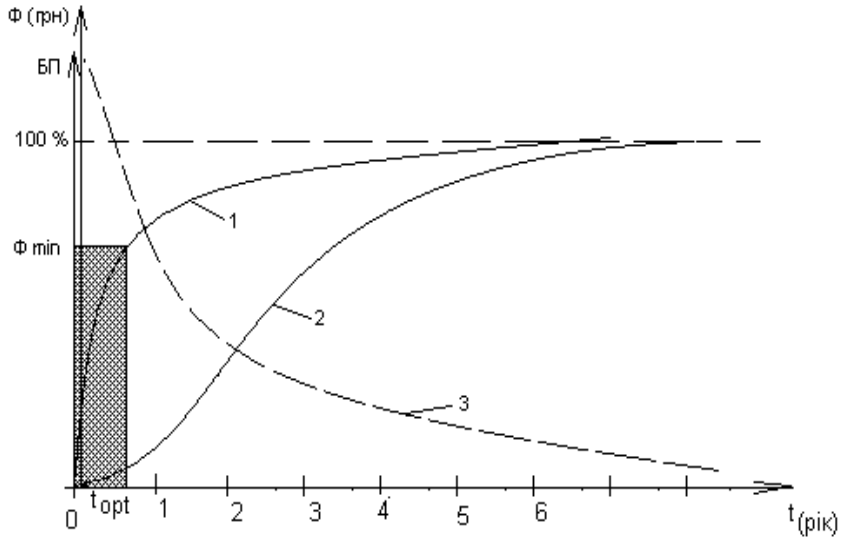

Рис. 1.5. Співвідношення нарощування бойового потенціалу збройних сил та фінансових витрат:

1 – графік нарощування бойового потенціалу з застосуванням високотехнологічних систем ОВТ;

2 – графік нарощування бойового потенціалу звичайними засобами озброєння;

3 – графік обсягу фінансових витрат.

Якісний аналіз реалізації вказаних концепцій показаний на рис. 1.6. Враховуючи показник часу, необхідного для нарощування до 80% бойового потенціалу збройних сил, приходимо до висновку, що найбільш раціональною є перша з розглянутих концепцій. Відповідно до цієї концепції необхідна зміна принципів трансформації ЗС України: за рахунок наявного озброєння та високотехнологічних систем і засобів створити боєздатні сили превентивного реагування та сконцентрувати управління ними в єдиному органі. При відповідній концентрації сил, засобів і управління буде забезпечений високий оборонний потенціал держави, а резерв часу дасть можливість визначити напрями розвитку й удосконалення ОВТ, розробити зброю нових поколінь. У подальшому це дозволить без шкоди для воєнної безпеки держави подолати технологічний розрив у переозброєнні порівняно зі збройними силами інших держав.

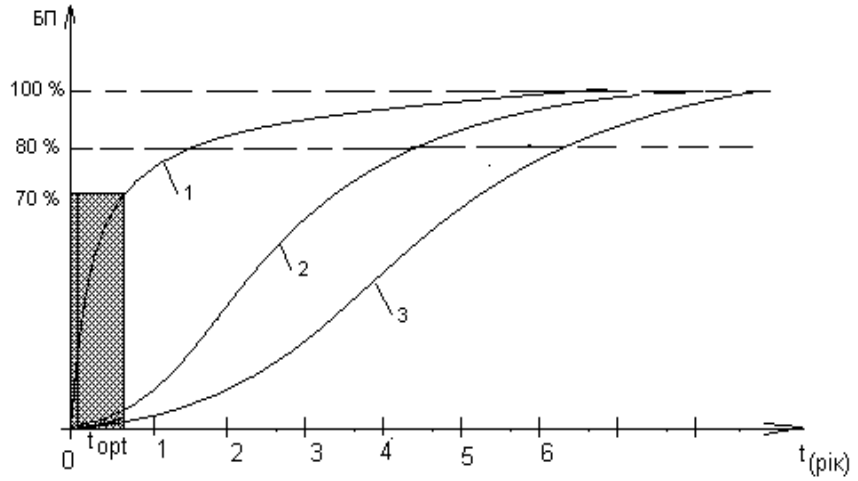

Рис. 1.6. Зіставлення варіантів нарощування бойового потенціалу збройних сил держави:

1 – нарощування бойового потенціалу за рахунок застосування високотехнологічних систем ОВТ;

2 – нарощування бойового потенціалу за рахунок модернізації ОВТ;

3 – нарощування бойового потенціалу за рахунок структурної перебудови збройних сил, продовження термінів експлуатації існуючих зразків ОВТ, нарощування обсягу виробництва існуючих зразків.

Для практичної реалізації зазначеного після апробації ВТС ОВТ визначаються найбільш перспективні зразки і здійснюється їх впровадження в масове виробництво для переоснащення збройних сил. Показником належності зразка зброї до високотехнологічних систем є коефіцієнт співвідношення максимальної ефективності досягнення поставленої мети та мінімальних загальних витрат. Показником, за яким відбирають високотехнологічні системи і засоби для масового переоснащення збройних сил, слід вважати здатність ВТС ОВТ забезпечити стратегічну перевагу протягом певного проміжку часу (декілька років і більше) поки не з’явиться ефективний засіб протидії.

Таким чином, дослідження сутності високотехнологічних воєнних конфліктів показав, що найбільш прийнятним, стосовно забезпечення національної безпеки у воєнній сфері у високотехнологічному суспільстві, шляхом є реалізація стратегії превентивної оборони.

Розроблення і практична реалізація стратегії превентивної оборони держави, яка спроможна забезпечити адекватне і своєчасне реагування на загрози національній безпеці України у воєнній сфері, об’єктивно буде базуватися на застосуванні високотехнологічного озброєння і військової техніки та інноваційних технологіях управління.

Високотехнологічні системи і засоби здатні не тільки забезпечити реалізацію превентивної оборони, збереження бойового потенціалу збройних сил на час їх переозброєння і трансформації, а також дозволяють підтримати необхідний рівень обороноздатності держави. У разі розвитку високотехнологічних систем ОВТ за визначений проміжок часу та при необхідному рівні фінансування розробки озброєння, час досягнення

мінімально достатнього потенціалу скорочується на декілька років, порівнянно з варіантом нарощування потенціалу збройних сил за рахунок збільшення кількості звичайних зразків ОВТ, та дозволяє отримати резерв часу на переозброєння збройних сил у цілому.

Інноваційні технології ведення війн та управління сучасними бойовими діями передбачають, що удари будуть наноситися перш за все по системі державного і воєнного управління, ключовим акторам (особам) Сектору національної безпеки й оборони, найважливішим об'єктам із забезпеченням гранично досяжних швидкості й точності дії на їх "критичні" складові, здебільшого одночасно на всій території держави (регіону). Реалізація таких підходів забезпечує найбільш ефективне досягнення мети. Це підтверджується й результатами розгляду систем забезпечення національної безпеки будь-яких держав з якого видно, що в них обов'язково є найбільш уразливі точки (підсистеми, складові, об'єкти), які отримали назву "слабких ланок", "слабких місць", "больових" або "критичних" точок (елементів, об'єктів), "центрів гравітації" або "центрів тяжіння", вплив на які або знищує систему, або неприпустимим чином змінює її характеристики й алгоритми функціонування. Порушення їхнього функціонування або знищення позбавляє державу, по якій завдаються удари, та її збройні сили здатності чи сенсу подальшого ведення війни.

Завдяки використанню інноваційних технологій у цих війнах став можливим перехід від дій загальноруйнівного характеру до дій із перевагою функціонально-структурного, виборчого впливу на супротивника. Базовий принцип досягнення мети дій трансформувався із інформаційно-економіко-силового протиборства в принцип інформаційно-кібер-технологічно-економіко-силового протиборства. При цьому технологічна складова включає не тільки високі технології виготовлення та застосування озброєння та військової техніки, інформаційні технології й інноваційні технології управління, а повний спектр найбільш передових та досконалих технологій, які забезпечують ефективне ведення бойових та інших дій і війни в цілому із забезпеченням безумовної переваги над противником.

Мережноцентрична війна

Вперше концептуальні питання та основи теорії мережноцентричної системи управління та організації бойових дій та кібердій (реалізована у воєнних доктринах США "Joint Vision 2010", "Joint Vision 2020") і фактично розгляд воєнних дій та їх організації з позицій воєнної кібернетики були сформульовані Миколою Огарковим наприкінці 70-х – початку 80-х років XX століття [27].

Впровадження та апробацію нового підходу до організації дій під час проведення військових операцій для отримання максимального ефекту від впливу на три сфери (моральну, ментальну та фізичну) здійснив Джон Бойд під час проведення операції "Буря в пустелі" в 1991 році. Він розглядав війну, як поєднання цих трьох складових. Руйнування волі противника до досягнення перемоги шляхом його відділення від союзників (або потенційних союзників) і

внутрішнього роздроблення, підриву загальної віри і спільних поглядів (moral warfare). Дії спрямовані на деформацію і спотворення сприйняття противником реальності на основі дезінформації та створення неправильних уявлень про ситуацію (mental warfare). Руйнування фізичних ресурсів противника (озброєння, жива сила, інфраструктура і предмети постачання тощо) (physical warfare). При цьому всі дії, як своїх сил, так і сил противника він запропонував розглядати в рамках циклу, що має у своїй структурі 4 процеси: спостереження, орієнтація, рішення, дія (OODA – цикл або "петля Бойда"), який, за думкою автора, сам відтворюється і саморегулюється (опубліковано в 1995 р. [28]). Надалі він був покладений в основу концепції командування й управління, а також можливостей пов'язаних з ними, під кодовою назвою RTO-TR-SAS-050, яка була введена в Пентагоні та в НАТО, як модель C2 (Command and Control, тобто командування й управління) та згодом перетворилася в C4IR (Command, Control, Communication, Computers, Intelligence And Recognition – командування, управління, комунікації, комп'ютери, розвідка, усвідомлення), а також в інші модифікації, наприклад C4IEWS & IM (Command, Control, Communications, Computers, Intelligence, Electronic Warfare, Sensors and Information Management – командування, управління, комунікації, комп'ютери, розвідка, електронна війна, сенсори й інформаційний менеджмент).

В 2003 році модифікований варіант "петлі Бойда" – "Критика-Дослідження-Порівняння-Адаптація" був запропонований Девідом Брайантоном [29].

Питання системного порушення управління та функціонування держави до кризового рівня були запропоновані та реалізовані під час підготовки операції "Буря в пустелі" в 1991 році Джоном Уорденом. Він розробив системний підхід до сучасних бойових дій, назвавши його "операції на основі ефектів" (EBO – Effect-based-Operations), який враховував розробки Дж. Бойда та став подальшим розвитком кібер-інформаційної концепції мережецентричної організації дій з елементами теорії обмеження систем. Відповідно до цієї концепції є п'ять основних сегментів: збройні сили, виробництво, інфраструктура і комунікації, населення і уряд – життєво важливих для будь-якої держави. Кожна держава має в них свої унікальні місця уразливості (які отримали назви: "центри тяжіння", "центри гравітації", "критичні вузли (точки)" тощо). Їх правильне виявлення та деструктивний вплив на них призводить до ефекту системного "паралічу" держави в тих чи інших сферах або в цілому.

Генерал Девід Дептула здійснив подальший розвиток поглядів Уордена та змісту війн 4GW. Він запропонував розгляд ворога як системи на всіх національних рівнях, включаючи дипломатичний, інформаційний, економічний тощо і вважав, що невійськові дії є невід'ємною складовою нової теорії конфлікту. В рамках цього у США були створені спецгрупи для роботи в Іраку і Афганістані, до яких входили соціологи, етнографи, лінгвісти та інші фахівці. Команди Human Terrain спілкувалися з місцевим населенням, досліджували його звички, поведінку, ієрархічну структуру, слабкі і сильні сторони тієї чи іншої соціальної, етнічної і релігійної групи, впливали на їх свідомість тощо. Тобто, фактично формували інформаційний базис для ведення когнітивних дій. В 2014 Девід Дептула разом з

Джоном Алленом на конференції “Нова воєнна стратегія США для нової ери: перевага, швидкість і ефективність» презентував новий концепт: “DIMET” – операцій (DIMET: дипломатія, інформація, військова сила, економіка (включно фінанси) і технології), в якому ключовою складовою є високі технології [30].

Вперше системно-концептуальне викладення теорії мережецентричних війн з визначенням в ній ролі і місця інформаційних та інших високотехнологічних складових здійснили в публікації “Мережноцентрична війна: її походження і майбутнє” (січень 1998 р.) Артур Себровскі (тоді директор програми Пентагону N6 (Space, Information Warfare, Command and Control) і Джон Гарстка (тоді науковий і технічний радник Управління систем С4 Об'єднаного штабу).

З початку 2000 років у США в інтересах підвищення ефективності дій сил спеціальних операцій було впроваджено інформаційно-кібернетичний цикл F3EAD (Find, Fix, Finish, Exploit, Analyze and Disseminate). Його реалізація спрямована на отримання можливостей передбачати дії противника, виявляти і визначати місцезнаходження і цілі ворожих сил. Центральним місцем у процесі F3EAD є функціональне злиття в єдиний процес розвідки й операцій.

Поява концепції мережноценричних воєн обумовлено стрімким розвитком високих технологій і можливостей, які вони надають у військовій сфері. За поглядами Артура Себровскі і Джона Гарстки “мережноцентрична війна” – це комплекс взаємоузгоджених заходів по розгортанню цифрових мереж з метою забезпечення, як вертикальної, так і горизонтальної інтеграції всіх учасників операції, зміна тактики дій перспективних формувань з розосередженими бойовими порядками, оптимізація способів розвідувальної діяльності, спрощення процедур узгодження та координації вогневого ураження, а також деяке нівелювання розмежування засобів по ланках управління. При цьому, підвищення бойових можливостей сучасних формувань – прямий наслідок поліпшення інформаційного обміну і зростання ролі самої інформації, а досягнення цілей залежить від випередження супротивника в часі за всімах основними аспектами.

Прикладами реалізації даної концепції є: “Комплексні мережні можливості” в НАТО (NATO Network Enabled Capabilities), “Інформаційно-центрична війна” (Guerre Infocentre) у Франції, “Мережна оборона” (Network Based Defense) у Швеції, “Система бойового управління, зв'язку, обчислювальної техніки, розвідки і вогневого ураження” (Command, Control, Communications, Computers, Intelligence, Surveillance, Recognizance & Kill) в Китаї і т.ін.

Зазначені та подібні їм системи призначені для:

– забезпечення й отримання всієї необхідної розвідувальної інформації в реальному масштабі часу, її узагальнення та розподілу, аналізу отриманих відомостей та їх обробки;

– відображення розвідувальних даних на електронних картах всіх зацікавлених осіб із занесенням їх одночасно в базу даних, розподіляючи її за споживачами;

– аналізу різних варіантів загроз, що виходять від розвіданих об'єктів, здійснення прогнозу розвитку ситуації в районі їх дислокації на поточний час і на певну перспективу і можливих раціональних варіантів дій, на основі реальних даних з генеруванням пропозицій по нейтралізації загроз, як одиночного, так і

комплексного характеру;

– розрахунку потреб у силах і засобах для реалізації прийнятих рішень, кількості ракет, боєприпасів інших матеріальних засобів, а також, необхідний час на реакцію, на реалізацію, на забезпечення необхідними силами і засобами, необхідними запасами матеріальних засобів і їх відновлення на необхідному рівні (для безумовної реалізації рішення по кожній наступній задачі);

– способах і термінах їх поповнення, термінах та способах виконання задач, із зазначенням результатів виконання та термінів готовності до подальших дій;

– підготовки та видачі необхідних розпоряджень, після прийняття рішення та інформування взаємодіючих структур;

– аналізу результатів, отриманих в ході виконання задач, з урахуванням інформації, що надходить від вищестоящих, взаємодіючих і підлеглих штабів і т.п.

Практична реалізація концепції мережноцентричних війн залежить від можливостей систем розвідки, зв'язку, систем вогневого і невогневого ураження (придушення) і особливо від системи управління, що об'єднує їх в єдине ціле.

Необхідними умовами успішності мережноцентричних дій, є:

– перевага своїх систем розвідки перед системами розвідки противника, включаючи достовірність, своєчасність і точність добутої інформації;

– перевага інформаційно-комунікаційних систем, що дозволяють в реальному масштабі часу отримувати і передавати великі обсяги інформації різним споживачам, включаючи і централізовану і розподілену передачу, забезпечуючи систематичний і своєчасний обмін між суб'єктами системи;

– всебічна підготовка особового складу, який експлуатує всі технологічні системи і програмні комплекси, що утворюють єдиний інформаційно-кібернетичний бойовий простір.

У цілому, мережноцентричну війну можна розглядати, як сукупність дій, заснованих на повній інформаційній та ситуаційній обізнаності по всьому спектру інформації, включаючи і доступність особистої інформації про індивідуумів, за умови переваги інформаційно-комунікаційних систем, системи управління силами і засобами на додаток до переваги в засобах вогневого (кінетичного) і невогневого впливу.

Кібервійна й інформаційна війна є складовими частинами мережно-центричної війни, як і будь-якої високотехнологічної війни.

Під кібервійною будемо розуміти високотехнологічний конфлікт, продовження політики держав і (або) коаліцій, політичних угруповань, транснаціональних корпорацій і т.д. з метою нав'язати опонентам свою волю за допомогою впливу на них у кіберпросторі і через нього в різних сферах життєдіяльності у формі кіберпротиборства, військових (кібер-) дій між їх кіберсилами (кібервійськами).

Особливості даного типу війн є: складність (неможливість) ідентифікації агресора; скритність впливу і відсутність (на початкових етапах) видимих руйнувань; надзвичайна швидкість проведення атак, коли проміжок часу між початком “агресії” і її наслідками скорочується до мінімуму; на даному етапі для кіберзброї не мають значення кордони та відстань, а також відсутні технологічні,

юридичні та інші перешкоди; наявність синергетичних, ланцюгових, вторинних, третинних і т.п. ефектів.

Всі основні теоретичні дослідження і практика ведення війн нового високотехнологічного типу яскраво демонструють, що запорукою перемоги в них є забезпечення досягнення інформаційної і технологічної переваги над противником та високоефективне управління. При цьому інформаційна перевага передбачає створення систем отримання, обробки та аналізу інформації, надійних мереж, які об'єднують свої війська (сили) і засоби та надають їм змогу покращеного обміну інформацією та забезпечують своєчасну і повну загальну ситуаційну поінформованість командирів. Загальна ситуаційна обізнаність дозволяє забезпечувати співробітництво і самосинхронізацію, підвищує стійкість і швидкість роботи команди, а це, у свою чергу, підвищує ефективність місії. Апробація такої розподіленої інформаційної системи бойового керування FBCB2 (Force XXI Battle Command Brigade or Below), яка охоплювала рівень "бригада-батальйон-рота" відбулася в Іраку у 2003 році [31]. Разом з цим, проведена апробація яскраво продемонструвала, що необхідно забезпечити випереджаюче знищення (виведення з ладу, придушення) системи розвідувально-інформаційного забезпечення та управління у противника (засобів та систем розвідки, мережноутворюючих вузлів, центрів обробки інформації та управління).

Як зазначив адмірал Вернер Кларк: "У майбутніх операціях будуть використовуватися революційні інформаційні технології і можливості розосереджених сил, об'єднаних єдиним інформаційним простором, для досягнення безпрецедентної наступальної могутності, гарантованої оборони й операбельності у складі об'єднаних з'єднань".

На цей час у світі існує близько 40 ключових макротехнологій, які за думкою провідних експертів визначають рівень економіки та обороноздатності країн у сучасних умовах.

До високих оборонних технологій та технологій подвійного призначення (англ. high technology, hi-tech) частіше за все відносять такі найбільш нові і прогресивні технології сучасності: штучний інтелект, космічні, робототехнічні, інформаційні та кібертехнології; нано-, квантові, нейронні, біотехнології, генну інженерію, інноваційні електромеханіку, електроніку, матеріаловедення, створення нових напівпровідникових матеріалів, генерування, акумулювання та передача енергії, "чисті" (cleantech) та енергозберігаючі технології, телекомунікаційні, інфокомунікаційні технології та технології управління й автоматизації тощо.

Гібридна війна

Гібридна війна, яка де-юре ведеться на території України, а де-факто охоплює все більше учасників в усьому світі [1, 3-5, 33] за своїм змістом, формами і способами ведення може розглядатися як специфічний варіант реалізації воєн четверного покоління [2]. Тобто конфлікт, який характеризується стиранням відмінностей між безпосередньо війною, політикою й економікою, між військовими, які беруть участь у війні, і мирним населенням. Ці ідеї виникли ще за часів Холодної війни, коли наддержавам стало зрозуміло, що широкомасштабне

використання танків, авіації і ракет у цих умовах є малоефективним, а роль підривних операцій (як партизанських, так і політичних, економічних, інформаційних, психологічних) якісно і кількісно зросла.

Під інформаційними операціями (InfoOp) в керівних документах НАТО [61] прийнято вважати скоординоване використання (під час військових операцій) спроможностей, що пов'язані з використанням інформації, та узгоджене з іншими лініями діяльності в рамках операції з метою впливу на порушення функціонування, підриву та отримання контролю (узурпації) над процесом прийняття рішення противниками або потенційними противниками, захищаючи при цьому свій процес прийняття рішенння.

Психологічні операції (PsyOp) – це операції з поширення визначеної інформації та виконання дій щодо цільових аудиторій для впливу на їх емоції, мотиви, об'єктивне мислення та поведінку урядів, організацій, груп та окремих осіб. Процес PsyOp складається з наступних елементів: планування, аналізу, синхронізації, розробки, дизайну, вироблення, доставки, розповсюдження, управління та оцінювання PsyOp продукції та дій, що спрямовуються на обрану цільову аудиторію (target audiences – TAs) [62, 63].

Взагалі, у сучасних конфліктах досягнення мети агресії зазвичай починається з несилових методів, головним чином економічних, політичних, дипломатичних, інформаційних, психологічних, кібер-, когнітивних і т.ін. дій.

У цілому, у сучасних війнах (воєнних конфліктах, а особливо у гібридних конфліктах) будь-якої інтенсивності, бойові дії (операції) є складовою взаємоузгоджених за єдиним задумом і планом інших (несилових) дій, які превалюють на всіх їх стадіях. Цим створюються дестабілізуючі внутрішні і зовнішні процеси в державі, яка є об'єктом агресії (стурбованість і невдоволення населення, міграція, акції громадянської непокори тощо). Надалі для досягнення стратегічних цілей застосовуються методи ведення дій з широкомасштабним залученням сил і засобів розвідки, оперативного управління військами (силами) і засобами, а також традиційних засобів ураження, державних збройних формувань, некомбатантів й інших учасників (терористів, радикальних озброєних груп, рухів опору , найманців, партизан), сил спеціальних операцій і т.п. Таким чином, гібридність сучасних конфліктів базується на можливостях, які є похідною високотехнологічного розвитку людства. А сама ***гібридна війна*** є високотехнологічним конфліктом, продовженням політики держав (коаліцій, політичних угруповань, транснаціональних корпорацій і т.п.) з метою нав'язування опонентам своєї волі за допомогою комплексних адаптивних і асиметричних синхронізованих впливів на них в різних просторах і сферах з поєднанням конвенційної та неконвенційної складових, забезпеченням багатовимірності, мультипликативності і синергетичних результатів та високого рівня невизначеності для опонентів по відношенню до кінцевих цілей і шляхів їх досягнення (рис. 1.7) [33].

Гібридна війна не оголошується і тому не може бути завершена в класичному розумінні завершення воєн і воєнних конфліктів. Це перманентна війна змінної інтенсивності. Вплив йде на всі сфери життя, на всі верстви суспільства і на всій території держави. Завдяки використанню інноваційних технологій став можливим

перехід від дій загально-руйнівного характеру до дій з переважно функціонально-структурним впливом на противника, а найголовніше – досягненням над ним когнітивної переваги.

Деструктивні впливи в ній супроводжуються, як правило, ланцюговими ефектами і синергетичними наслідками. У гібридних війнах тою чи іншою мірою свідомо чи несвідомо задіяне не тільки все населення країни, яка стала об'єктом агресії, а й міжнародне співтовариство. У гібридних конфліктах військові дії поєднуються з іншими, головним чином економічними, політичними, дипломатичними, інформаційними, психологічними, кібер-, когнітивними й іншими діями, які комплексно призводять до системної дестабілізації в усіх сферах життя і діяльності держави, яка є об'єктом агресії.

Гібридна війна, яка ведеться на території України з 2014 року, фактично охоплює все більше учасників в усьому світі. Це конфлікт, в якому стираються відмінності між безпосередньо війною в її класичному розумінні, і політикою та економікою, між військовими й іншими її учасниками та мирним населенням.

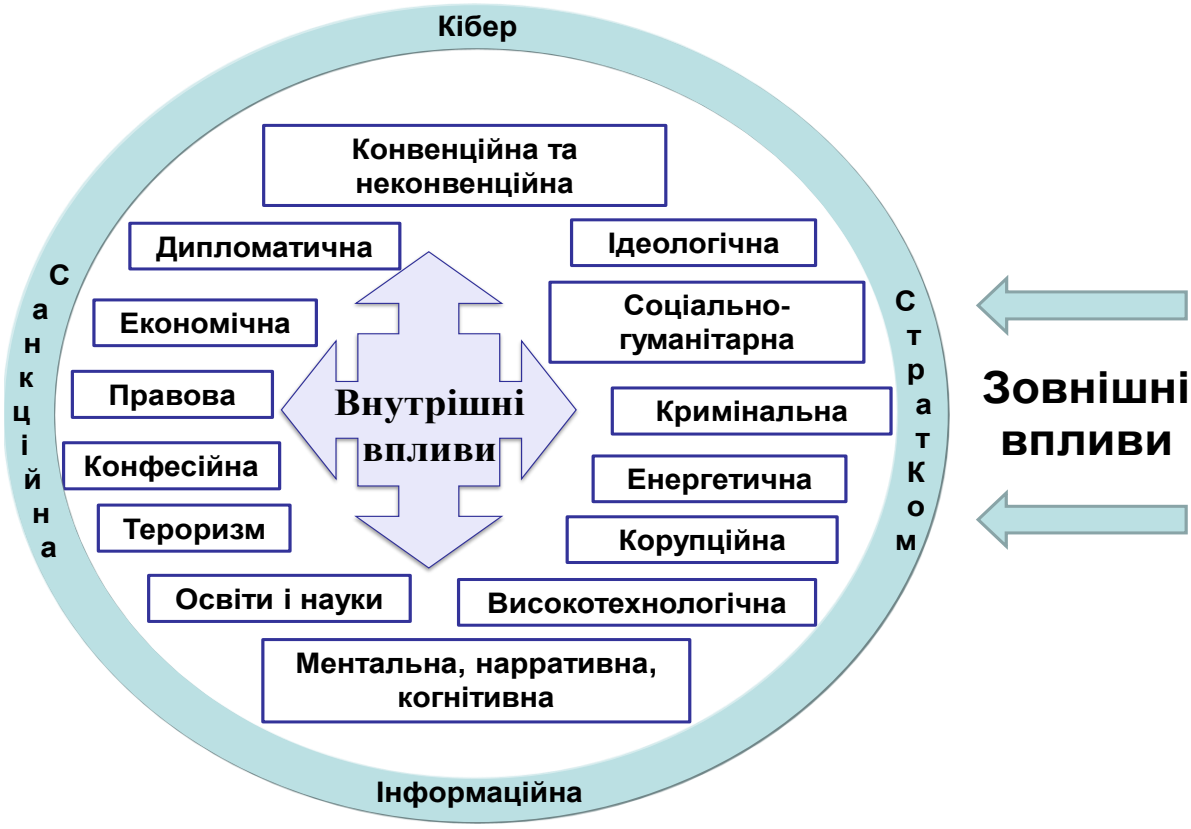

Рис. 1.7. Сфери гібридної війни

Сили та засоби гібридної війни застосовуються за єдиним замислом і планом, узгоджені в діях за часом і простором (рис. 1.8). До них можна віднести:

– системи оперативного управління силами та засобами;
– класичні та інноваційні засоби озброєння та військової техніки;
– високотехнологічні сили та засоби;

– стратегічні комунікації;
– сили та засоби розвідки;
– недержавні, нерегулярні збройні формування, волонтери;
– сепаратистські рухи;
– кримінальні елементи;
– регулярні збройні формування та сили спеціальних операцій;
– некомботанти, партизани, рухи опору;
– приватні військові формування;
– кібервійська та інформаційно-психологічні підрозділи;
– високотехнологічна система логістики.

Рис.1.8. Сили та засоби гібридної війни

Начальник Генерального штабу ЗС РФ Валерій Герасимов у своєму виступі на щорічних зборах Академії військових наук 4 березня 2019 року вказав на суттєве зростання значущості інформаційної сфери протиборства: “При цьому інформаційні технології становлять, по суті, одним із найбільш перспективних видів зброї. Інформаційна сфера, не маючи чітко окреслених національних кордонів, забезпечує можливості дистанційного, прихованого впливу на критичну важливу інформаційну інфраструктуру, а також на населення країни, безпосередньо впливаючи на стан національної безпеки держави. Саме тому опрацювання питань підготовки та ведення дій інформаційного характеру є важливим завданням військової науки. Цифрові технології, роботи, безпілотні системи, РЕБ – все це повинно бути в порядку денному розвитку воєнної науки, у том числі, воєнної стратегії”. Як бачимо,

акцент зроблено на комплексне застосування новітніх засобів ведення сучасної війни гібридного типу, але з націленістю на критично важливу інформаційну інфраструктуру.

За його поглядами гібридна війна має такі особливості:

− акцент змістився на використання політичних, економічних, інформаційних, гуманітарних та інших невійськових заходів поряд із застосуванням протестного потенціалу місцевого населення. Все це повинно супроводжуватися прихованими військовими операціями – наприклад, методами інформаційної війни і застосуванням спецназу;

− широке розповсюдження отримали асиметричні дії, що дозволяють нівелювати перевагу противника у збройній боротьбі. До них належать використання сил спеціальних операцій та внутрішньої опозиції для створення постійно діючого фронту на всій території держави противника, а також інформаційний вплив, форми і засоби якого весь час удосконалюються. Інформаційне протиборство відкриває широкі асиметричні можливості для зменшення бойового потенціалу противника;

− фронтальні зіткнення великих угруповань військ (сил) на стратегічному та оперативному рівнях поступово відходять в минуле. Дистанційний, безконтактний вплив на противника стає головним засобом досягнення цілей бою та операції;

− відкрите використання сили, часто під прикриттям миротворчої діяльності та посередництва у вирішенні кризи, повинно застосовуватися на фінальній стадії, як правило, щоб домогтися повної перемоги у війні.

Очевидно, що за задумом ГШ ЗС РФ це має привести до дисфункції або як мінімум паралічу системи державного та воєнного управління противника з подальшою його хаотизацією. [32].

Ментальні, наративні, когнітивні аспекти гібрідної війни

Когнітивне протиборство стало невід'ємною складовою сучасних і майбутніх війн і воєнних конфліктів, як міждержавних і внутрішньодержавних, так і між будь-якими геополітичними і регіональними акторами. Когнітивній складовій належить виняткова роль у сукупності факторів, що формують і викликають воєнний конфлікт, впливають на його хід і результати, інтенсивність і наслідки. Тому, сучасні війни, особливо війни майбутнього, ведуться за когнітивну сферу соціуму (суспільства, соціальних груп, особи) й управління нею (ним).

Когнітивні впливи можуть бути навмисними і випадковими, багатовекторними і комплексними, загальної спрямованості або цільовими (цілеспрямованими), спрямованими на суспільство в цілому або на конкретні спільноти або індивідів, на досягнення короткочасного або довготривалого ефекту, негайно або після латентної фази, з варіацією значень або без і т.д.

У сучасних умовах всі сторони конфлікту прагнуть взяти під контроль саме когнітивний простір, що охоплює сприйняття, усвідомлення, переконання, розуміння і цінності, інтелектуальне середовище, як індивідів, так і соціальних

груп і суспільства в цілому, в якому, власне, і відбувається прийняття ними рішень. Тому головний результат успішних когнітивних процесів – це зміна моделі світу і його сприйняття в людині, соціальних групах суспільства, і суспільство в цілому, що забезпечує можливість взяття їх під контроль і здійснення зовнішнього управління ними на емоційному, моральному, культурному, світоглядному і ментальному рівнях, з формуванням стереотипів для сприйняття дійсності через їх призму. Особливе значення мають при цьому нав'язування і просування помилкових наукових, громадських, економічних, державних, військових теорій, парадигм, концепцій, стратегій, наративів, які найбільш ефективно просуваються і впроваджуються через навчальні заклади і наукові установи, громадські організації, електронні, соціальні мережі і блогосферу. Наратив – це найсильніший тип впливу. Тому їх використання у гібрідній війні є однією з особливостей. Наратив допомагає людині створити ментальну картинку дійсності. Рішення залежать від ментальної моделі, яку виробляє людина для розуміння того, що відбувається. Саме звідси виникають оцінки та дії.

З цією метою використовуються всі можливості стратегічних комунікацій, ведуться інформаційні, психологічні, кібер- та інші дії (акції, операції тощо), які спрямовані як на безпосередніх учасників конфлікту, так і на населення країн, які беруть у ньому участь, міжнародне співтовариство. Особливістю є те, що навіть при проведенні державними акторами (actors – діючі особи, учасники) дій планово й узгоджено, вони проходять на тлі хаотичних цільових і випадкових подібних дій всіх інших акторів. Це трансформується в інформаційно-кібернетичний і когнітивний варіант війни “всіх проти всіх” (в кібер-, інформаційному і когнітивному просторах). В результаті, як показують проведені дослідження, об'єкти, на які спрямовані когнітивні впливи можуть бути не просто введені в стан когнітивного резонансу, дисонансу або дисбалансу, а й можуть отримати інформаційні та когнітивні травми, дійти до когнітивної межі сприйняття (неможливості подальшого безпечного сприйняття когнітивних та інформаційних впливів), часткової або повної когнітивної дезорієнтації і навіть до інформаційно-когнітивного колапсу, з подальшим переходом в стан когнітивної агресії або розчарування в усьому, апатії і депресії. Тобто, отримати стресові розлади обумовлені інформаційно-когнітивним травмуванням.

В гібридній війні практично вся територія країн є зоною активних інформаційних (кібер-, когнітивних) деструктивних дій різної природи і характеру.

Наслідки гібридної війни (конфлікту) не обмежуються кількістю загиблих, покалічених і руйнувань. Вони також включають наслідки впливу на когнітивну сферу громадян, соціальних груп і суспільства в цілому. Це обумовлено, як прямим, так і непрямим й опосередкованим впливом на свідомість і підсвідомість, психофізіологічний, психічний стан і здоров'я людей, які як брали участь у конфлікті, так і просто перебували в зоні воєнних дій (конвенціональна складова гібридної війни) і на все населення країни

(частково й інших країн) де відбувається конфлікт з геопросторовою й іншими видами диференціації такого впливу. Як результат, когнітивна сфера людей, підвладна впливам факторів гібридного конфлікту різної інтенсивності і змісту, виявляється трансформованою у сприйнятті мирної обстановки (в тому числі в обстановці постгібридного світу), стандартних цінностей суспільства, оцінки мирними громадянами пережитого учасниками військових дій.

У ньому вперше повною мірою проявляється інформаційно-когнітивне ураження, як окремих суб'єктів, так і соціальних груп. Крім того, також вперше, починають мати місце суспільно-соціальні групові симптоми і т.ін.

Інформаційні контексти змінюються вже з більшою швидкістю, ніж сучасна людина може їх обробляти. А в умовах їх деструктивності та в поєднанні зі стресовими впливами, відбувається інформаційно-когнітивний розлад осіб, від часткового до повного. Тобто, в умовах сучасних воєнних конфліктів різноманітним, в першу чергу інформаційно-когнітивним стресовим впливам на свідомість і підсвідомість піддаються не тільки ті люди, які брали безпосередню участь у бойових діях, але й, тою чи іншою мірою, все населення країни де відбувається гібридна війна. Взагалі, особливо сильними та найбільш інтенсивними інформаційні, психологічні, кібернетичні, когнітивні впливи є саме в умовах "гібридної війни", коли вони є цілеспрямованими і фактично є уражаючими факторами інноваційної зброї, яка все ширше і масивніше застосовується разом з іншими засобами впливу.

Когнітивний простір є метою будь-якої інформаційної війни. Первинна мета, в зміні моделі світу в мозку людини. Можна прекрасно передавати повідомлення, які в результаті не ведуть нікуди.

Сьогодні Інтернет як засіб маніпуляції посідає одне з головних місць, в якому формуються нові форми соціального спілкування. Саме Інтернет є засобом маніпуляції, контролю та управління свідомістю, коли оформлення повідомлень реалізується шляхом модифікації інформації про події чи факти з використанням таких прийомів, як фабрикація фактів, пропаганда, створення паніки. У полі публічної політики активно використовуються технології Інтернет-дискусій за участю "веб-бригад". "Веб-бригади" – контрольовані замовником Інтернет-користувачі, основна мета яких – формування потрібної замовнику громадської думки та маніпуляція суспільною думкою в Інтернеті.

Кібервпливи часто приховують своїх дійових осіб та мотиви за технологічними методами, які можуть маскувати їх маніпулятивні цілі. До таких методів можна додати анонімні претензії на владу, новинні повідомлення, які маніпульовані напівправдою, повторення таких повідомлень, інформаційне перевантаження, а також операції Astroturfing, Cyber-Pseudo, Cyber-Herding та Sock-Puppeting [33, 46].

Астротурфінг (англ. *Astroturfing*) – створення штучної громадської думки за допомогою гласних чи негласних заходів, форм та методів впливу зацікавленими іноземними спеціальними службами, окремими організаціями, групами та особами, що використовують програмне забезпечення або наймають представників засобів масової інформації, блогерів, інтернет-коментаторів,

спеціалістів з метою витіснення думки реальних людей і створення враження, наче значна кількість людей вимагає чогось конкретного або виступає проти чого-небудь. Наприклад, просування товарів, ідей або прийняття певних рішень органами державної влади та органами місцевого самоврядування у політичній, соціальній, економічній та інших сферах.

Cyber-Pseudo – це дії, коли уряд видає себе за повстанців.

Cyber-Herding – це дії, коли урядові агенти грають роль онлайн-коментаторів.

Sock-Puppeting – створення хибних аккаунтів, з метою в ведення в оману або маніпулювання.

Отже, характерною особливістю ведення війн та збройних конфліктів XXI століття є те, що вони вирізняються низкою певних факторів. До них відносяться наступні: висока динамічність бойових дій, відсутність чіткої лінії фронту, застосування сучасного озброєння і бойової техніки, інформаційні, психологічні, когнітивні та кібердії стають невід'ємною і превалюючою складовою воєнних дій; виникнення єдиного бойового простору (простору ведення операцій) з новими характеристиками: нелінійність, відсутність у традиційному розумінні фронту, флангу, тилу, розподіленість одночасно з інтегрованістю та багатомірністю; динамічність зміни просторових масштабів конфліктів, можливість швидкого їх переростання з локального на глобальний рівень зростання швидкості змін обстановки та загальної динаміки дій, маневреності дій військ (сил) на розрізнених напрямах ведення дій в зонах (районах) з високим ступенем урбанізації; зростання асиметричності в характері бойових дій та широке залучення до протиборства іррегулярних та спеціальних формувань; значна частина бойових дій ведеться на високоурбанізованих територіях зі значною щільністю населення, серед житлових, виробничих, рекреаційних, інфраструктурних та інших об'єктів.

1.1.2. Кіберпростір як сфера ведення війн сучасності та майбутнього

Розвиток інформаційних і кібертехнологій та глобальна інформатизація призвели до того, що інформаційна та кіберсфери стали сферами, в яких та через які здійснюються різноманітні деструктивні впливи на усі сфери діяльності суспільства. Кіберпростір доповнив існуючі: сухопутний, морський, повітряний, космічний та став новою і першою штучно утвореною сферою конфліктів і можливих бойових дій. При цьому, за рахунок дій, які мають місце в ньому, відбувається зміна традиційних форм і способів ведення протиборства в усіх природніх просторах. Більше того, майбутня війна може бути спровокована в кіберпросторі.

Поняття "***кіберпростір***" (cyberspace) вперше використано у 1984 р. американським письменником Уільямом Гібсоном ("Нейромант") для позначення всієї сукупності інформації, що міститься у комп'ютерних мережах. У Доктрині інформаційних операцій ЗС США 2006 р. (JP 3-13 Information

Operations Doctrine) було визначено: “*кіберпростір* – віртуальна обстановка, в якій цифрова інформація циркулює в комп’ютерних мережах”.

Перше офіційне визначення кіберпростору було дано військовими експертами США у “Настанові з інформаційних операцій” 2006 року: “**Кіберпростір** – сфера, в якій застосовуються різні радіоелектронні засоби (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення), що використовують широкий діапазон електромагнітного спектра частот для прийому, передачі, обробки, зберігання, перетворення й обміну інформацією, і пов'язана з ними інформаційна інфраструктура ЗС США”. З розвитком та розповсюдженням цифрових технологій поняття розширилось до позначення сукупності всіх електронних систем.

Так, згідно з рекомендаціями Міжнародного союзу електрозв’язку (МСЕ, англ. International Telecommunication Union, ITU) [35] ***кіберпростір*** – сукупність користувачів, мереж, пристроїв, програмного забезпечення, процесів, збереженої або транзитної інформації, додатків, послуг та систем, які можуть бути прямо чи опосередковано під’єднані до мереж.

У спільній публікації США JP 3-12 (Cyberspace Operations) [36] та у Словнику військових термінів Міністерства оборони США [37] визначено, що ***кіберпростір*** **–** це глобальний домен в інформаційному середовищі, що складається зі взаємозалежних мереж інфраструктури, інформаційних технологій і резидентних даних, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори та контролери. Кіберпростір складається з трьох шарів: фізичної мережі, логічної мережі та кіберперсон.

Шар фізичної мережі *(physical network layer)* – включає ІТ прилади та інфраструктуру у фізичному вимірі, що забезпечують зберігання, передачу та обробку інформації у кіберпросторі, включаючи сховища даних та сполучення, які передають дані між компонентами мереж.

Шар логічної мережі *(logical network layer)* – складається із тих елементів мереж, що поєднуються одні з іншими у спосіб, який є абстрактним від фізичної мережі та базується на логічному програмуванні (коді), який управляє компонентами мережі (тобто, взаємозв'язки не обов'язково стосуються конкретних фізично існуючих зв'язків чи вузлів, але їхньої здатності зв'язуватися логічно та обмінюватися або обробляти дані).

Шар кіберперсон *(cyber-persona layer)* – складається із мережі або ІТ аккаунтів користувачів, як реальних людських, так і автоматичних, та їхніх взаємозв'язків між собою.

Модель рівнів кіберпростору показана на рис. 1.9.

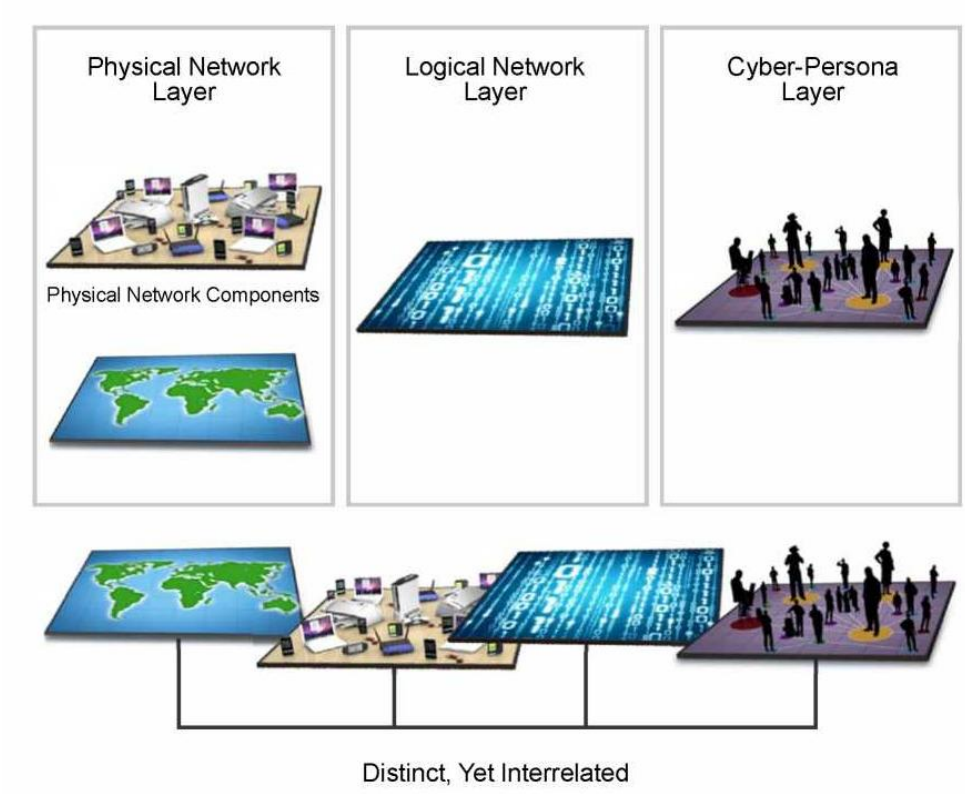

Рис. 1.9. Модель рівнів кіберпростору

У законодавстві України [39] визначено, що ***кіберпростір*** – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

За поглядами окремих військових фахівців США, домінування у кіберпросторі повинно виходити за рамки телекомунікаційних та інформаційних технологій і потребує переваги в усіх його складових: соціальній, технічній, телекомунікаційній, інформаційній, мережнокомп'ютерній тощо та по всьому електромагнітному спектру – "від постійного струму до денного світла, включаючи радіохвилі, інфрачервоне і рентгенівське випромінювання, спрямовану енергію, а також області, про які ще не почали навіть замислюватись, для забезпечення глобального командування й управління, глобального доступу і глобальної могутності" [34]. Тому, складовими кіберпростору слід вважати: частину інформаційного простору, яка безпосередньо пов'язана з кіберпростором, комунікаційний простір, віртуальний комп'ютерно-мережний простір та соціотехнічний простір.

На думку дослідницької організації RAND (США), яка була опублікована у науковій праці "Information Warfare Boundaries for an Army in a Wireless World" [38], кіберпростір представлений у поєднанні соціальних мереж та інформаційно-телекомунікаційних систем, (рис. 1.10.).

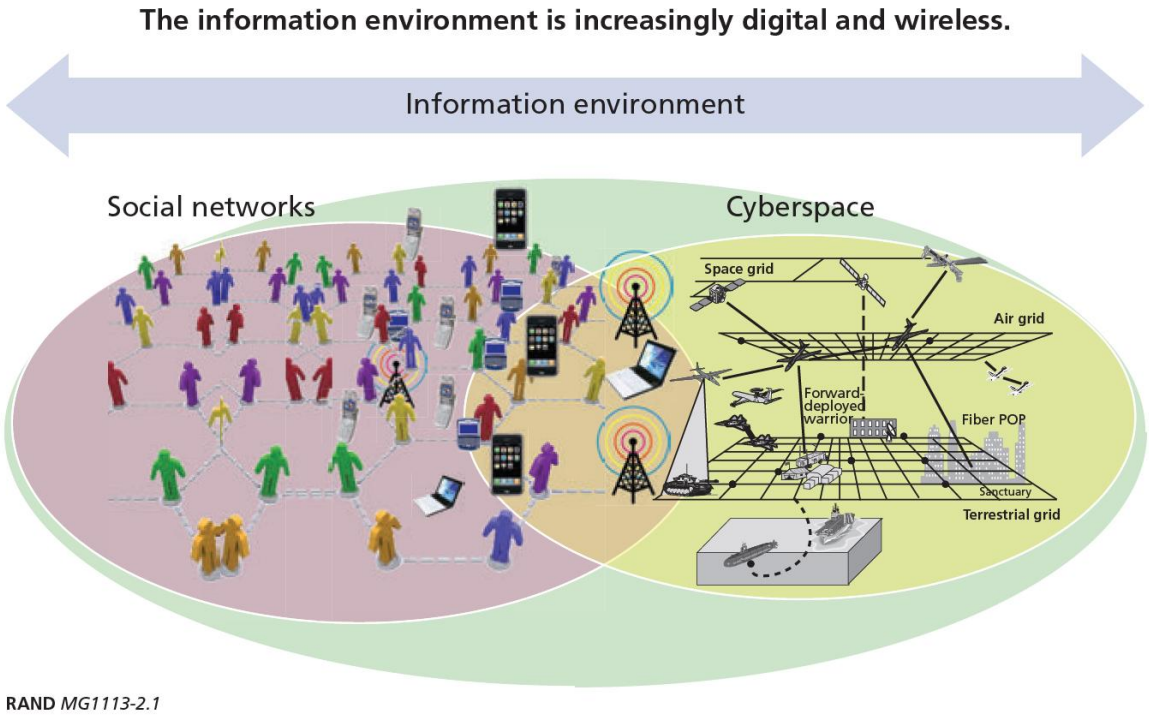

Рис. 1.10. Кіберпростір та соціальні мережі в інформаційному середовищі

Складні соціотехнічні системи, або ергатичні – це системи, складовою яких є людина, знання, уміння, настрої, ціннісні переваги й ставлення до виконуваних обов'язків якої у взаємодії з технічним пристроєм у процесі, наприклад, виробництва матеріальних цінностей, управління певними процесами, обробки інформації тощо сприяють підвищенню ефективності розв'язання відповідних завдань або поліпшенню їх результативності [40].

На цей час кіберпростір розглядають як поєднання соціуму, який формує соціальну складову кіберпростору, та сукупність технічних і програмних засобів, які є технологічною основою формування технічної складової кіберпростору та їх перетин і об'єднання соціотехнічної системи, який формує уявлення про його соціотехнічну природу.

До появи діючого штучного інтелекту людина є невід'ємною складовою феномену кіберпростору, яка є учасником усіх процесів, формує кіберпростір та підтримує його існування, функціонування та розвиток. Він може стати самоорганізуючим та самокерованим лише за наявності штучного інтелекту. Люди в кіберпросторі представлені у їх діяльності, у взаємодії в кіберпросторі та через нього.

Отже, розглядаючи сферу оборони (військовий аспект), визначимо, що ***кіберпростір*** – це єдиний простір сформований з інформаційного, комунікаційного, віртуального комп'ютерно-мережного і соціотехнічного просторів та об'єднаний системою зв'язків, в якому відбувається генерування, зберігання, модифікація та передача інформації, управління об'єктами (системами) та зброєю, вплив на об'єкти (системи) протидіючої сторони, захист власних об'єктів (систем) в існуючих фізичних полях та середовищах.

Сучасне суспільство практично повністю залежить від стану безпеки інформаційної інфраструктури. Не лише урядові структури держав, але й злочинні та терористичні організації отримали можливість використання глобальної мережі для досягнення своїх цілей. Через це забезпечення безпеки кібер- та інформаційної інфраструктури об'єктів управління є надважливою умовою забезпечення обороноздатності держави, її економічного та соціального розвитку.

У січні 2018 року в Сенаті США здійснено доповідь [42], в якій відзначено, що з 2014 року Росія невпинно й різноманітно використовує кіберпростір України в якості театру кібердій та полігону для випробовування російської кіберзброї, а кібератаки, як головний інструмент гібридної війни в російській операції в Україні, спрямовані на всі сектори суспільства та економіки, зокрема такі, як медіа, фінанси, транспорт, політика, енергетика і військова справа.

Принаймні у двох випадках, у грудні 2015 року та грудні 2016 року, російські кібератаки були спрямовані на українську систему розподілу електроенергії, знеструмлюючи на тривалий час об'єкти економіки, інфраструктури та оселі. Після нападу на українську енергетичну мережу, американські чиновники Департаменту енергетики, Департаменту внутрішньої безпеки, ФБР і Корпорації Північноамериканської електричної надійності активізували свою діяльність, визнавши необхідність використання такої ситуації для розуміння тактики й практики дій російського уряду, прогнозування типів майбутніх кіберударів та відпрацювання ефективних заходів захисту від них, з одночасним наданням допомоги Україні в побудові оборонних сил. Співпраця з Україною щодо протидії цим загрозам вважається також критично важливим елементом створення кібероборони Сполучених Штатів [42].

Начальник Генерального штабу Збройних Сил Великої Британії генерал сер Нік Картер зазначив, що у цій щоденній війні не задіяні бомбардування чи важка артилерія. Йдеться передовсім про кіберпростір як основне поле битви. На думку британського генерала, Росія використовує нові реалії і нові підходи у веденні бойових дій з сильними західними супротивниками, і союзники з НАТО мають змінювати свій підхід до самої концепції ведення війни за сучасних умов [43].

1.2. Сутність кібербезпеки інформаційного суспільства

1.2.1. Кібербезпека як складова міжнародної, регіональної та національної безпеки

Інтегральний ефект, обумовлений новими досягненнями в галузі науки і техніки, поступово набуває глобальних рис та досить динамічно змінює облік цивілізації. Такі зміни не можуть не торкатися і поняття "безпека", яке включає у себе все більш вагоме та змістовне наповнення. В Законі України "Про

національну безпеку України” [43] дається визначення щодо **національної безпеки України** – захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз.

Поступовий перехід у розвитку людської формації “інформаційного суспільства” до “високотехнологічного суспільства” обумовлює еволюцію підходів до забезпечення безпеки у нових умовах на різних рівнях. Відбувається поступова трансформація концепції інформаційної безпеки громадянина, суспільства, держави до необхідності її доповнення новою концепцією – кібербезпека.

Виходячи з дефініції “кібернетична безпека”, єдиною й об’єднуючою ознакою в усі епохи розвитку людської цивілізації, яка однозначно характеризує явища та факти пов’язані з проблематикою її забезпечення, є безумовно ознака, яка визначає наявність систем та процесів управління. Виокремлення кібербезпеки в окремий вид безпеки сталося порівняно недавно. Вперше у світі в 1996 р. у військовій доктрині США “Concept Force XXI” на законодавчому рівні визнано необхідність захисту кіберпростору.

З урахуванням того, що проблема кібербезпеки носить глобальний характер, важливою є позиція міжнародних організацій. Так, Міжнародний союз електрозв’язку (ITU) [35, 41] визначає, що **кібербезпека** – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування і технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача. Загальні завдання безпеки у кіберсередовищі включають забезпечення ***доступності, цілісності, конфіденційності*** інформації. Глобальна програма [60] включає п’ять стратегічних напрямів та сім стратегічних цілей, що їх слід враховувати при створенні системи кібероборони, причому вимога щодо уніфікації глобального законодавства у сфері кібербезпеки розглядається як головна стратегічна ціль.

За поглядами американських військових фахівців [58] до цього часу **кібербезпека США** розглядалася як комплекс заходів, спрямованих на захист комп'ютерів, електронних даних і мереж їх передачі від несанкціонованого доступу (конфіденційність), та інших дій, пов'язаних з маніпулюванням або крадіжкою, блокуванням (доступність), псуванням (спотворення), руйнуванням і знищенням (цілісність) умисного і випадкового характеру. Згідно зі Словником, [37] виданого у січні 2019 року **кібербезпека** (безпека кіберпростору) – це дії, вжиті в захищеному кіберпросторі для запобігання несанкціонованому доступу, експлуатації або пошкодженню комп'ютерів, електронних систем зв'язку та інших інформаційних технологій, включаючи інформаційні технології платформи, а також інформацію, що міститься в ній, для забезпечення її ***доступності, цілісності***, аутентифікації, ***конфіденційності*** і неспростовності. Зазначений приклад наданий з метою підтвердження зміни базового термінологічного апарату МО США в сфері

кібербезпеки на 25-30%, що свідчить про гнучкість термінологічної системи сфери кібербезпеки США. Українське ж законодавство [41] комплекс цих заходів однозначно визначає як - технічний захист інформації (ТЗІ).

В Україні термін “кібербезпека” вперше використано у 2007 році [40], але лише в контексті необхідності “розробки та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність”. З 2016 року кібербезпека України визначається як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. Відповідно до Закону України [39], **кібербезпека** – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

При цьому має місце процес розмежування різних видів безпеки за геополітичними рівнями та усвідомлення ролі кібербезпеки на кожному з них. Необхідність такого усвідомлення ролі кібербезпеки покликана, в першу чергу, активізацією міжнародних терористичних, екстремістських організацій та злочинних угруповань, окремих держав, які здійснюють кібервпливи на громадян, суспільство, держави з метою реалізації своїх інтересів. Тому, забезпечення кібербезпеки на міжнародному, регіональному та національному рівнях є однією з найважливіших складових системи забезпечення національної безпеки для будь-якої держави.

На сьогодні загальноприйняте таке розмежування рівнів безпеки держави: міжнародний, регіональний та національний. На кожному з них через зазначені вище об’єктивні та суб’єктивні причини виокремлюється й кібербезпека. Характеристику визначених рівнів надано у табл. 1.1.

Трансформація суспільства та глобалізація світових процесів фундаментально впливає на всі геополітичні рівні безпеки – міжнародний, регіональний та національний. Після першого прообразу кібервійни, яка відбулася в Естонії у квітні 2007 р., провідні країни світу в системі безпеки суттєвого значення стали надавати кіберкомпоненті.

За допомогою такої компоненти “невідомий і невидимий противник” у будь-який час з будь-якої точки світу має можливість здійснення кібервпливів через кіберпростір на фізичне, матеріальне та ідеологічне становище будь-якої країни або групи країн. Тому, усвідомлення ролі і місця кібербезпеки та реальності кіберзагроз для безпеки на усіх рівнях поступово відбувається у більшості країн світу.

Таблиця 1.1

Геополітичні рівні безпеки держави

№ з/п	Геополітичний Рівень	Зміст поняття “безпека”
1	Міжнародний	Стан міжнародних відносин, який забезпечує нормальну життєдіяльність світового співтовариства, стабільний розвиток і співробітництво народів, держав, міждержавних об'єднань, захищеність життєво-важливих інтересів кожного з них від загроз, що виникають. Формується на основі національної те регіональної безпеки. Складовими міжнародної безпеки виступають економічна, політична, екологічна, військова, інформаційна, кібер- та інші види безпеки. Міжнародна безпека передбачає забезпечення: − прав кожної людини на існування і стійкий розвиток; − суверенітету і територіальної цілісності держави; − незалежності та самобутності розвитку країн і народів; − збереження навколишнього середовища і раціонального використання природних ресурсів; − свободи переміщення людей, капіталів, інформації; − повноправності й рівноправності громадян та ін. Запорукою міцності міжнародної безпеки залишаються принципи активізації всіх форм міжнародного співробітництва, дотримання всіма державами загальновизнаних принципів і норм міжнародного права згідно зі Статутами ООН тощо.
2	Регіональний	Стан відносин між соціально-територіальними спільнотами даного регіону, в якому для всіх держав, народів, громадян, суспільств, інститутів і груп забезпечуються захищеність їх життєво важливих інтересів, надійне існування та стабільний розвиток. Рівні регіональної безпеки: − окрема адміністративно-територіальна одиниця країни; − група країн, що входять до певної географічної зони. На будь-якому рівні будується відповідно до національної і міжнародної безпеки та включає такі основні види безпеки: політичну, економічну, екологічну, інформаційну, кібер- та інші види безпеки. До сфери регіональної безпеки входить: − регулювання суперечок, попередження конфліктів між членами регіону; − організація колективних заходів з метою припинення актів агресії й усунення загроз безпеці: превентивна дипломатія, підтримка, встановлення та зміцнення зв’язків у постконфліктний період. Регіональна безпека формується, як правило, через угоди, з сукупності яких утворюється регіональна система безпеки.
3	Національний	Стан суспільства, відносин, гарантована захищеність життєво важливих інтересів особистості, суспільства та держави від зовнішніх та внутрішніх загроз. Основними об’єктами національної безпеки є: − особистість з її правами та свободами; − соціальні та національні групи, їх внутрішня цілісність, самоврядування, матеріальні та духовні цінності; − держава, її конституційний лад, суверенітет та територіальна цілісність. Види національної безпеки виокремлюються залежно від сфери потенційних загроз безпеці. Основними її видами є: економічна, політична, екологічна, інформаційна, воєнна тощо. Особливо виокремлюється кібербезпека, яка має безпосередній вплив на кожен з видів.

На міжнародному рівні кібербезпека є транснаціональною задачею. Вона не може забезпечуватися однією державою або групою держав. Це задача усіх цивілізованих країн. Тільки сумісні зусилля з питань забезпечення кібербезпеки матимуть інтегральний ефект та сприятимуть підвищенню рівня міжнародної безпеки в кіберсфері, як окремо взятої держави, так і світового співтовариства в цілому. Досягнення такої мети потребує пошуку нових шляхів побудови такої системи міжнародних інститутів, механізмів, заходів і гарантій, які у своїй сукупності мінімізуватимуть ймовірність реалізації кіберзагроз та нейтралізуватимуть їх.

Кібербезпека на міжнародному рівні формується на основі національних стратегій кібербезпеки окремих держав, регіональної (субрегіональної) безпеки груп держав і регіонів світу та інтегрується до рівня глобальної міжнародної кібербезпеки, коли мова йде про кіберзахист і реалізацію загальнолюдських інтересів від загроз планетарного характеру, які за своїми масштабами і наслідками виходять за національні межі держав і здатні впливати на безпеку людства.

Наприклад, явище міжнародного кібертероризму становить реальну загрозу міжнародній, регіональній та національній безпеці. Тому, питання кібербезпеки в глобальному масштабі виходять на перший план і визначають стратегічний напрям розвитку світової економіки, регіональної та міжнародної стабільності, добробуту кожної нації.

Кібербезпека на регіональному рівні визначається в рамках якої-небудь частини країни, її окремих адміністративно-територіальних одиниць, стосовно декількох сусідніх районів, областей тієї або іншої держави, у масштабі групи країн, що входять до певної географічної зони. До особливостей забезпечення кібербезпеки на регіональному рівні належать: її обмеженість певною територією зі своїми неоднаковими природно-географічними, соціально-економічними, культурно-історичними й іншими умовами життєдіяльності;
специфічність інтересів, що склалися саме в даному життєвому середовищі соціально-територіальної спільності людей; зміст і форми прояву суперечностей між цією спільністю і центром, іншими регіонами, світовою спільнотою.

На регіональному рівні кібербезпека реалізується на основі низки принципів, до яких належать: територіальна організація кіберзахисту населення, місця існування та об’єктів з критичною інформаційною інфраструктурою; інтегральний комплексний підхід до створення системи кібербезпеки в регіоні; нероздільність безпеки і стійкого розвитку; безперервність зусиль, включаючи організацію постійного спостереження і контролю за станом захищеності суспільства, природного середовища і потенційно небезпечних об’єктів від цілеспрямованого кібервпливу тощо.

Кібербезпека окремо взятого регіону не може бути достатньою мірою забезпечена поза рамками систем кібербезпеки більш високого рівня. Але слід зазначити, що саме на регіональному рівні закладаються фундаментальні основи кібербезпеки міждержавних утворень, націй і народів, їх стійкого та стабільного розвитку.

Інколи, коли мова йде про кібербезпеку у масштабах кількох географічно близьких країн регіону, кібербезпека регіонального рівня трансформується у кібербезпеку субрегіонального рівня.

1.2.2. Кіберінциденти: передумови скоєння та наслідки

Еволюція кібератак, яка спостерігається за останні кілька років, показує, що докорінно змінюються не тільки суб'єкти та об'єкти кібервпливу, а змінюються й їх цілі та мета – від примітивних кібератак на компанію конкурента, до міждержавного протистояння у кіберпросторі. Кардинальні зміни, що обумовлені найбільш відомими інцидентами останніх років у кіберпросторі та навколо нього, ставлять перед воєнним та політичним керівництвом провідних країн світу нетривіальні задачі, ефективність знаходження розв'язання яких визначатиме найближчі перспективи розвитку людської цивілізації. Кіберпростір та пов'язані з ним нові виклики та загрози, що спричинили виникненню нової сфери протиборства з метою вироблення єдиної стратегії протидії, потребують ґрунтовного аналізу найвідоміших кіберінцидентів, що мали місце за останні роки. Серед таких кіберінцидентів, які позначилися на розвитку порядку денного подій в усьому світі, за оцінками фахівців, стали ті, що відбулися в Естонії у травні 2007 р., в Грузії у серпні 2008 р., в Ірані в липні 2010 р., у Франції в грудні 2010 р., у М'янмі (Бірмі) в 2010 р., у Бельгії в березні 2011 р., на Близькому Сході в 2012 р., в Україні у 2014 та 2017 р. Але перед тим, як дослідити передумови скоєння даних кіберінцидентів та наслідків, до яких вони призвели, доцільно встановити початок ери кіберінцидентів в комп'ютерних мережах.

Кібератаки проти Естонії (2007) – перші відомі масовані кібератаки спрямовані проти національної безпеки країни. Кібератаки відбувались в декілька хвиль на тлі розхитування російськими спецслужбами суспільно-політичної ситуації в країні під приводом "протестів" "проти" перенесення пам'ятника "Бронзовий солдат" у Таллінні. Пік атак припав на 9 травня 2007 року. Зловмисникам вдалось вчинити "дефейс" деяких сайтів, урядові та банківські сервери і служби були виведені з ладу внаслідок масованих атак на відмову в обслуговуванні.

Скоординовані кібератаки на комп'ютерні системи державних установ Естонії почалися 27 квітня 2007 року під час загострення російсько-естонських відносин, пов'язаних з перенесенням пам'ятника Бронзовому солдату у Таллінні. Скоординована атака хакерів вивела на деякий час з ладу сайти парламенту Естонії, міністерств, банківських установ, засобів масової інформації. На думку деяких оглядачів, кібератака на Естонію належала до одних з найкраще організованих та масових в історії Інтернету.

Події розгортались у три хвилі: перші атаки були зареєстровані 28 квітня, наступна, потужніша хвиля була зареєстрована 4 травня, найпотужніша, третя хвиля була зареєстрована 9 травня 2007 року. Інтернет-трафік із закордону зріс вчетверо, що зробило недоступними атаковані сайти. Через атаки до 90%

банківських транзакцій в Естонії зазнали проблем в обробці або не змогли бути завершені в нормальному режимі. На піку, створений зловмисниками трафік сягав 100 Мб/с. Для здійснення атак були використані ресурси мережі Storm. Дещо згодом, коли відбувались процеси над учасниками заколотів квітня 2007 року, боти BlackEnergy були використані для атаки на сайт видання delfi.ee.

З початку естонська сторона звинуватила РФ в організації кібератак, однак пізніше міністр оборони країни спростував ці звинувачення за відсутності доказів. Однак, пізніше того ж року, депутат Державної думи Росії Сергій Марков на прес-конференції визнав, що один з його помічників був причетним до організації кібератак. У 2007 році лідер руху "Наші" у Придністров'ї Костянтин Голоскоков визнав причетність цієї організації до атак проти Естонії. У відповідь Естонія проголосила Сергія Маркова і лідера руху "Наші" Василя Якименка персонами "нон ґрата". Оскільки Придністров'я залишається невизнаним жодною країною світу, не існувало можливості притягнути до відповідальності організаторів кібератак з цього регіону.

Кібератаки проти Грузії (2008), які відбувались спільно зі збройною агресією Російської Федерації проти країни. Умовно кібератаки поділені на дві хвилі. Перша хвиля розпочалась 7 серпня 2008 року – за день до початку гарячої фази збройної агресії проти Грузії. Перевага була віддана DDoS-атакам (атакам типу відмови в обслуговуванні) на урядові веб-сайти та засоби масової інформації. Під час другої хвилі вже відбувались дефейси різних сайтів, а також DoS-атаки проти ширшого кола сайтів (великих приватних підприємств тощо).

Кібератака проти Ірану (2010). Кіберінцидент в Ірані з мережним хробаком "Stuxnet" заслуговує на особливу увагу. Різні дослідження висувають різні версії щодо цільового призначення "Stuxnet", але щодо передумов виникнення кіберінциденту та наслідків від його реалізації точка зору більшості експертів збігається.

Технічна складність зі створення мережного хробака "Stuxnet" вимагає значних ресурсів, надати під силу які у повному масштабі здатен тільки уряд або декілька зацікавлених урядів розвинених держав. Об'єктом кібернападу даного шкідливого програмного забезпечення є іранські ядерні об'єкти (системи контролю та збору даних (SCADA)), які було виготовлено компанією "Siemens". Якщо звернути увагу на активізацію діяльності США в кіберпросторі (у 2009 році створено Кіберкомандування США) та врахувати політичну ситуацію на Близькому Сході (бажання Ізраїлю призупинити ядерну загрозу, що надходить від Ірану), то відповідь на питання щодо розробника та замовника даного кіберінциденту є очевидною. Про це свідчать такі факти. По-перше, США є однією з найбільш розвинених держав світу, а відповідно вона й найбільш залежить від якісного функціонування кібернетичних систем різного цільового призначення у різних сферах. По-друге, США здійснює послідовну внутрішню політику щодо створення та нарощування потужності власного Кіберкомандування. Виконання завдань за призначенням таким органом воєнного управління неможливе без розроблення спеціалізованих засобів

кібервпливу та кіберзахисту. По-третє, програма під кодовою назвою “Олімпійські ігри ” розроблена в адміністрації попереднього Президента США Д. Буша та підтримана й нарощена адміністрацією Президента Б. Обами передбачає нарощення кількості та технологічної складності кібератак проти Ірану.

Як наслідок, у кінці вересня 2010 року урядом Ірану офіційно визнано, що у програмному забезпеченні системи управління Бушерської атомної електростанції (АЕС) виявлено серйозні збої, які тривали протягом двох діб. У результаті розслідування спеціалістами було встановлено, що шкідливе програмне забезпечення знищило не лише деякі спеціальні дані й пошкодило програмні коди, а й призвело до виникнення передумов для виходу з ладу реального обладнання цього дуже важливого для економіки Ірану енергетичного об’єкта. Наслідки даного кіберінциденту мали суттєвий інформаційно-психологічний вплив на уряди інших держав, у яких розвиваються ядерні програми. Таким чином, світові, на прикладі Ірану, вперше без застосування військової сили та інших засобів врегулювання міжнародних політичних неузгодженостей було продемонстровано уразливість окремої промислової галузі від прихованих кібервпливів.

Кібератаки проти України (2013 - по теперішній час)

На особливу увагу заслуговує низка кіберінцидентів, що почалися в Україні з 2013 року. Перші атаки на інформаційні системи приватних підприємств та державні установи України фіксували ще під час масових протестів у 2013 році. Російсько-український конфлікт став першим конфліктом в кіберпросторі, коли була здійснена успішна атака на енергосистему з виведенням її з ладу. Мали місце атаки проти інформаційної системи “Вибори” під час виборів Президента, численні атаки на відмову обслуговування, дефейси, кібершпигунство тощо.

У лютому 2014 року розпочалась російська збройна агресія проти України, яка велась також і в кіберпросторі. Майбутній директор американського Агентства національної безпеки Майкл Роджерс з цього приводу зазначає, що разом з військовою операцією із захоплення Криму, Росія розпочала проти України кібервійну.

Кіберзагрози Українській державі та суспільству умовно можна поділити на два ключових рівні. Перший – “класичні” кіберзлочини – як абсолютно оригінальні, так і звичайні, для своєї реалізації вони потребують лише сучасних інформаційних технологій.

Другий – злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм, кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодіння коштами громадян, так і з метою кібершпигунства.

Першим масованим випадком хактивізму, з яким зіткнулася Україна, були події довкола закриття файлообмінного сервісу ex.ua. Після спроб

правоохоронних органів втрутитися в роботу файлообмінного сервісу було здійснено DDoS-атаки на понад 10 інтернет-сайтів органів державної влади, зокрема, на сайт Президента України та сайт Міністерства внутрішніх справ України. Події довкола ex.ua вперше наочно продемонстрували, наскільки Українська держава не готова ані ідеологічно, ані технічно до подібних атак. Саме відсутність прямих економічних збитків стала причиною того, що реальних висновків тих подій так і не було зроблено, а країна виявилась непідготовленою до ефективного протистояння агресії Російської Федерації в кіберпросторі.

Наступна хвиля хактивізму сталася на тлі політичного протистояння у жовтні 2013 року – лютому 2014 року (події Євромайдану). Це протистояння активно відбувалось у соціальних мережах, де спостерігався значний сплеск зацікавленості проблемою. З першого дня Євромайдану невідомі особи почали масово використовувати нетботи з метою засмічення інформаційного поля, введення людей в оману та поширення чуток. Наприклад, у Twitter, де можна відслідковувати всі події за хештегом #євромайдан, десятки нетботів вкидали різноманітне інфосміття.

Також були використані механізми ускладнення традиційних комунікацій, зокрема мобільного зв'язку (через автоматичні дзвінки на телефони певних активістів чи політиків, що унеможливило використання їхніх мобільних телефонів у роботі).

Після початку збройної агресії Російської Федерації проти України, компанії, що спеціалізуються на наданні послуг кібербезпеки, стали реєструвати зростання кількості кібератак на інформаційні системи в країні. Зазвичай, кібератаки були спрямовані на приховане викрадення важливої інформації, ймовірніше для надання Росії стратегічної переваги на полі бою. Жертвами російських кібератак ставали урядові установи України, країн ЄС, Сполучених Штатів, оборонні відомства, міжнародні та регіональні оборонні та політичні організації, аналітичні центри, засоби масової інформації, дисиденти.

З початком російсько-української війни стали з'являтись загони антиукраїнських хактивістів, які йменують себе “Кіберберкутом” та проукраїнська “Кіберсотня Майдану”, “Анонімусами” з російською або українською “пропискою” тощо. Попри складності у визначенні ступеня співпраці хакерських угруповань з державними органами, спираючись на зібрані докази можна стверджувати, що проросійські хакерські угруповання перебувають на території Росії, і що їхня діяльність відбувається на користь кремлівського режиму.

Можна стверджувати, що з початку Російсько-української війни в середовищі дослідників кібербезпеки поліпшились можливості виявлення, відстеження та захисту від угруповань російських хакерів. Серед можливих пояснень можна навести те, що із загостренням протистояння російським хакерам бракує часу на вчасне оновлення та вдосконалення тактики, технологій та методів діяльності.

Дослідники компанії FireEye виокремили два угруповання російських хакерів, які активно проявили себе у Російсько-українській кібервійні: так звана APT29 (також відома як Cozy Bear, Cozy Duke) та APT28 (також відома як Sofacy Group, Tsar Team, Pawn Storm, Fancy Bear).

В період між 2013 та 2014 роками деякі інформаційні системи урядових установ України були уражені комп'ютерним вірусом, відомим як Snake/Uroborus/Turla. Даний різновид шкідливого програмного забезпечення надзвичайно складний, стійкий до контрзаходів та ймовірно створений в 2005 р. Починаючи з 2013 розпочалась "операція Армагедон" – російська кампанія систематичного кібершпигунства за інформаційними системами урядових установ, правоохоронних та оборонних структур. Здобута в такий спосіб інформація ймовірно могла сприяти Росії й на полі бою. Істотним відхиленням від цього правила стала кібердиверсія – атака на "Прикарпаттяобленерго".

Операція "Змія"

Дослідники британської фірми BAE Systems Applied Intelligence зафіксували в 2013—2014 роках сплеск виявлених випадків зараження інформаційних систем приватних підприємств та державних установ України комп'ютерним хробаком (з руткітом), який вони назвали "Змія" (англ. snake). Дослідники з німецької фірми GData назвали цього хробака "уроборос", англ. uroborus (також англ. ouroborus – гадюка в грецькій міфології, або англ. sengoku та англ. snark). На думку дослідників обох фірм, цей хробак можливо пов'язаний та був створений на основі хробака Agent.BTZ, який у 2008 році уразив інформаційні системи Центрального Командування ЗС США.

Пік виявлення атак із використанням хробака "уроборос" збігся з розвитком масових протестів. Протягом січня 2014 року було зафіксовано 22 випадки інфікування інформаційних систем, при цьому протягом 2013 року "уроборос" був виявлений не більше 8 разів. В Україні зловмисники із застосуванням "уроборос" отримували повний доступ до уражених систем. На думку британських експертів, є всі підстави вважати, що за "уроборос" стоять спецслужби Російської Федерації.

Атака на "Вибори"

21 травня 2014 року зловмисники з угруповання КіберБеркут здійснили успішну кібератаку на інформаційну систему "Вибори" Центральної виборчої комісії України. Їм вдалось вивести з ладу ключові мережеві вузли корпоративної мережі та інші компоненти інформаційної системи ЦВК. Майже 20 годин поспіль програмне забезпечення, яке мало показувати поточні результати підрахунку голосів, не працювало як слід. В день виборів, 25 травня, за 12 хвилин до закриття виборчих дільниць (19:48 EET), зловмисники розмістили "картинку Яроша" на серверах ЦВК.

Увечері 25 травня фахівцями CERT-UA було отримано інформацію про те, що на російських телеканалах анонсували новину про нібито виграш Дмитра Яроша на "президентських перегонах". З метою підтвердження цієї інформації на російському ТБ було продемонстровано картинку, яку в мережі вже назвали як "Картинка Яроша". 25 травня, о 20:16:56 було зафіксоване перше звернення

до веб-сайта ЦВК виключно за IP-адресою внутрішнього веб-сервера з вказівкою у GET-запиті повного шляху до картинки “result.jpg” з IP-адреси 195.230.85.129. Ця адреса входить до діапазону IP-адрес телеканалу ОРТ.

В результаті атаки “Перший канал” російського телебачення повідомив своїм глядачам про те, що найбільшу кількість голосів виборців в першому турі на виборах Президента України набрав лідер “Правого сектора” Дмитро Ярош. Про це йшлося у випуску вечірніх новин, присвяченому позачерговим виборам Президента України. Ведуча повідомила, що незважаючи на дані екзит-полів, які свідчать про перемогу Петра Порошенка в першому турі, на сайті ЦВК з'явилася “дивна картинка” (так звана “Картинка Яроша”). За їхньою інформацією, Дмитро Ярош набрав 37,13 % голосів виборців, натомість за фаворита Петра Порошенка проголосувало лише 29,63 %.

Рано вранці наступного дня, 26 травня, сервери системи “Вибори”, які приймали та обробляли дані про підрахунок голосів, зазнали розподіленої DoS-атаки, та були недоступні в проміжку між 1-3 годинами ранку.

Окрім інформаційної системи ЦВК, кібератак зазнали інші організації, які мали дуже віддалений зв'язок до виборів, жертвою міг стати сайт, який містив сторінку зі словом “вибори”. Однак більшість атак проти таких сайтів відрізнялись низьким рівнем технічної реалізації. Натомість, атака проти ЦВК відрізнялась високою складністю та технологічністю. За словами Миколи Коваля, тогочасного голови CERT-UA, атака на інформаційну систему ЦВК стала однією з найскладніших кібератак, які йому тоді довелось розслідувати.

І хоча відповідальність за атаки взяло на себе угруповання начебто хактивістів КіберБеркут, Микола Коваль припускає, що значна складність атаки може свідчити про те, що за нею стояли підрозділи іншої держави. Також, у мережі ЦВК було виявлене шкідливе програмне забезпечення, яке пов'язують з угрупованням APT28/Sofacy Group.

Опитані американською газетою Christian Science Monitor фахівці з комп'ютерної безпеки назвали атаку на інформаційною систему “Вибори” надзвичайно небезпечною, а також попередженням на майбутнє про уразливість комп'ютерних систем, залучених у виборчий процес. Можливість зриву виборів, або маніпуляція результатами виборів, набула нової ваги під час виборів Президента США 2016 року після успішної кібератаки проти Демократичної партії.

Атака на “Прикарпаттяобленерго”

23 грудня 2015 року сталась перша у світі підтверджена атака, спрямована на виведення з ладу енергосистеми: російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління в диспетчерській “Прикарпаттяобленерго”, було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy.

Водночас синхронних атак зазнали “Чернівціобленерго” та “Київобленерго”, але з меншими наслідками. За інформацією одного з обленерго, підключення зловмисників до його інформаційних мереж

відбувалося з підмереж глобальної мережі Internet, що належать провайдерам в Російській Федерації.

Загалом кібератака мала комплексний характер та складалась щонайменше з таких складових:

− попереднє зараження мереж за допомогою підроблених листів електронної пошти з використанням методів соціальної інженерії;

− захоплення управління АСДУ з виконанням операцій вимикань на підстанціях;

− виведення з ладу елементів IT інфраструктури (джерела безперебійного живлення, модеми, RTU, комутатори);

− знищення інформації на серверах та робочих станціях (утилітою KillDisk);

− атака на телефонні номери кол-центрів, з метою відмови в обслуговуванні знеструмлених абонентів.

Масштабна хакерська атака, що відбувалась у декілька етапів, розпочалась щонайменше 14 квітня 2017 року з компрометації системи оновлення програми M.E.Doc. Останній етап, з використанням різновиду вірусу Petya, відбувся 27 червня 2017 року, та спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Внаслідок атаки була заблокована діяльність таких підприємств, як аеропорт "Бориспіль", ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низка інших великих підприємств.

Жертвою вірусу також стали телеканал "Інтер", медіахолдинг ТРК "Люкс", до складу якого входять "24 канал", "Радіо Люкс FM", "Радіо Максимум", різні інтернет-видання, а також сайти Львівської міської ради, Київської міської державної адміністрації. Трансляції передач припинили канали "Перший автомобільний" та ТРК "Київ".

28 червня 2017 року Кабінет Міністрів України повідомив, що атака на корпоративні мережі та мережі органів влади була зупинена.

Масштабна деструктивна атака різновидом вірусу Petya (також відомого як NotPetya, Eternal Petya, Petna, ExPetr тощо) стала можливою завдяки компрометації системи оновлення програми M.E.Doc та встановлення прихованого бекдору. Таким чином, масштабною деструктивною атакою зловмисники закрили собі наявний в них завдяки бекдору доступ до комп'ютерів та комп'ютерних мереж у близько 80% українських підприємств (в тому числі – представництв закордонних компаній). Є підстави вважати, що зловмисники пішли на такий крок оскільки або здобули надійніший доступ до інформаційних систем важливих для них жертв, або ж вважають, що зможуть доволі просто відновити його.

В цих умовах, забезпечення кібербезпеки стає нагальною проблемою не тільки для кожної окремої країни, але й в міжнародному масштабі. Сьогодні у світі діє величезна кількість різних міжнародних програм співробітництва, які тою або іншою мірою стосуються забезпечення кібербезпеки. Їхніми відправними точками стали відповідні міждержавні угоди, конвенції, інші документи ООН та ЄС.

1.3. Загрози у сфері кібербезпеки

1.3.1. Зміст, класифікація та ознаки кіберзагроз

Події, які відбулися в квітні-травні 2007 року в Естонії наочно продемонстрували всьому цивілізованому світові уразливість окремо взятої держави від нового класу загроз для національної безпеки. Характер прояву таких загроз значною мірою був обумовлений абсолютною залежністю практично усіх систем державного управління та приватного сектору Естонії, у тому числі банківських структур, закладів торгівлі, засобів масової інформації тощо від інфокомунікаційних та інших електронних засобів та програмних продуктів. Різноманітні прояви загроз їх правильному функціонуванню набули нової форми й отримали у сфері національної безпеки назву «кіберзагроз».

Зважаючи на провідну роль та місце інфокомунікацій та різноманітних електронних засобів і програмних продуктів у житті сучасного високотехнологічного суспільства будь-якої розвиненої держави, прийняття практично в усіх країнах курсу на інформатизацію та інтенсифікацію процесів впровадження ІТ-інновацій в усі без виключення сфери життя, очевидним залишається факт того, що кіберзагрози та їх прояви матимуть місце і в майбутньому. Саме тому, при побудові ефективної системи кібербезпеки важливо знати перелік тих загроз, яким вона повинна протистояти. При цьому, процес виявлення кіберзагроз вимагає глибокого аналізу їх сутності з подальшою систематизацією набутих знань. Якщо враховувати ще й те, що кіберзагрози можуть мати найрізноманітніший характер – від підліткового вандалізму до цілком спланованих державних кібероперацій, визріває нагальна потреба у чіткому розмежуванні таких загроз за різними класифікаційними ознаками. У такому разі основну увагу слід акумулювати на тому, що спектр кіберзагроз породжений феноменом кіберпростору є досить обмеженим, а множина їх проявів залишається практично безмежною. Отже, упорядкування можливих кіберзагроз за певними класифікаційними ознаками дозволить забезпечити необхідний рівень достовірності їх ідентифікації та створить передумови для організації ефективної протидії їх проявам.

Відомі підходи до класифікації кіберзагроз в основному зорієнтовані на їх розгляд у площині інформаційних загроз, загроз безпеці інформації, загроз розподіленим системам обробки даних тощо. Тобто основний акцент у таких класифікаціях розставлено на інформаційній складовій загрози, а не на кібернетичній. Ситуація, що склалася обумовлена відсутністю єдиного розуміння сутності дефініції кіберзагрози.

Відповідно до Закону України “Про основні засади забезпечення кібербезпеки України” це визначення має наступне тлумачення.

Кіберзагроза – наявні та потенційно можливі явища і фактори, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів.

На даний час цією проблематикою займається багато вчених, як в нашій державі, так і за її межами. Наступне визначення більш повно описує це явище, з наукової точки зору.

Кіберзагроза – фактори (події, явища), які мають місце або можуть виникнути в інформаційній, комунікаційній, комп'ютерно-мережній та соціотехнічній складових кіберпростору (або їх комбінації у певному поєднанні), за умови умисного цілеспрямованого або випадкового впливів та створити небезпеку порушення процесів управління і передачі інформації, що відбуваються у кібернетичних системах різних сфер (соціальної, технічної, соціотехнічної), або можуть зашкодити елементам таких систем.

Під ***кібернитичною системою*** (cybernetic system) (за редакцією Глушкова В.М.) будемо розуміти множину взаємопов'язаних об'єктів, які є елементами системи, що здатні сприймати, запам'ятовувати та переопрацьовувати інформацію, а також здійснювати її обмін.

Виходячи зі сформульованого визначення обов'язковими ознаками будь-якої кіберзагрози є:

− об'єкт, щодо якого може бути реалізована загроза, – носій або виразник того чи іншого інтересу, який підлягає захисту;

− суб'єкт або носій загрози, – іноземна держава, вітчизняні й іноземні організації, групи осіб, самоорганізовані технічні системи тощо, дії (функціонування) яких можуть негативно вплинути на реалізацію інтересів об'єкта у будь-якій сфері;

− методи та способи реалізації загроз – дія чи послідовність узгоджених дій, яка може завдати шкоди інтересам об'єкта, що підлягають захисту;

− причини виникнення кіберзагроз – комплексна ознака, що поєднує у собі наявність відповідних можливостей і намірів суб'єкта загрози та уразливостей об'єктів захисту;

− можливі наслідки або негативні результати, до яких може призвести реалізація загрози – негативні зміни або відсутність позитивних змін у стані об'єкта захисту, що відповідають меті та поставленим цілям суб'єкта загрози.

Впорядкування наданих ознак дозволяє подати їх узагальненою схемою вигляду рис. 1.11.

Таким чином, будь-якій кіберзагрозі можуть бути поставлені у відповідність притаманні їй ознаки, за якими її можна ідентифікувати, а виявлення сукупності таких ознак або певної їх частини, забезпечить виявлення образу тієї чи іншої загрози та дозволить сформулювати судження про її зміст.

Виявлення кіберзагрози дозволяє у подальшому оцінити її рівень та сформувати пропозиції щодо відповідних заходів нейтралізації та запобігання (якщо загроза ще не реалізується) чи стримування та протидії (якщо реалізація загрози уже відбувається у формі кібервпливу).

Отже, визначення поняття "кіберзагроза" на основі критичного поєднання існуючих тлумачень, дозволяє формулювати основні загрози у сфері кібербезпеки та виявляти ознаки таких загроз, за якими вони можуть бути виявлені.

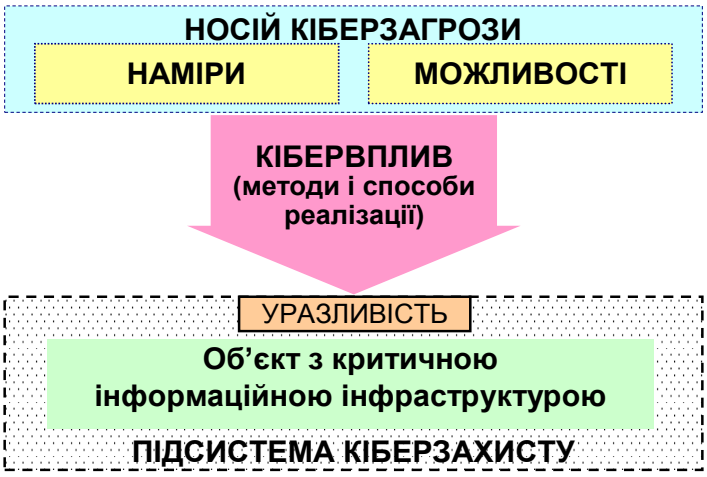

Рис. 1.11. Узагальнена схема ознак кіберзагрози

Відомо, що до складу будь-якої кібернетичної системи входять такі елементи: об'єкт управління, суб'єкт управління та канал передачі даних. Природа усієї системи визначається її призначенням та, зазвичай, є комбінованою. При цьому, природа окремих елементів може бути абсолютно різною: біологічною, технічною або соціальною. Кожен із трьох зазначених вище елементів кібернетичної системи, у свою чергу, може також розглядатися як кібернетична система, але нижчого за ієрархією рівня, але вже така, що складається зі своїх елементів. Особливості процесів управління, які відбуваються у кібернетичній системі, обумовлені специфікою алгоритмів перетворення вхідної дії, яка надходить через рецептори і видозмінюється на виході системи у вихідну дію. Порушення будь-якого з етапів таких алгоритмів може призвести до дезорганізації усього процесу управління та невиконання системою її функцій.

Середовище передавання інформації є однією із найбільш уразливих складових, що забезпечують функціонування кібернетичної системи. Під час передавання інформації вона може перехоплюватися, модифікуватися або взагалі знищуватися. Властивості середовища передачі інформації характеризуються видом фізичного середовища, у якому поширюється інформація, і визначаються при оцінюванні можливості реалізації кіберзагрози тій або іншій системі.

Можливості джерел (суб'єктів) кіберзагрози обумовлені сукупністю способів доступу (проникнення, впливу) до елементів кібернетичної системи, в результаті якого можливе порушення їх функціонування або виведення зі стану нормальної роботи.

Спираючись на подане визначення кіберзагрози та враховуючи особливості функціонування комп'ютерних (інформаційних) систем, була застосована класифікація їх за такими ознаками:

− вид кібернетичної системи (КС), на яку спрямована кіберзагроза;
− елемент КС, на який безпосередньо спрямована реалізація кіберзагроз;
− уразливості (системи та її елементів), що використовуються;

− розташування джерела (суб’єкта) кіберзагроз;
− спосіб реалізації кіберзагроз;
− середовище поширення;
− умисність;
− походження;
− повторюваність появи;
− прихованість прояву;
− масштаби наслідків від реалізації загрози;
− ієрархія управління, що відбувається у КС;
− доцільність реалізації кіберзагроз;
− час появи кіберзагроз;
− умовність реалізації.

Розглянем кожну ознаку більш детально.

За видом КС (її фізичною природою), на яку спрямовані кіберзагрози, розрізняють:
− технічні;
− біологічні;
− соціальні;
− комбіновані.

Слід зазначити, що вид КС, яка підлягає захисту, обмежує не лише діапазон її потенційних загроз, а й значною мірою можливі заходи протидії таким загрозам. Так, наприклад, при розгляді суто технічних КС, можна знехтувати загрози біологічної або соціальної природи, що дозволить скоротити перелік можливих заходів захисту та протидії.

За елементом КС, на який безпосередньо спрямовані (або через який здійснюється) кіберзагрози, можна виділити такі класи загроз:
− загрози об’єкта управління;
− загрози суб’єкта управління;
− загрози каналу передачі даних;
− комплексні загрози.

Класифікація за такою ознакою як елемент КС, на який спрямована загроза, дозволяє підвищити ефективність протидії за рахунок раціонального використання сил та засобів (ресурсів) захисту. Завчасне зосередження ресурсів захисту на певній складовій КС, щодо якої існує загроза, дозволяє забезпечити необхідний рівень захисту всієї системи із найменшими витратами.

За уразливостями (системи та її елементів), що використовуються, мають місце такі загрози:
− загрози, що реалізуються за рахунок уразливостей складових КС;
− загрози, що реалізуються за рахунок використання уразливостей підсистеми захисту КС (за наявності такої підсистеми);
− загрози, що реалізуються із застосуванням недоліків в алгоритмах управління та обробки інформації (сигналів).

Класифікація загроз за уразливістю, що використовується, дозволяє підвищити точність локалізації небезпеки та мінімізувати витрати на

проведення заходів захисту КС.

За розташуванням джерела (суб'єкта) кіберзагроз відносно об'єкта, на який вона спрямована, слід виділяти загрози:

− зовнішні;

− внутрішні.

Об'єкти, з якими взаємодіють КС, що підлягають захисту, виступають джерелом зовнішніх загроз, а складові таких систем – внутрішніх.

Зовнішні кіберзагрози, у свою чергу, поділяються на загрози від середовища функціонування КС та загрози від конкуруючих (протидіючих) систем. До загроз першого підкласу можна віднести стихійні лиха, революції тощо. Прикладом загроз другого підкласу можуть бути загрози протиборчих сторін одна одній у військовому конфлікті.

Клас внутрішніх кіберзагроз розгалужується з урахуванням складу конкретної КС. Наприклад, для сучасних інформаційно-управляючих систем до внутрішніх кіберзагроз можуть належати загрози від носіїв інформації; технічних засобів; програмних засобів; засобів захисту інформації (апаратних, алгоритмічних, програмних); людини-оператора (обслуговуючого персоналу) тощо.

Завчасне визначення джерела загрози дозволяє застосовувати відносно нього активні (превентивні) заходи протидії.

Спосіб реалізації кіберзагроз залежить від конкретного об'єкта та його особливостей (технічних, соціальних, біологічних, психологічних), але в загальному випадку виділяються:

− загрози, що передбачають активне втручання у процес функціонування КС (активні кіберзагрози);

− загрози, що безпосередньо не впливають на роботу КС (пасивні кіберзагрози);

− загрози із комплексним характером впливу.

За середовищем поширення загрози виділяються класи, що відповідають існуючим небезпечним середовищам:

− інформаційному;

− комунікаційному;

− комп'ютерно-мережному;

− соціотехнічному.

Середовище поширення кіберзагроз не в останню чергу визначає форми та способи протидії таким загрозам. Наприклад, недоцільно (хоча й можливо) застосовувати фізичне знищення комунікаційних каналів для захисту від атаки типу "відмова в обслуговуванні", а від завдання превентивного удару по противнику, що готується до збройної агресії, можна вважати ефективним.

За умисністю загрози бувають:

− навмисними;

− ненавмисними.

Навмисні загрози передбачають цілеспрямований намір заподіяння шкоди КС або її елементам. Ненавмисні загрози виникають і реалізуються безвідносно

до волі носія (джерела) загрози.

За походженням можна виділити загрози:

− штучного походження (антропогенні, техногенні);

− природного походження.

Загрози штучного походження є наслідком діяльності людини або функціонування технічних систем. Загрози ж природного походження виникають внаслідок природних процесів, що відбуваються у живій та неживій природі.

За повторюваністю появи виділяються загрози:

− повторювані (періодичні, аперіодичні);

− неповторювані.

Віднесення тієї або іншої загрози до класу повторюваних дозволяє ефективніше протидіяти їй у майбутньому за рахунок формування образу такої загрози та застосування відпрацьованого алгоритму протидії. Неповторювані ж загрози вимагають залучення більш значних ресурсів для їх усунення через необхідність додаткового вивчення та моделювання. Показник повторюваності може бути визначений, наприклад, кількістю випадків появи тієї чи іншої кіберзагрози за деякий проміжок часу.

За прихованістю прояву виділяються:

− приховані;

− неприховані.

Рівень прихованості загроз визначає складність алгоритмів їх ідентифікації, що неодмінно позначається на тривалості виявлення загроз та врешті-решт визначає принципову можливість такого виявлення за допустимий час.

Реалізація однієї із кіберзагроз наведених класів або їх сукупності може призвести до *наслідків різного масштабу* для КС або її елементів. Відповідно й кіберзагрози можна поділити на:

− локальні;

− частковосистемні;

− загальносистемні.

Локальні загрози характеризуються несуттєвим ускладненням роботи окремого елемента КС, що не позначається на функціонуванні КС у цілому.

Загрози частковосистемного характеру призводять до порушення роботи кількох елементів або сегмента КС, що здатне негативно позначитися на виконанні КС частини своїх функції або призначення в цілому з можливістю відновлення ураженого сегмента.

Загальносистемні загрози спрямований на ураження кількох сегментів системи або ключових її елементів, що неодмінно призводить до відмови функціонування КС у цілому без можливості відновлення її роботи.

За ієрархією управління, що відбувається у КС, виділяються кіберзагрози:

− вищого (стратегічного) рівня;

− середнього (оперативного) рівня;

− нижчого (тактичного) рівня.

На вищому (стратегічному) рівні управління приймаються та реалізуються найбільш важливі рішення для КС у цілому. Очевидно, що загрози цього рівня найбільш небезпечні для функціонування КС.

Проміжний (оперативний) рівень забезпечує управління ходом окремих операцій (оперативне управління), а тому є не просто буфером між вищою та нижчою ланками управління, а відіграє вкрай важливу роль у виконанні КС свого призначення. Порушення управління у проміжній ланці здатне призвести до дезорганізації КС, а тому загрози на проміжному рівні управління також становлять небезпеку.

Нижча (тактична) ланка управління, як правило, найбільш чисельна (що дозволяє застосовувати в управлінні дублювання та резервування), тому загрози на цьому рівні не становлять значної небезпеки, а можуть лише вплинути на реалізацію певної часткової функції КС. Проте одночасна реалізація деякої сукупності кіберзагроз відносно критичних елементів на нижчому рівні управління може призвести до синергетичного ефекту, тому безпекою цієї ланки управління КС також не слід нехтувати.

Прийняття рішення про *доцільність реалізації* КЗ можливо за критерієм “ефективність/вартість”. Тобто, якщо отриманий від реалізації кіберзагроз ефект перевищує витрати на її підготовку і здійснення, є сенс розглядати можливість такої загрози. В іншому випадку реалізація кіберзагроз недоцільна. Відповідно до цього виділимо такі класи кіберзагроз:

− гіпотетично можливі, але малоймовірні;

− з високою ймовірністю реалізації.

Важливим фактором, що впливає на ймовірність реалізації тієї чи іншої кіберзагрози, є її залежність від певних подій. Тобто реалізація одних кіберзагроз можлива лише за умови, якщо відбудеться відповідна сприятлива подія (або група подій), а реалізація інших не вимагає виконання такої умови.

Відповідно *за умовністю реалізації* виділимо кіберзагрози:

− умовні;

− безумовні.

За часом появи кіберзагрози виділимо:

− загрози, які закладено при створенні КС;

− загрози, які виникають у процесі функціонування КС.

Недосконалості у структурі та конструкції КС або її окремих елементів є уразливими місцями, які потенційно можуть використовуватися для порушення сталої роботи системи. Такі уразливості закладаються під час створення системи або проявляються у процесі її функціонування (для комп’ютерних систем це “загрози нульового дня”). Виявлення закладених при створенні КС уразливостей дозволяє значно підвищити захист таких систем від кіберзагроз уже на ранніх етапах експлуатації. Уразливості, що проявляються з часом, більш небезпечні, оскільки їх виникнення складно передбачити чи спрогнозувати, а тому протидія загрозам, що використовують такі уразливості, украй складна.

Застосований для класифікації кіберзагроз ознаковий принцип дозволяє

описати будь-яку загрозу множиною якісних та кількісних ознак, які можуть бути використані при моделюванні та подальшій ідентифікації такої загрози.

Надана класифікація кіберзагроз передбачає можливість доповнення та розгалуження на підкласи, що досить зручно при розробці переліку загроз для кожної конкретної КС, залежно від рівня необхідної деталізації.

Розглянемо, наприклад, деяку КС, що належить до класу інформаційно-управляючих систем, які на даний час набули найбільшого поширення. Такі системи складаються із інформаційних та програмно-апаратних елементів, а також операторів, що їх експлуатують.

Основними елементами такого класу КС є:

− масиви даних як сукупність інформації та її носіїв;

− технічні засоби, які автоматизують процеси, що відбуваються у системі (засоби обчислювальної техніки, інформаційно-обчислювальні комплекси і мережі, засоби і системи передачі, прийому та обробки інформації та команд, інші виконавчі технічні засоби, засоби і система охоронної та пожежної сигналізації, засоби і система оповіщення і сигналізації, контрольно-вимірювальна апаратура, засоби кондиціонування, електропостачання, зв'язку, оргтехніка тощо);

− програмні засоби (операційні системи, системи управління базами даних тощо);

− засоби захисту інформації (апаратні, алгоритмічні, програмні);

− людина-оператор (обслуговуючий персонал) з усіма притаманними психофізіологічними станами та реакціями.

З огляду на інформацію, яка забезпечує функціонування інформаційно-управляючої системи, запропоновану класифікацію можна розширити і у класі загроз каналу зв'язку (інформації, командам, що передаються) виділити підкласи:

− за видом інформації, яка передається;

− за видом властивості інформації, що порушується; за метою здійснення загрози тощо.

Зважаючи на присутність у контурі управління інформаційно-управляючої системи операторів, можна виділити такі *способи реалізації кіберзагроз*:

− інформаційно-психологічний вплив;

− психогенний вплив;

− психоаналітичний вплив;

− нейролінгвістичний вплив;

− психотронний вплив;

− психотропний вплив.

Якщо розглядати особливості процесів управління та обміну інформацією, які відбуваються у таких системах, то слід зазначити, що на даний момент вони здійснюються згідно з еталонною моделлю взаємодії відкритих систем ISO/OSI, викладеною у стандарті *ISO 7498*. Кіберзагроза як фактор, що впливає на процеси управління та передачі інформації, може бути спроектована на еталонну модель. Тому клас кіберзагроз, який характерний відкритим

системам, можна розширити такими підкласами:

− загрози фізичного рівня;
− загрози канального рівня;
− загрози мережного рівня;
− загрози транспортного рівня;
− загрози сеансового рівня;
− загрози рівня представлення;
− загрози прикладного рівня.

Таким чином, така класифікація кіберзагроз дозволяє вирішувати такі основні завдання:

− встановлювання основних зв'язків між існуючими та потенційними кіберзагрозами;
− формування достовірних прогнозів щодо виникнення і розвитку нових загроз;
− визначення ефективних способів захисту кібернетичних систем та їх складових від деструктивних кібервпливів та протидії кіберзагрозам;
− забезпечення подальших досліджень впливу кіберзагроз на відповідні об'єкти захисту [13].

1.3.2. Основні характеристики кіберзагроз

Оцінюючи високий ступінь кіберзагроз для держави, орієнтуючись на провідні держави світу в Україні впродовж останніх років значно інтенсифікується діяльність щодо прийняття та внесення змін до низки нормативно-правових актів, які стосуються кібербезпеки.

1. Указом Президента України №287/2015 "Про рішення Ради національної безпеки і оборони України" від 6 травня 2015 року "Про Стратегію національної безпеки України" була затверджена "Стратегія національної безпеки України". В Стратегії національної безпеки України були визначені актуальні Загрози національній безпеці України, серед яких є загрози інформаційній безпеці, загрози кібербезпеці і безпеці інформаційних ресурсів та загрози безпеці критичної інфраструктури. Відповідно до загроз визначені Основні напрями державної політики національної безпеки України.

2. Указом Президента України №96/2016 "Про рішення Ради національної безпеки і оборони України" від 27 січня 2016 року "Про Стратегію кібербезпеки України" була затверджена "Стратегія кібербезпеки України" та визначений робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки. Це документ довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави,

підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів Сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів.

3. Указом Президента України №240/2016 "Про рішення Ради національної безпеки і оборони України" від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" був затверджений "Стратегічний оборонний бюлетень України". Де на підставі положень Стратегії національної безпеки України, Воєнної доктрини України та Концепції розвитку Сектору безпеки і оборони України визначені стратегічні цілі.

Наприклад. Оперативна ціль 1.5. Удосконалення системи кібербезпеки та захисту інформації. Очікуваний результат: створено в Міністерстві оборони України, інших складових сектору оборони, підрозділи з кіберзахисту, протидії технічним розвідкам, впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC.

4. Закон України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року (набув чинності 9 травня 2018 року), в якому визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Також зроблено низку змін в інші нормативно-правові акти: "Про Державну службу спеціального зв'язку та захисту інформації України", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про оборону України", "Про засади внутрішньої і зовнішньої політики", "Про об'єкти підвищеної небезпеки" тощо.

Враховуючи вищезазначене були сформовані основні кіберзагрози у найважливіших сферах та їх характеристики:

− кіберзагрози у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою;

− кіберзагрози в інформаційній безпеці;

− загрози кібертероризму;

− кіберзагрози в енергетичній сфері;

− кіберзагрози у воєнній сфері.

Кіберзагрози у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою. Системі державного управління приділяється ключова роль в управлінні державою. Це визначається тим, що державне управління, з одного боку, є конкретним специфічним видом управлінської діяльності державними інститутами зі своєю компетентнісною та функціональною специфікою, яка суттєво відрізняє його

від інших видів управлінської діяльності. З іншого боку, державне управління є прерогативою спеціальних суб'єктів управління – органів державного управління, які згідно зі своїм функціональним призначенням здійснюють управління державними процесами у межах свої компетенції. Важливо також відзначити дві обставини. Перша: системі державного управління властива ієрархічна структура, яка визначається прийнятою у тій чи іншій державі технологією побудови вертикалі влади. Друга: для системи державного управління зберігаються усі базові принципи управління, прийняті в теорії управління.

Навіть поверхневий аналіз сфери державного управління у таких провідних країн світу як США, Китай, ФРН та ін. показує, що система державного управління, незалежно від територіального розміщення держави, прийнятої у ній політичної ідеології та інших особливостей державного устрою, охоплює такі основні складові елементи, як:

− суб'єкти державного управління (органи виконавчої влади);

− об'єкти державного управління (усі сфери життєзабезпечення суспільства та держави, у тому числі й об'єкти з критичною інформаційною інфраструктурою, що перебувають в компетенції управління держави);

− процеси управління державою (суспільні відносини, що виступають регулятором прямих та зворотних зв'язків між суб'єктами та об'єктами управління).

Зважаючи на наявність у системі державного управління типових ознак кібернетичної системи, таких як суб'єктів управління, об'єктів управління та середовища для обміну процесами управління у подальшому її декомпозицію здійснюватимемо саме з позицій кібернетичної системи.

У широкому розумінні під кіберзагрозами у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою розуміються потенційно можливі кібервпливи природного, технічного або антропогенного характеру, які можуть спричинити небажані наслідки для суб'єктів і об'єктів системи та процесів управління нею. Виникнення будь-якої кіберзагрози у сфері державного управління характеризується наявністю уразливості у системі державного управління. Чим більше уразливостей має система державного управління, тим більша кількість кіберзагроз їй загрожує. Зважаючи на те, що усі кіберзагрози не можуть бути піддані повному описові, розглянемо головні з них.

Головна кіберзагроза у сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою для будь-якої держави – це загроза через кібервплив протиборчої сторони на свідомість, підсвідомість, інформаційні ресурси, інфосферу об'єктів з критичною інформаційною інфраструктурою держави нав'язати людині, суспільству й державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у сфері державного управління та управління об'єктами з критичною інформаційною інфраструктурою, керувати їх поведінкою і розвитком у бажаному для іншої сторони напрямі. Тому очевидним є факт того, що держави

з вищим ступенем економічного, політичного, соціального та інших рівнів розвитку намагаються через сферу державного управління інших держав з нижчим рівнем керувати їх розвитком у своїх інтересах під постійним інформаційним контролем.

При реалізації кіберзагроз у сфері державного управління також переслідується ціль, яка полягає у зміні правлячого режиму шляхом руйнування базових основ системи державного управління. Означена мета досягається не за рахунок руйнування економічного або військового потенціалу держави, а за рахунок реалізації таких кіберзагроз, які здійснюються у вигляді масованого кібервпливу, що як наслідок призводять до змін в морально-психологічному стані її населення та керівництва держави. Кіберзагрози при цьому спрямовуються для вирішення таких цілей:

− створення атмосфери бездуховності та аморальності, негативного відношення до органів державної влади;

− маніпулювання громадською свідомістю і політичною орієнтацією соціальних прошарків населення держави в інтересах створення політичної напруги та хаосу;

− дестабілізація політичних відносин між політичним партіями, громадськими об’єднаннями та рухами з метою провокації конфліктів, розпалювання атмосфери недовіри та підозрілості;

− загострення політичної боротьби, провокування репресій проти опозиції;

− розв’язування у суспільстві громадянської війни;

− зниження рівня керованості органів державної влади і органів управління з метою утруднення прийняття важливих державних рішень;

− дезінформація населення про роботу органів державної влади, підрив їх авторитету, дискредитація органів управління;

− провокування соціальних, політичних, національних і релігійних сутичок;

− ініціювання страйків, масових безладів й інших акцій економічного протесту;

− підрив міжнародного авторитету держави, його співпраці з іншими державами;

− нанесення втрат життєво важливим інтересам держави в політичній, економічній, оборонній, інформаційній, науково-технологічній та інших сферах.

Досвід більшості держав, де відбулись так звані “кольорові революції”, свідчить про те, що такі держави не були у змозі не тільки протистояти негативним кібервпливам, але й виявляти сам факт такої агресії. Такий стан справ можна пояснити тим, що оперативність і якість управлінських рішень напряму залежать від повноти та достовірності вхідної та вихідної інформації, викривлення та маніпулювання якою є однією з головних задач інформаційної війни.

До джерел загроз кібербезпеці у сфері державного управління та у сфері управління об’єктами з критичною інформаційною інфраструктурою належать:

− руйнування об’єктів з критичною інформаційною інфраструктурою у результаті кібервпливів, що можуть призвести до виникнення техногенних катастроф або спалаху воєнних конфліктів;

− інформаційна ізоляція держави та блокування діяльності системи державного управління у результаті цілеспрямованих кібервпливів іноземних держав, неадекватної зовнішньої та внутрішньої політики у різних сферах;

− діяльність іноземних спецслужб;

− діяльність державних та недержавних політичних та економічних структур, спрямованих проти системи державного управління та об’єктів з критичною інформаційною інфраструктурою;

− недосконаліть систем виявлення кібервпливів та попередження їх наслідків, недостатній рівень кваліфікації персоналу відповідних систем;

− “віртуалізація” процесів державного управління та управління об’єктами з критичною інформаційною інфраструктурою через кіберпростір без приділення належного рівня уваги організації заходів щодо забезпечення їх гарантованої захищеності;

− міжнародний кібертероризм;

− недосконаліть нормативно-правової бази щодо протидії негативним кібервпливам на системи державного управління та об’єкти з критичною інформаційною інфраструктурою;

− зниження темпів науково-технічного розвитку у результаті неадекватної внутрішньої та зовнішньої політики держави в інформаційній сфері.

До об’єктів загроз кібербезпеці систем державного управління та у сфері управління об’єктами з критичною інформаційною інфраструктурою належать різні управлінські аспекти діяльності системи державного управління, а саме:

− система формування суспільної свідомості через формування у суб’єктів певного менталітету, світогляду, політичних поглядів, моральних цінностей тощо;

− механізми прихованого управління індивідуальною свідомістю та підсвідомістю суб’єктів державного управління, що є потенційними мішенями цілеспрямованого кібервпливу;

− управління об’єктами з критичною інформаційною інфраструктурою, що включають відповідну інфраструктуру (системи накопичення, обробки та аналізу інформації, комутаційні канали, системи та мережі тощо).

Кіберзагрози у сфері державного управління та у сфері управління об’єктами з критичною інформаційною інфраструктурою можуть реалізовуватися за різними напрямами. До основних напрямів реалізації впливу кіберзагроз можна віднести такі, як:

− цілеспрямоване використання засобів масової інформації з позицій, що суперечать інтересам системи державного управління;

− маніпулювання інформацією (дезінформація, приховування або спотворення інформації та процесів управління);

− порушення процесів управління за рахунок несанкціонованого доступу сторонніх суб'єктів до процесів прийняття управлінських рішень або необґрунтованого обмеження доступу легальних суб'єктів управлінської діяльності;

− деструктивний вплив на національний сегмент кіберпростору з метою використання його в антидержавних інтересах;

− формування нових "підставних" суб'єктів державного управління з метою реалізації через них кібервпливів деструктивного характеру на систему державного управління та об'єкти з критичною інформаційною інфраструктурою;

− різні види кібервпливів;

− реалізація помилкової (нав'язаної із зовні) економічної та науково-технічної політики у процесі управління державною системою та об'єктами з критичною інформаційною інфраструктурою.

У сфері управління об'єктами з критичною інформаційною інфраструктурою потенційно кіберзагрози можуть бути спрямовані на: інформаційно-телекомунікаційні системи державного управління та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів, систем і об'єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв'язком, банківським сектором, підприємств, під час діяльності яких використовуються та (або) виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур й оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави. До таких об'єктів з критичною інформаційною інфраструктурою можна віднести такі групи об'єктів, як:

− державні електронні інформаційні ресурси;

− автоматизовані системи управління або електронні інформаційні ресурси де обробляється (зберігається) інформація, яка є власністю держави, або інформація, несанкціоновані дії щодо якої можуть створювати загрозу національній безпеці та обороноздатності держави (у тому числі відкрита інформація);

− автоматизовані системи управління, що використовуються суб'єктами воєнної організації держави;

− телекомунікаційні системи загального користування та спеціальні телекомунікаційні системи;

− автоматизовані системи управління, що здійснюють керування виробничими та (або) технологічними процесами на об'єктах підвищеної небезпеки та інші інформаційно-телекомунікаційні системи та автоматизовані системи управління.

Наслідки впливу кіберзагроз у визначених сферах проявляються на всіх рівнях, оскільки найбільш уразливими об'єктами кібервпливів виступають механізми управлінської діяльності індивідів, що відповідають за формування

їх ментальності, свідомих та підсвідомих сфер мислення та поведінки. На рівні суб'єкта реалізація визначених кіберзагроз призводить до формування викривленого поняття про навколишню дійсність, права, свободи, життєві цінності, державний устрій тощо, що призводить до втрати відчуття самореалізації. Як результат створюються передумови для реалізації кібервпливів деструктивного характеру, ускладнюються соціальні процеси, загострюються протиріччя між різними соціальними прошарками, зростає політична напруженість у суспільстві, знижується ступінь керованості суспільством та державою.

Вплив кіберзагроз на систему державного управління, що регулює процеси, які безпосередньо впливають на безпеку держави, рівень та якість життя населення, як показує світовий досвід, призводить до катастрофічних наслідків і для держави, і для суспільства. Результатом пливу кіберзагроз на систему державного управління є спотворення процесів управління державою таким чином, що унеможливлюються усталені процеси управління державою та об'єктами з критичною інформаційною інфраструктурою. Наслідком порушенням таких процесів може бути втрата державою суверенітету.

Реалізація кіберзагроз має й інші, не менш негативні наслідки. Це наслідки економічного характеру, що охоплюють усю сукупність процесів від втрати керованості державою до повної руйнації її критичної інформаційної інфраструктури. Втрата керованості унеможливлює прийняття найважливіших політичних та економічних рішень. На етапі формування основ державної політики реалізація визначених кіберзагроз призводить до підриву авторитету системи державного управління не тільки у суспільстві, а й на міжнародній арені. Порушення процесів управління у системі державного управління ускладнює контроль та управління об'єктами з критичною інформаційною інфраструктурою. У результаті порушуються баланс у відносинах між суспільством і державою, уповільнюються темпи економічного, соціального та культурного розвитку.

У сфері державного управління та у сфері управління об'єктами з критичною інформаційною інфраструктурою кіберзагрози можуть бути спрямовані на:

− посягання на державний суверенітет держави та її територіальну цілісність, на прояв територіальних претензій з боку інших держав;

− здійснення спроб втручання у внутрішні справи будь-якої держави з боку інших держав;

− провокування воєнно-політичної нестабільності, яка може призвести до розпалювання регіональних та локальних війн;

− створення сприятливих умов для розвідувально-підривної діяльності іноземних спецслужб;

− поширення корупції у системі державного управління, створення умов для налагодження співпраці між бізнесом, політикою й організованою злочинністю;

− поширення кібертероризму та кіберзлочинності;

− несанкціоноване використання об’єктів з критичною інформаційною інфраструктурою з метою вчинення техногенних аварій та катастроф;

− створення сприятливих умов для використання в інтересах протиборчої сторони діяльності військових формувань і правоохоронних органів держави;

− зародження та провокування проявів сепаратизму та екстремізму;

− створення умов для порушення системою державного управління норм діючого законодавства;

− розбалансування системи державного управління внаслідок порушення усталених процесів управління те регулювання державних механізмів;

− формування несприятливих умов, що призводять до критичної залежності системи державного управління та об’єктів з критичною інформаційною інфраструктурою від закордонних високотехнологічних розробок в ІТ- сфері;

− створення підґрунтя на тлі якого в управлінській діяльності системи державного управління превалюватимуть особистісні інтереси над загальнонаціональними;

− створення передумов для моральної та духовної деградації суспільства;

− зведення до мінімуму ефективності державної інноваційної політики;

− обмеження свободи слова та доступу громадян до інформації;

− поширення засобами масової інформації культу насильства, жорстокості, порнографії;

− розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

− маніпулювання суспільною свідомістю шляхом поширення недостовірної, неповної або упередженої інформації;

− провокування інформаційної війни.

Кіберзагрози в інформаційній безпеці

Питанням дослідження впливу проявів кіберзагроз на інформаційну безпеку останнім часом приділяється значна увага наукової спільноти. Це пов’язано не лише з високотехнологічністю суспільства, а й з тими новими викликами та загрозами, що породжуються у інформаційній сфері внаслідок її розвитку. У силу політичного та економічного протистояння держав породжені новими викликами та загрозами проблеми з часом тільки загостюються. Змінюються цілі протистояння, нового обрису набувають об’єкти та суб’єкти впливу. Для прикладу: основною ціллю реалізації кіберзагрози в інформаційній сфері, незалежно від її виду, є здійснення таких кібервпливів, які призводять до управління масовою та індивідуальною свідомістю таким чином, що протиборча сторона (інколи навіть не знаючи про це) діє всупереч власним інтересам. При цьому, суб’єктом впливу кіберзагроз у вузькому сенсі завжди виступає людина та її психіка, а у більш широкому – масова свідомість. Ці кібервпливи, незалежно від того усвідомлювані вони чи ні, призводять до серйозних порушень психічного та фізичного здоров’я, поступового

розмивання природних і культурних норм поведінки, до нагнітання соціальної напруженості у суспільстві та виникнення непередбачуваних критичних ситуацій.

Для визначення кіберзагроз в інформаційній сфері та з'ясування джерел їх появи досить важливо правильно вміти виокремлювати об'єкти кібервпливу від суб'єктів кібервпливу. До об'єктів кібервпливу в інформаційній сфері відносяться ті об'єкти, у відношенні яких можуть бути реалізовані кіберзагрози у вигляді кібервпливів, що, як наслідок, призводять до модифікації властивостей таких об'єктів як кібернетичних систем. При цьому, ключовою ознакою об'єкта, що дозволяє розглядати його як об'єкт кібервпливу є наявність у ньому процесів управління. Конкретизуючи такі об'єкти, до них можна віднести такі системи, як: систему соціальних відносин; систему політичних відносин; систему психологічних відносин. Об'єктом кібервпливів в інформаційній сфері може бути також будь-який компонент або сегмент кіберпростору, в якому відбуваються процеси управління. Наприклад, масова та індивідуальна свідомість, соціально-політична система, критична кібернетична інфраструктура, психологічні ресурси (система цінностей, психологічне здоров'я) тощо.

Суб'єктами кібервпливу в інформаційній сфері можуть виступати держави, їх союзницькі утворення і коаліції, міжнародні утворення, незаконні збройні формування, терористичні та екстремістські організації, транснаціональні компанії, різні соціальні мережі, медіа-корпорації, віртуальні коаліції та ін. Головними ознаками, що дозволяють відносити розглядувані утворення до суб'єктів кібервпливу в інформаційній сфері, є такі:

− суб'єкти мають власні цілі та інтереси;

− суб'єкти у своєму складі мають соціальні утворення, що можуть бути використані для здійснення інформаційно-психологічних впливів;

− суб'єкти спроможні до розробки або розробляють кіберзброю для здійснення інформаційно-психологічного впливу;

− суб'єкти спроможні здійснювати контроль над визначеним сегментом кіберпростору у рамках якого вони спроможні встановлювати регуляторні норми інформаційно-психологічних відносин;

− наявність у суб'єкта спеціальної ідеології (доктрини або стратегії), що передбачає правила його участі в заходах інформаційно-психологічного протиборства.

Встановивши відмінність між суб'єктами та об'єктами впливу в інформаційно-психологічній сфері можна помітити, що кіберзагрози для них можуть спрямовуватися на:

− особистість, суспільство, державу;

− масову свідомість;

− індивідуальну свідомість.

Кіберзагрози для особистості проявляються у двох основних аспектах. Перший аспект проявляється при впливі на особистість, як суб'єкта політичного життя, носія певного світогляду співвимірного з його життєвими

та особистісними ціннісними установками й духовними ідеалами, що володіє правом вираження політичного волевиявлення, і другий – при вивченні особистості як свідомого індивіда, що піддається різним маніпуляціям із застосуванням кібервпливів, що призводять до реалізації загроз щодо втрати ним фізичного та психічного здоров'я.

У першому випадку реалізація кіберзагрози щодо особистості, як суб'єкта політичного життя, призводить до побудови між цим суб'єктом, суспільством та державою такої лінії поведінки, яка набуває рис екстремізму, що загрожують існуванню політичної системи в державі й сприяють утвердженню політичної байдужості суспільства.

У другому випадку – при впливі на особистість, як свідомого індивіда, кіберзагрози проявляють себе як цілеспрямовані довготривалі кібервпливи, що призводять до формування бажаної для зацікавленої сторони морально-психологічної атмосфери, яка сприяє зародженню кіберзлочинності, кібертероризму і, як наслідок, призводить до порушень фізичного та психічного здоров'я. Зважаючи на те, що для конкретного індивіда головними системоутворюючими рисами є цілісність (тенденція до стійкості) та розвиток (тенденція до зміни), то перекручування або руйнування цих рис призводить до припинення його існування, як соціального суб'єкта. Це говорить про те, що вплив кіберзагроз на індивідуальну свідомість індивіда слід розцінювати з двох позицій – з позиції збереження індивіда як особистості та з позиції руйнування його, як цілого. Прикладом небезпек при впливі на особистість, як свідомого індивіда, може бути цілеспрямований процес поширення порнографічної продукції, що ображає суспільну мораль, руйнує дитячу психіку та призводить до спонукання індивіда до здійснення протиправних вчинків.

Кібервпливи можуть ісуттєво змінювати масову (суспільну) свідомість і поводження великих соціальних груп, навіть незважаючи на той факт, що такий вид свідомості формується насамперед у процесі історичного розвитку нації, народності, великої соціальної групи. Велика соціальна група – це необмежена за кількістю певна соціальна спільнота, яка має стійкі цінності, норми поведінки і соціально-регулятивні механізми. Їх прикладом можуть бути партії, етнічні групи, виробничо-галузеві та громадські організації. Соціально-психологічними регуляторами життєдіяльності великих груп є: групова свідомість, менталітет, звичаї, традиції тощо. Велика група характеризується низкою групових факторів до яких відносять психічний склад групи, групову психологію та групову свідомість. Остання, у свою чергу, впливає на формування у носіїв цієї групи відповідного типу особистості, що обов'язково враховується і використовується при здійсненні інформаційно-психологічних впливів. Метою впливів на масову свідомість суспільства є виклик особливої, конфліктної поведінки його в різних життєвих ситуаціях. Наприклад, ініціювання паніки у суспільстві, примус до здачі у полон, мобілізація мітингувальників тощо. Такі підходи та механізми їх реалізації знайшли ґрунтовне відображення у спеціалізованій науковій літературі.

Наслідки впливу кіберзагроз для суспільства зокрема та держави в цілому

проявляються у локальному (регіональному) та загальнонаціональному масштабах. Маніпулювання масовою свідомістю досягається у результаті цілеспрямованого інформаційно-психологічного впливу у вигляді потужного психологічного і морального тиску на суспільство на фоні його бідності та соціальної незахищеності, що призводять до проявів непокори діючій системі державного управління. Окремі види інформаційно-психологічного впливу, які спрямовуються на визначені цілі (суспільство чи окремих індивідів) здатні до серйозного порушення нормального функціонування державних інститутів.

Прояв кіберзагроз на індивідуальну свідомість призводить до того, що в ній відбуваються дві взаємопов'язані зміни. Це зміни у психіці та психічному здоров'ї та зміни у життєвих цінностях, орієнтирах та світогляді. У першому випадку втрачається адекватне сприйняття світу та подій, які у ньому відбуваються. Притупляються усі психічні реакції, відбувається деградація особистості, здійснюється перехід від потреб вищого рівня (духовного) до потреб нижчого рівня (фізіологічного). У другому випадку зміна життєвих цінностей спонукає здійснення антисоціальних вчинків, які становлять небезпеку не тільки для самого суб'єкта, а й суспільства та держави в цілому.

Масова свідомість також уразлива до проявів кіберзагроз, навіть не зважаючи на те, що її підвалини в першу чергу, формуються насамперед життєвим досвідом, а вже потім внаслідок кібервпливу. У психології мас, згідно з французьким психологом Г. Лебоном, інформаційні процеси та процеси управління можуть розглядатися у трьох формах при впливі на населення, натовп та колектив. При цьому, основними джерелами, що дозволяють впливати на масову свідомість, а відповідно і керувати масами для населення, є ЗМІ та чутки, для натовпу – не обов'язково грамотний, але обов'язково харизматичний і бажано фанатичний лідер та його найближче оточення, для колективу – офіційна інформація від посадових осіб та неформального (обраного або призначеного) лідера.

Таким чином, метою реалізації кіберзагроз у інформаційно-психологічній сфері може бути реалізація кібервпливів спрямованих на:

− нанесення шкоди психічному здоров'ю особи;

− порушення традиційних устоїв особистості, суспільства, держави;

− порушення стійкості процесів управління в кіберпросторі;

− цілеспрямований кібервплив на особистість та суспільство, спрямований на блокування вільного волевиявлення, штучне нав'язування йому синдрому залежності і здійсненням ним через ці обставини протиправних дій;

− розробку, створення і застосування спеціальних технічних і програмних засобів інформаційно-психологічного впливу на психіку особистості;

− цілеспрямоване втручання іноземних спецслужб у роботу державних кібернетичних систем;

− управління масовою свідомістю з використанням спеціалізованих засобів інформаційно-психологічного впливу;

− підготовку до кібервійн з використанням кіберзброї.

Потенційними джерелами виникнення та поширення кіберзагроз для визначених суб'єктів та об'єктів впливу є:

− ЗМІ і спеціальні засоби, що мають інформаційно-пропагандистську спрямованість. Сучасні ЗМІ (радіо, газети, телебачення) виконують роль засобів комунікацій між суб'єктами та об'єктами кіберпростору. З одного боку ЗМІ, як потенційні джерела поширення кіберзагроз в інформаційно-психологічній сфері, можуть бути стримуючим фактором при розв'язанні кібервійн, з іншого – як їх ініціатор та підсилювач. Засоби інформаційно-психологічної спрямованості (мобільні телерадіомовні пропагандистські центри) на відміну від ЗМІ мають менше за територіальними ознаками охоплення цільової аудиторії, але характеризуються конкретним, спрямованим на певний регіон (територію) контентом, який поширюється, як приховано, так і з використанням засобів телерадіомовлення та друкованої продукції (флаєрів, листівок, плакатів тощо);

− мережа Інтернет та спеціалізоване програмне забезпечення прискореного поширення відповідних впливів. Мережа Інтернет, яка має високу ресурсоспроможність на сьогодні перетворюється в нове соціальне середовище (*е*-середовище) та досить динамічно набуває вигляду базису дієвої медіатехнології прихованого кібервпливу світового масштабу. Спеціалізоване програмне забезпечення прискореного поширення кібервпливів тільки сприяє підсиленню дієвості таких впливів, причому без порушення законів та при повній безконтрольності з боку держави;

− спеціальні технічні пристрої та програмні засоби, що здатні модифікувати (порушувати цілісність) інформації, на основі якої приймаються стратегічні рішення;

− засоби віртуальної реальності;

− чутки;

− засоби підпорогового психосемантичного впливу;

− фізичні особи, що від природи наділені здатністю неусвідомленого кібервпливу на особистість, суспільство, державу, масову та індивідуальну свідомість;

− релігійні та інші об'єднання громадян;

− нові зразки зброї на нетрадиційних принципах дії (наприклад, генератори фізичних полів та випромінювань тощо).

Загрози кібертероризму

Протягом останнього десятиріччя проблема кібертероризму була актуальною в основному для держав з високим ступенем розвитку інформаційної інфраструктури. При цьому досить чітко простежувалася тенденція між ступенем інформаційного, технологічного, економічного розвитку такої держави та кількістю здійснених у ній (проти неї) актів кібертерору. На сьогодні ж дана тенденція змінюється. Проблема кібертерору стає актуальною й для тих держав, темпи впровадження високих технологій у національну економіку в яких тільки нарощуються. У світі вже практично немає

держави, де б ще не використовувалися передові надбання науково-технічного процесу, а тому проблема кібертероризму стає реальною загрозою для усього людства.

Однією з причин масового поширення явища кібертероризму є значний вплив процесу глобалізації на світову економіку, який призвів до дисбалансу між державами з різним рівнем розвитку, а відповідно й до зростання невдоволеності певних верств населення політикою, що нав'язується державами – лідерами. Проблема загострюється ще й тим, що в передових державах світу рівень розвитку інфокомунікаційних та інших високих технологій та просякнення ними всіх сфер життя, а відповідно і залежності від їх стану та захищеності суттєво зростають. Масова комп'ютеризація таких їх життєво важливих сфер діяльності, як зв'язок, енергетика, транспорт, системи зберігання та транспортування нафти і газу, фінансова і банківська системи, оборонні структури, структури із забезпечення роботи міністерств і відомств, перехід на методи електронного управління технологічними процесами у виробництві та державою ("електронний уряд"), Інтернет речей є підгрунтям зростання негативних наслідків від кібертероризму та сприяє його поширенню.

З метою встановлення сутності загрози кібертероризму, доцільно дослідити зміст терору, як такого. Тероризм є багатогранним поняттям, що поєднує у собі елементи екстремістської ідеології, комплекс організаційних структур для здійснення тероризму в різних його формах та проявах, а також практику здійснення терористичних актів. Як суспільно небезпечне явище тероризм має глибоке історичне підґрунтя, зародки якого походять з біблійних часів. Але тільки у XX ст. тероризм з локального внутрішнього фактора перетворився на міжнародне суспільно небезпечне явище, як за складом його учасників та сил підтримки, так і за характером цілей, що переслідуються.

Аналіз відповідної спеціалізованої наукової літератури, присвяченої дослідженню проблеми тероризму показує, що на сьогодні існує не менш ніж сто різних визначень тероризму. Але кожне із них має одну характерну спільну рису – це присутність елементу насильства. Відмінності у відомих визначеннях проявляються лише при розмежуванні таких категорій, як "насильство", "екстремізм", "війна" тощо. Таке розмежування значно ускладнює вироблення єдиних міжнародних уявлень феномену тероризму.

Тероризм (у перекл. з лат. *terror* – жах) – це спосіб досягнення політичних або інших цілей шляхом диверсій, шантажу життям заручників і нагнітання страху у суспільстві. Вперше терор як спосіб досягнення політичних цілей застосовано радикальними революціонерами під час Великої французької революції для здійснення репресій проти політичних опонентів.

У Законі України "Про основні засади забезпечення кібербезпеки України" [39] наведено наступне визначення "**кібертероризм** – терористична діяльність, що здійснюється у кіберпросторі або з його використанням".

Відповідно до Закону України "Про боротьбу з тероризмом" [54] терористична діяльність – діяльність, яка охоплює:

− планування, організацію, підготовку та реалізацію терористичних актів;

− підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об'єктів у терористичних цілях;

− організацію незаконних збройних формувань, злочинних угруповань (злочинних організацій), організованих злочинних груп для вчинення терористичних актів, так само як і участь у таких актах;

− вербування, озброєння, підготовку та використання терористів;

− пропаганду і поширення ідеології тероризму;

− фінансування та інше сприяння тероризму.

Отже, в цьому Законі нічого не сказано про кібертероризм. У площині кіберпротистояння дамо власне бачення "кібертероризму". **Кібертероризм** – це цілеспрямоване залякування населення та органів влади реальними або можливими та проголошеними (заявленими) кібервпливами на соціум, соціотехнічні та технічні системи, вчинення яких призводить до виникнення (створення передумов для виникнення) небезпеки для громадян, суспільства, держави та має високий потенціал страхання (залякування).

Отже, до основних ознак кібертероризму можна віднести:

− високу ефективність наслідків, які можуть мати як локальний, так і глобальний характер;

− невизначеність джерела кібертерору;

− невизначеність місця, часу та процесу підготовки до здійснення кібертеракту;

− можливість організації актів кібертерору одночасно на різні об'єкти або суб'єкти з зірних напрямів без необхідності порушення будь-яких кордонів;

− високий ступінь анонімності при здійсненні кібертерактів;

− просторово-часова віддаленість від об'єкта або суб'єкта кібератаки. Усі кібервпливи здійснюються в кіберпросторі та безпосередньо через кіберпростір.

Кібертероризм має такі особливості:

− як міжнародні, так і внутрішні, національні прояви;

− різноманіття і не завжди очевидність цілей;

− високий рівень латентності і низький рівень розкривання;

− проведення кібертерактів не завжди потребує великих фінансових витрат, а наслідки від їх здійснення можуть наносити значний матеріальний збиток.

Основною відмінністю кібертероризму від тероризму в усталеній його інтерпретації є те, що кібервплив на процеси управління, які протікають у соціумі, соціотехнічних та технічних системах, здійснюється через кіберпростір з використанням надбань сучасних високих технологій.

Здійснення кібертерактів надає можливість:

− формування реальних загроз життю та найбільш важливим інтересам громадян;

− створення критичних ситуацій на особливо небезпечних об'єктах інфраструктури (у тому числі таких, які можуть привести до техногенних катастроф на атомних електростанціях, підприємствах хімічної, нафто -

і газопереробних й інших галузях) та на інших об’єктах забезпечення життєдіяльності (банки, медичні заклади, транспорт) за рахунок пошкодження систем управління ними, програм, баз даних, мікропроцесорів, комп'ютерів, відомчих та загальних комп'ютерних мереж, інфокомунікаційних систем тощо;

− створення атмосфери бездуховності та аморальності, негативного ставлення до національної та світової культурної спадщини;

− маніпулювання суспільною свідомістю різних соціальних груп населення для формування соціальної та політичної напруженості та відчуття некерованості у визначеному регіоні;

− дестабілізації відносин між політичними та релігійними рухами в цілях провокації конфліктів та загострення політичного та релігійного протистояння;

− зниження рівня керованості органами системи державного і військового управління, ускладнення прийняття ними стратегічних рішень;

− дезінформації населення про роботу державних органів управління, підрив їх авторитету та дискредитації, створення атмосфери страху та невпевненності;

− провокування соціальних, політичних, національних і релігійних конфліктів;

− ініціювання масових страйків, заворушень та підбурювання до інших акцій громадської непокори;

− підриву авторитету держави-опонента на міжнародній арені та нанесення їй збитків у різних ключових для її економіки сферах, за рахунок впливу на процеси управління в них.

Як видно – основними ознаками кібертерактів є загроза настання суспільно небезпечних наслідків та значних суспільних резонансів при створенні умов для відповідного широкого інформування населення. При цьому, кібертеракт завжди зорієнтований на використання різноманітних форм і способів порушення процесів управління інформаційною інфраструктурою держави або на використання її для створення обстановки, що приводить до катастрофічних або особливо небезпечних (неприйнятних) наслідків для особи, суспільства, держави.

Метою кібертероризму може бути таке порушення процесів управління, яке призведе до:

− дезорганізації діяльності державних та приватних структур з управління транспортними, інформаційними, фінансовими та іншими потоками тощо;

− блокування нормальної діяльності систем державного управління та окремих приватних структур, а також стратегічних галузей національної та світової економіки тощо.

Засобом здійснення кібертерактів є високі технології, специфічні способи та прийоми, застосування яких дозволяє порушувати процеси управління у соціумі, соціотехнічних системах та технічних системах шляхом:

− отримання через кіберпростір несанкціонованого доступу до державної таємниці та інформації з обмеженим доступом у різних сферах;

− нанесення збитків об’єктам з критичною кібернетичною інфраструктурою (руйнування мереж електроживлення, водопостачання тощо);

− крадіжки або знищення управлінської інформації, програм і технічних ресурсів за рахунок подолання систем захисту, впровадження вірусів, програмних закладок тощо;

− впливу на програмне забезпечення та процеси управління з метою їх модифікації;

− розкриття і загрози оприлюднення інформації з обмеженим доступом;

− маніпуляції репутацією осіб, кібербуллінгу;

− захоплення каналів засобів масової інформації з метою поширення дезінформації, чуток, демонстрації сили терористичної організації й оголошення своїх вимог;

− знищення або активного радіоелектронного подавлення ліній зв’язку, неправильної адресації сигналів управління, перенавантаження вузлів комунікацій, здійснення кібервпливів на суб’єктів кіберпростору (операторів, розробників інформаційно-комунікаційних систем, управлінців різного рангу тощо);

− проведення різноманітних інформаційно-психологічних впливів тощо.

За наслідками прояву кібертеракти можуть бути поділені на два рівні – першого та другого рівнів.

Реалізація кібертерактів першого рівня призводить до тимчасового виведення з ладу кібернетичних систем, незалежно від природи їх походження. Кібертеракти першого рівня є найбільш поширеним проявом кібертероризму. Унаслідок їх реалізації через тимчасове виведення з ладу кібернетичної системи можливе її безконтрольне функціонування або функціонування за непередбачуваним для штатних режимів роботи алгоритмів. Особливо небезпечні наслідки прояву впливу кібертерактів такого рівня для об’єктів з критичною кібернетичною інфраструктурою (атомної енергетики, хімічної промисловості, систем озброєння і військової техніки тощо).

Кібертеракти другого рівня мають руйнівні наслідки для кібернетичних систем. Вони призводить до фізичного знищення критичної кібернетичної інфраструктури.

Крім того, інформаційний і кіберпростір та можливості сучасних високотехнологічних систем (засобів) використовуються (слугують інструментами та є необхідною, невідємною складовою) при підготовці та здійсненні практично всіх без виключення терористичних актів.

Можливими джерелами кібертерору можуть бути будь-які організації і навіть особи, що мають доступ до високих технологій.

Терористичні організації та угруповання активно використовують здобутки високих технологій для зв’язку та обміну інформацією, ведення пропагандистської діяльності, вербування нових членів та організації терористичної діяльності. Наприклад, один із виконавців теракту на Всесвітній торговий центр в Нью-Йорку 11 вересня 2001 року Р. Юзеф керувався зашифрованими інструкціями, що надходили мережею Інтернет.

Названі джерела спроможні до провокування виникнення нової системної світової кризи, здатної поставити під загрозу існування окремих регіонів світу, що не було характерним для “традиційних” терористичних актів. Саме тому протидія кібертероризму є однією з ключових міжнародних проблем.

З метою протидії кібертероризму, як на міжнародному, так і на національному рівнях слід, по-перше, закріпити відповідні юридичні норми; по-друге – розробити і впровадити передові методи його профілактики; по-третє – готувати кваліфікований кадровий потенціал; по-четверте – налагоджувати міжнародну співпрацю та, по-п’яте – створювати національні відомчі підрозділи протидії кібертероризму.

Отже, в усьому світі визнано, що кібертероризм є актуальною проблемою сучасності глобального характеру, яка без вжиття відповідних засобів протидії буде неухильно нарощуватися використовуючі результати розвитку та розповсюдження високих технологій.

Кіберзагрози в енергетичній сфері

Глибоке проникнення енергетики в усі галузі економіки та у соціальну сферу визначає її особливу роль у забезпеченні безпеки розвитку сучасного суспільства. Енергетична безпека характеризує міру виконання енергетикою її функцій перед суспільством, державою, як у звичайних, так і в критичних умовах, зокрема в умовах надзвичайного чи воєнного стану, особливий період тощо.

На території України в кожній області присутні об’єкти енергетики, які відносяться до критичної інфраструктури, і на кожному із них є так звані “критичні точки”, елементи порушення нормального функціонування яких призводить до порушення їх функціональної придатності, а у низці випадків викликає ланцюгові деструктивні ефекти .

Всі вони пов’язані певною ієрархією, системою управління та системою захисту. Основу електроенергетики становить об’єднана енергетична система України, яка централізовано забезпечує електроенергією внутрішніх споживачів, а також здійснює її експорт та імпорт. Дана система об’єднує вісім регіональних електроенергетичних систем, пов’язаних між собою системоутворюючими та міждержавними високовольтними лініями електропередач.

Вся сукупність загроз, які можуть впливати на функціонування систем енергетики умовно можливо поділити на ординарні загрози (ймовірні відмови та аварії) та неординарні (унікальні за причиною виникнення, характером розвитку та наслідками). Для протидії неординарним загрозам у системах енергетики передбачені різноманітні форми резервування потужностей, з вироблення та транспортування паливно-енергетичних ресурсів, систем забезпечення гарантованого енергопостачання та створення запасів паливно-енергетичних ресурсів. За умов розвитку та функціонування національної економіки подібні ординарні явища майже не становлять загроз енергетичній безпеці, на відміну від неординарних впливів, які здатні негативно впливати на

енергетичний комплекс в цілому. Серед неординарних загроз провідне місце займають кіберзагрози, які здатні спровокувати такі проблеми, як порушення забезпечення енергоресурсами, так і надзвичайні ситуації в енергетичному комплексі (ЕК) держави.

Такі кіберзагрози можуть бути реалізовані шляхом впливу на весь ЕК в цілому, або на його окремі елементи, як без, так і з досягненням синергетичності результатів. Вплив може бути проведений комплексно, одночасно, послідовно або змішано на автоматизовану систему управління (АСУ), апаратно-програмний комплекс, персонал, фінансову систему енергетики. Найбільш уразливим місцем об'єднаної енергетичної системи (ОЕС) є АСУ.

Система управління ОЕС відіграє провідну роль у функціонуванні всього ЕК України. Саме на АСУ ОЕС може бути здійснений потужний кібервплив, який може призвести до порушення управління певним об'єктом енергетики або ЕК в цілому. За допомогою шкідливого програмного забезпечення кіберзловмисник може контролювати, а в окремих випадках, керувати частиною або всією АСУ. АСУ ОЕС має бути стійкою до кібервпливів та мати відповідну комплексну систему реагування на кібератаки.

У грудні 2015 року здійснені розосереджені синхронні кібератаки типу "розвинена стійка загроза" (Advanced Persistent Threat – APT) на АСУ енергосистемами компаній ПАТ "Прикарпаттяобленерго", "Чернівціобленерго" та "Київобленерго". Внаслідок кібератак виникли збої в роботі систем віддаленого доступу, протягом однієї-шести годин повністю або частково відключено понад 100 населених пунктів, вимкнено близько 60 підстанцій, в тому числі такі, від яких живляться стратегічні об'єкти, значна кількість користувачів залишилися без енергопостачання. Наслідки такої атаки можливо були здійснені з метою перевірки функціонування системи захисту енергокомпаній та системи реагування на критичні ситуації.

Кібератаки були комплексними та системно організованими, в ході яких було здійснено:

− попереднє зараження мереж за допомогою підроблених листів електронної пошти;

− захоплення управління АСУ з виконанням операцій вимикань на підстанціях;

− виведення з ладу елементів АСУ;

− видалення за допомогою утиліти KillDisk інформації на серверах та робочих станціях;

− атака на телефонну мережу кол-центрів, з метою забезпечення відмов в обслуговуванні знеструмлених абонентів.

Система управління виявилася уразливою до кібератак такого роду. Реагування на таку кібератаку не було своєчасним, система захисту не виконала свої функції.

У грудні 2016 року була проведена менш масштабна за наслідками кібератака енергокомпанії "Укренерго", яка призвела до виведення з ладу

підстанції “Північна” та знеструмлення північної частини м. Київ та прилеглих районів. Атака мала за мету “демонстрацію сили” та була частиною операції проти державних установ України.

Кібератаки проведені на енергетичні підприємства у 2015 році були не повною мірою самостійно організованими. В 2016 році дії стали більш оперативними, а шкідливе програмне забезпечення (ПЗ) “Crash Override” забезпечувало проведення спланованих атак на декілька «критичних точок» ЕК, передбачало самоорганізацію дій в процесі атак, було спроможним надсилати команди обладнанню енергетичної мережі щодо включення або відключення живлення. Що могло призвести до віяльного відключення електроенергії по всій державі.

У червні 2017 року зловмисниками проведена масштабна деструктивна хакерська атака, яка була спрямована на порушення роботи web-сайтів компаній та на систему клієнтської підтримки, яка отримала назву “Petya”. Під деструктивним впливом опинились й “критичні точки” енергетичної галузі України. У травні 2018 року фахівці компанії Cisco повідомили про зараження більш ніж 500000 маршрутизаторів та роутерів у 54 державах. Для проведення такої атаки було використане деструктивне шкідливе ПЗ “VPNFilter”, що дозволило зловмисникам здійснювати моніторинг протоколів Modbus, які використовуються в АСУ системи диспетчерського управління (СДУ) і збору даних (Supervisory Control And Data Acquisition, SCADA), перехоплювати весь трафік, що проходить через уражений пристрій, збирати інформацію (включно дані авторизації та персональні дані платіжних систем), віддалено керувати інфікованим пристроєм та виводити його з ладу.

На фоні довготривалої політичної кризи у Венесуелі 7 березня 2019 року, внаслідок кібератак на АСУ СДУ гідроелектростанції “Ель-Гурі”, відбулася аварія, що спричинила широкомасштабне відключення електрики. Без енергопостачання залишилися 23 з 25 штатів, або 80% території країни. а також її столиця – Каракас. Системи управління енергопостачанням розбалансовані. У столиці обмежена подача води, виникли проблеми з каналізацією, магазини зачинені або працюють в умовах обмежень, гостро не вистачає продовольства та медикаментів. Платіжні банківські системи не працюють, телекомунікації, зокрема мобільний зв'язок, порушені. Припинив роботу міжнародний аеропорт Майкетія, знеструмлені лінії метро. За три місяці у лікарнях Венесуели з причин пов’язаних із відсутністю електрики померло 79 осіб. Уряд закликав до жорсткої економії пального. Жителі декількох районів Каракаса вийшли на вулиці, вимагаючи від влади відновити електропостачання. У країні проходять масові протести опозиції і зіткнення з поліцією. 10 березня 2019 року тимчасовий президент Венесуели Х. Гуайдо, який є головою парламенту країни – Національної асамблеї, запропонував оголосити надзвичайний стан у зв'язку з масштабними відключеннями електроенергії, що дозволяє запросити міжнародної допомоги, та закликав військових країни перейти на бік опозиції. Уряд США ввів санкції проти посадовців урядових силових структур, під керівництвом яких здійснювалися акції насильства та спалення гуманітарних

вантажів продовольства та медикаментів, а також проти 35 нафтових танкерів декількох кампаній, в тому числі найбільшого державного нафтового концерну PDVSA [64-66].

Основні особливості APT-атак:

− спрямованість на елементи критичної інфраструктури;

− проведення групою висококваліфікованих зловмисників «хакерів»;

− залишення невідомими (невиявленими) протягом тривалого часу;

− ретельне маскування з використанням спеціально розроблених програмних засобів (спеціалізовані Shell-коди, RootKit та ін.);

− належність до розвідувально-підривних операцій і підкріплення розвідувальними або руйнівними акціями [67].

Отже, автоматизовані системи управління енергетичними комплексами є уразливими перед кібератаками. В результаті проведеного аналізу виокремлюються категорії можливих кібератак, які можуть бути спрямовані на:

− елементи систем управління, наприклад віддалені термінали зв'язку з об'єктом (Remote Terminal Unit), або людино-машинного інтерфейсу (Human Machine Interface – ЛМІ), які зазвичай мають можливість віддаленого налаштування або управління;

− протоколи передачі даних, які добре задокументовані та їх опис знаходиться у відкритому доступі.

Через віддалений доступ зловмисник може перехопити управління системою та спричинити повне або часткове виведення елементів системи з ладу; пошкодити обладнання, внести зміни в інформацію та передані оператору дані. Що може призвести до значних матеріальних та фінансових витрат через пошкодження обладнання, вимкнення ліній електропередач, аварії під час роботи працівників, перевиробництво електричної енергії, перенавантаження систем тощо.

Кіберзагрози у воєнній сфері

Характер загроз у воєнній сфері у сучасних умовах набуває кардинальних змін. Нині до загроз у воєнній сфері воєнні аналітики починають відносити ті загрози, яким ще кілька років тому навіть не приділялася увага, оскільки вони були настільки маловірогідними, що їх плив на воєнну безпеку навіть не брався до уваги. Не в останню чергу це пов'язано з тими змінами, які відбуваються у способах та формах збройної боротьби сучасності та використовуваних при цьому засобах реалізації воєнних загроз. Також на зміну характеру воєнних загроз впливають процеси трансформації, які відбуваються у Збройних Силах та воєнізованих угрупованнях протиборчих сторін і які, останнім часом, зміщуються у бік високотехнологічності озброєнь військ (сил). Сучасні загрози у воєнній сфері набувають комплексного характеру. Поступово набуває умовного характеру поділ загроз на воєнні та не воєнні, оскільки останні, за певних умов, можуть бути легко трансформовані у воєнні.

Прояв кіберзагроз у воєнній сфері у мирний час не завжди має тісний зв'язок з початком військових приготувань протиборчою стороною до воєнних

дій. Спровокувати виникнення джерел кіберзагроз у воєнній сфері можуть найрізноманітніші явища та процеси й не завжди такі, що несуть воєнні ознаки. Наприклад, до таких джерел виникнення кіберзагроз воєнній сфері можна віднести:

− розробку, застосування та нарощування у світі потенціалу кіберозброєння;

− протиріччя, що виникають між державами на економічному, соціальному, етнічному, політичному або релігійному підґрунті;

− наявність і розгортання високотехнологічних армій та високотехнологічного оснащення Сектору безпеки і оборони держав, у тому числі й нарощування сил та засобів кібервійськ;

− загроза виникнення техногенних катастроф на об'єктах з критичною інформаційною інфраструктурою, у тому числі і військових, у результаті цілеспрямованих кібервпливів тощо.

До головних ознак існування кіберзагроз у воєнній сфері можна віднести такі:

− наявність на регіональному та міжнародному рівні гострих протиріч у різних сферах, розв'язання яких можливе, але не доцільне лише із застосуванням воєнної сили;

− наявність в однієї з протиборчих сторін зразків кіберзброї, а також відповідних сил і засобів для розв'язання протиріч, що існують безпосередньо з використанням елементів кіберпростору;

− відсутність політичної волі у керівництва держави для створення армії нового зразка, у якій не останню роль відіграватимуть підрозділи з кібербезпеки, а також на застосування такої армії й визначених підрозділів за призначенням у разі загрози виникнення та подальшої ескалації збройного конфлікту;

− сприятливі геополітичні умови й реальна (або прогнозована) військово-політична обстановка для реалізації кібервпливів.

Перелік існуючих та прогнозованих кіберзагроз у воєнній сфері на сьогодні ще не сформований повною мірою. Інколи, помилково, він збігається до однієї сутності – кіберзагроза і є загрозою воєнній сфері. Таким чином, зважаючи на відсутність подібного переліку, спираючись на положення Стратегії кібербезпеки та Закону України "Про основні засади забезпечення кібербезпеки України", сформуємо перелік основних кіберзагроз національній безпеці у воєнній сфері. До них можна віднести такі кіберзагрози, як:

− загроза поширення кіберзброї та технологій її виготовлення;

− загроза, яка проявляється у недостатній ефективності існуючих структур і механізмів забезпечення міжнародної кібербезпеки та глобальної й регіональної стабільності;

− загроза пов'язана з примусовим втягуванням держав в інформаційні війни та конфлікти, що призведуть до загострення протистояння в кіберпросторі між державами;

− нарощування іншими державами угруповань кібервійськ та кіберозброєння, які порушують співвідношення й розстановку сил у світі, що склалося;

− загроза прихованому управлінню військами та зброєю;

− загрози зриву процесів управління між військово-політичним керівництвом держави та збройними силами тощо.

Слід визнати, що даний перелік кіберзагроз не є повним, він достатньою мірою віддзеркалює вплив кіберзагроз на воєнну сферу. Наданий перелік основних кіберзагроз дозволяє умовно поділити наявні кіберзагрози на кіберзагрози зовнішнього та внутрішнього характеру.

До кіберзагроз зовнішнього характеру у воєнній сфері можна віднести:

− усі види розвідувальної діяльності з використанням усіх наявних технічних засобів розвідки, у тому числі й агентурної, спрямованої на викриття процесів управління, які протікають в кібернетичних системах протиборчої сторони, що спрямовані проти інтересів держави у воєнній сфері;

− сторонні кібервпливи на кібернетичні системи задіяні у забезпеченні воєнної безпеки держави;

− сторонні кібервпливи на особовий та керівний склад Збройних Сил та воєнно-політичне керівництво держави з боку інших країн;

− діяльність іноземних політичних, економічних і воєнних структур та міжнародних організацій спрямована проти державних інтересів у воєнній сфері.

Основними внутрішніми кіберзагрозами у воєнній сфері можуть бути загрози спрямовані на:

− порушення військовими частинами, установами Збройних Сил та підприємствами оборонного комплексу встановленого національним законодавством порядку обміну інформацією з обмеженим доступом у сфері оборони;

− вчинення навмисних, а також помилкових дій обслуговуючим персоналом при обслуговуванні систем спеціального призначення;

− організацію ненадійного функціонування інформаційних і телекомунікаційних систем спеціального призначення, яка виникає внаслідок цілеспрямованого та випадкового порушення процесів управління в таких системах;

− здійснення внутрішніх кібервпливів у вигляді акцій та окремих операцій тощо, що підривають престиж Збройних Сил та їх боєготовність.

Розглянувши основні внутрішні та зовнішній кіберзагрози у воєнній сфері, можна стверджувати, що основними об’єктами кібербезпеки у воєнній сфері мають бути:

− інформаційна інфраструктура центральних органів воєнного управління та органів воєнного управління видів Збройних Сил, об’єднань, з’єднань, військових частин і організацій, які входять до складу Збройних Сил, навчальних закладів, науково-дослідних установ, приватних компаній та організацій, які працюють в інтересах воєнної сфери;

− інформаційні ресурси підприємств оборонного комплексу і науково-дослідних установ, приватних компаній та організацій, які займаються оборонною проблематикою;

− програмно-технічні засоби та інформаційні ресурси автоматизованих і автоматичних систем управління військами й зброєю, озброєння і військової техніки, оснащених засобами інформатизації;

− особовий та керівний склад Збройних Сил, а також воєнно-політичне керівництво держави та представники приватного сектору, які займаються оборонною проблематикою.

Протидія кіберзагрозам у воєнній сфері може здійснюватися за такими напрямами:

− створення несприятливих умов щодо поширення та застосування кіберзброї шляхом запровадження міжнародних нормативно-правових регуляторів, які на відкритій основі забезпечують контроль за станом кібернетичних озброєнь;

− ужиття усіх можливих засобів та заходів, що виключають можливість втягування держави в інформаційні війни та конфлікти;

− підтримання належного рівня забезпечення Збройних Сил та інших військових формувань засобами кіберзахисту;

− підтримання високого ступеня боєздатності Збройних Сил та боєготовності спеціальних підрозділів тощо.

Серед основних факторів, що підвищують рівень кіберзагроз у воєнній сфері можна віднести такі:

− технологічний розрив між Збройними Силами держав з різним рівнем розвитку, який і надалі загострюється за рахунок нарощування бойових можливостей Збройних Сил розвинених держав при створенні нових зразків кіберозброєння та військової техніки, що ґрунтуються на нових принципах дії;

− зміщення традиційних сфер збройного протистояння в кіберпростір, для якого відсутні офіційно закріплені норми та принципи міжнародного права;

− критично низький рівень оперативної і бойової готовності Збройних Сил до ведення збройної боротьби у кіберпросторі.

Очевидно, що означенні вище фактори загострюватимуться й надалі та визначатимуть характер кіберзагроз у воєнній сфері і в найближчому майбутньому [13].

1.4. Дії у кіберпросторі та їх особливості

1.4.1. Сутність, цілі та задачі кібердій

До останнього часу вважалось, що бойові дії ведуться в чотирьох проекціях простору: на суші, на морі, в повітрі і в космосі. При цьому, інформаційні технології відігравали допоміжну роль: зв’язок, автоматизація управління, облік тощо.

Однак у сучасних умовах вже можна говорити про перенесення значної частки бойових дій безпосередньо в кіберпростір, тобто він вже може розглядатись як окремий простір ведення бойових дій. Його винятковість пов'язана з тим, що він єдиний з усіх п'яти наразі опанованих людиною просторів є екстериторіальним, адже практично позбавлений географічних обмежень. При цьому, залежність сучасної людини від кіберпростору є лише трохи меншою, ніж від інших. Саме від кіберпростору, від його стану, функціональності, передбачуваності та прогнозованості залежить стабільність світової економіки, безпека людей, всезагальне зростання добробуту, суспільний розвиток.

Кібердії, як специфічний вид протиборства, можна охарактеризувати такими особливостями:

− кібердії відбуваються у кіберпросторі, який вже сьогодні віднесений до нового театру воєнних дій поряд з космічним, морським, повітряним та наземним театрами;

− кібердії в переважній більшості мають асиметричний характер (наприклад, держава з достатньо малими за чисельністю Збройними Силами спроможна нанести серйозних втрат державі чисельність Збройних Сил у якій є значно більшою);

− наслідки від дій в кіберпросторі або безпосередньо, або опосередковано впливають на процеси глобалізації, що відбуваються у світі (економіку, фінанси, зброю та системи управління озброєнням, промисловість тощо);

− кібердії впливають на когнітивні та емоціональні процеси у соціумі, на адекватність сприйняття та правильність оцінювання ним подій, що відбуваються, та якість рішень, які ним приймаються;

− кібердії не мають єдиної загальноприйнятої стратегії та характеризуються великим ступенем невизначеності щодо задач, місця та часу їх проведення;

− на практиці досить складно розпізнавати факти здійснення кібердій цілеспрямованого або випадкового характеру;

− ведення дій у кіберпросторі потребує створення, впровадження та супроводження дієвої системи кібербезпеки. Ключовими елементами такої системи мають бути сили та засоби кіберрозвідки, захисту та впливу, які за сферами відповідальності об'єднується під егідою єдиного державного міжвідомчого координуючого органу із широким залученням громадськості, бізнесу, освітньої та наукової компонент тощо;

− кібердії обмежуються границями кіберпростору, але не обмежуються географічними та часовими рамками;

− кібердії на відміну від інших видів воєнних дій здійснюються протиборчими сторонами приховано та мають високий ступінь анонімності;

− джерело кібердій, як правило, складно піддається аналізу та виявленню;

− кібердії ґрунтуються на методології комплексного застосування усіх наявних сил та засобів, а також сил та засобів їх забезпечення або пов'язаних з їх застосуванням.

Успішне досягнення цілей кібердій та якісне вирішення задач, що стоять перед ними, безпосередньо пов'язані з чітким усвідомленням їх суб'єктами

усього спектра з виконання необхідних та достатніх умов для їх успішного здійснення. Саме тому у ході кібердій їх цілі та задачі, форми та способи здійснення можуть варіювати та носити різносторонній характер. Наприклад:

− розвідувальна форма кібердій має на меті добування усіма наявними засобами відомостей про процеси управління у воєнній, економічній, політичній, культурній та інших сферах діяльності суспільства та держави протиборчої сторони;

− кібердії набувають руйнуючої форми у випадку переслідування мети спрямованої на знищення, придушення або видозмінення з їх використанням процесів управління у кібернетичних системах протиборчої сторони, що можуть призвести до виведення з ладу її об'єктів з критичною інформаційною інфраструктурою частково або в цілому.

Цілі та задачі кібердій можуть полягати у:

− паралізації або взятті під контроль в найкоротші терміни об'єктів з критичною інформаційною інфраструктурою протиборчої сторони та його основних сил і засобів без нанесення фатальних втрат промисловості та території;

− дезорганізації функціонування органів державної влади та органів військового управління протиборчої сторони, об'єктів з критичною інформаційною інфраструктурою військового (стратегічних ядерних сил, систем попередження про ракетний напад, систем контролю космічного простору тощо), цивільного (атомної енергетики, хімічної та нафтопереробної промисловості тощо), подвійного призначення (об'єктів зі зберігання відходів ядерної та хімічної промисловості);

− перешкоджанні всіма наявними засобами нормальній роботі функціонування органів державної влади та органів військового управління протиборчої сторони;

− повному оволодінні стратегічною ініціативою, збереженні стійкого державного і військового управління своїх військ (сил);

− забезпеченні переваги на землі, морі, повітрі, космосі та в кіберпросторі;

− досягненні інформаційної переваги над протиборчою стороною шляхом реалізації кібервпливів на інформацію управління та команди управління інформаційними системами з одночасним захистом власної критичної інформаційної інфраструктури від аналогічних дій.

1.4.2. Класифікація форм і способів кібердій

Входження людства в епоху високотехнологічного суспільства обумовлює значні зміни в характері і в способах ведення збройної боротьби сучасності. Використання та контроль кіберпростору в національних інтересах потребує докорінного перегляду військових доктрин та стратегій застосування Збройних сил. У світі у низці держав, наприклад США, Франції, Естонії, Німеччині, Великобританії та ін., здійснюються спроби формування нової теорії збройної боротьби – теорії ведення бойових дій в кіберпросторі. Створення такої теорії неодмінно призведе до змін у військовому мистецтві.

Нік Харві, міністр збройних сил Великобританії, в інтерв'ю газеті "The Guardian" 31.05.2001 р. заявив: "Cyber weapons 'now integral part of Britain's armoury'". Також він сказав, що: "Кібердії стануть частиною бойовищ майбутнього, що проводитимуться паралельно з більш традиційними морськими, наземними та повітряно-космічними операціями. Кіберзброя стане невід'ємною частиною арсеналу держави".

Дії в кіберпросторі на сьогодні ще не набули визначеної в класичному розумінні форми збройної боротьби. Поряд з тим, зважаючи на останні збройні конфлікти та локальні війни, в яких мало місце протиборство в кіберпросторі, можна виділити такі форми ведення кібердій: кіберакції, кіберзаходи, кібероперації та кіберкампанії.

Отже, визначення поняття "кібератака" відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" має наступне тлумачення:

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби й обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Кібероперація – це скоординована й узгоджена за масштабом, місцем і часом паралельна або послідовна кібердія розвідувального, оборонного та (або) наступального характеру, яка має на меті завоювання переваги в кіберпросторі за рахунок нанесення збитків суб'єктам та об'єктам з критичною інформаційною інфраструктурою протиборчої сторони та захисту власних кібернетичних систем від аналогічних дій у відповідь [13].

При цьому така категорія, як кібервійна більшістю військових експертів нівелюється. Наприклад, у "Концептуальному плані розвитку можливостей сухопутних військ з ведення кібероперацій в кіберпросторі на період з 2016 по 2028 роки", опублікованому у 2010 році Командуванням навчально-наукового центру з розбудови сухопутних військ США, вона підміняється категорією "бойова операція в кіберпросторі" (Cyber Warfare Operations). Але, якщо не виключати ймовірність виникнення такого явища у майбутньому, то у першому наближенні можна запропонувати наступне трактування категорії кібервійна.

Кібервійна – це складне суспільно-політичне явище, що протікає у вигляді конфлікту в кіберпросторі між протиборчими сторонами (державами, коаліціями держав тощо) з використанням кібернетичних систем.

У найближчому майбутньому кібервійна може бути окремою й самостійною частиною широкомасштабних бойових дій із застосуванням

наземної, повітряної, космічної та морської компонент. Під веденням бойових дій в кіберпросторі слід розуміти кібердії, що здійснюються з метою забезпечення дій командувань на різних театрах воєнних дій.

Згідно з системою форм кібердій можна виділити три базові форми протистояння в кіберпросторі: розвідувальна, оборонна та наступальна, також можуть мати подвійне призначення.

Основною формою дій у кіберпросторі прийнято вважати кібероперації.

Розглянемо базові формі відповідно до кібероперації.

Розвідувальна кібероперація – це вид кібердій у кіберпросторі, що передбачає цілеспрямований процес добування даних, а також інформації про управління в кібернетичних системах протиборчої сторони. Процес добування даних, що становлять інтерес, їх аналіз та інтерпретація спрямовані на виявлення організаторами кібероперації уразливих місць протиборчої сторони та знаходження точок прикладання основних зусиль.

Добування інформації про кіберзагрози власним кібернетичним системам являє собою найбільш важливу проблему для розвідувального співтовариства. Розвідка у кіберпросторі, або кіберрозвідка використовує нові джерела, форми і способи добування даних, нові технології і технологічні прийоми. Проблемним питанням при організації розвідувальних кібероперацій залишається якісне укриття слідів на зворотному шляху доставляння розвідувальних даних. Дана обставина свідчить про те, що: по-перше, докорінного перегляду потребує усталена роками розвідувальна інфраструктура будь-якої держави світу; по-друге, розробленню підлягають нові форми і способи здійснення розвідувальних кібердій; по-третє, удосконалення потребують розвідувальні засоби та технології.

Оборонна операція в кіберпросторі – це кібердії з боку держави, спрямовані на застосування нею наявних кіберзасобів в інтересах захисту власних кібернетичних систем та процесів управління, які в них протікають, від кібердій з боку протиборчої сторони. Оборонна кібероперація ґрунтується на комплексному застосуванні можливостей власної системи кіберозброєння з метою своєчасного виявлення, відслідковування, аналізу, припинення та протидії кібервпливам протиборчої сторони, спрямованим на критичну інформаційну інфраструктуру держави. При формуванні оборонної стратегії кібероперації обов’язковому урахуванню підлягає порядок проведення процедур та заходів, спрямованих на мінімізацію наслідків кібердій протиборчої сторони.

Наступальна кібероперація – це форма ведення кібердій в кіберпросторі. Такі дії, як правило, спрямовуються на викривлення, блокування, знищення інформації управління та інші дії з інформацією та процесами управління, що циркулюють в кібернетичних системах протиборчої сторони.

Кількість кібероперацій, що проведено у світі до сьогоднішнього дня, є достеменно невідомою. З відкритих джерел принаймні відомо три кібероперації, які отримали світовий резонанс та піддалися ґрунтованому

науковому дослідженню з боку військових експертів. Це: розвідувально-наступальна кібероперація “Олімпійські ігри”, організована спецслужбами та представниками Збройних Сил США та Ізраїлю за підтримки відповідних урядів; розвідувальна кібероперація “Червоний жовтень” (державна належність та виконавець невстановлені); розвідувальна кібероперація “Мережний мандрівник” (державна належність та виконавець невстановлені).

Довідково.

Кібероперація “Олімпійські ігри” ініційована адміністрацією 43-го Президента США (Д. Буша) та підтримана його наступником Б. Обамою мала на меті знищення або досягнення суттєвого стримування іранської ядерної програми, а також недопущення ескалації збройного конфлікту на Близькому Сході між Ізраїлем та Іраном. Інструментом досягнення мети в кібероперації виступила кіберзброя Stuxnet та Flame.

Кібероперація “Червоний жовтень” мала на меті незаконне отримання та передавання інформації, що становить державну таємницю, а також добування конфіденційної інформації з баз даних приватних мереж та мобільних засобів. Серед держав, що найбільш підпали під цілі даної кібероперації, були переважно держави в минулому СРСР (Україна, Росія, Білорусь та ін), а також держави Східної Європи (Словакія, Угорщина Молдова, Чехія та ін).

Кібероперація “Мережний мандрівник” (“NetTrave/et або інші назви “Travnef, “Netfile”) проводилася з метою незаконного добування інформації про стан аерокосмічних досліджень, нанотехнологій, лазерної фізики, досліджень у галузі ядерної фізики, медичної справи, нафтопереробних та телекомунікаційних компаній 40 країн світу. Серед країн, які стали ціллю даної кібероперації були США, РФ, Україна, Канада, Монголія, Індія, Іспанія, Німеччина, Японія, Іран та ін.

Кібероперації можуть бути: тактичними, стратегічними, легальними та спеціальними.

Тактичні кібероперації здійснюються з метою демонстрації протиборчій стороні уразливостей її критичної інформаційної інфраструктури від сторонніх кібервпливів, що призводить до деморалізації населення та особового складу Збройних сил, нав’язування їм ідеї явної переваги протиборчої сторони і неминучої поразки у звичайній війні, у разі її початку.

Під час тактичних кібероперацій вирішуються такі основні задачі:

− ускладнення або вибіркова зупинка діяльності засобів телекомунікацій телекомпаній, операторів стільникового зв’язку, провайдерів Інтернету, відомчих мереж тощо;

− тимчасова зупинка або ускладнення діяльності систем управління життєзабезпеченням населення та Збройних Сил та порушення діяльності систем управління банківської та фінансової сфер. Прикладом тактичної кібероперації може бути естонський кіберінцидент у 2007 році.

Стратегічні кібероперації здійснюються з метою нанесення реальних збитків протиборчій стороні, які проявляються у руйнуванні системи

управління органів державної влади, системи управління національною економікою, а також створенні передумов до виникнення техногенних аварій та катастроф, що можуть призвести до появи значної кількості жертв серед особового складу збройних сил та мирного населення.

Під час стратегічних кібероперацій вирішуються такі основні задачі:

− злам та розкрадання найважливіших державних кодів і алгоритмів шифрування, паролів та кодів доступу, перехоплення переговорів перших осіб держави;

− проникнення у системи управління критичною інформаційною інфраструктурою, інформаційні системи різного цільового призначення та державні бази даних;

− розкрадання, навмисне спотворення або знищення інформації в базах даних спецслужб, силових міністерств та відомств, органів державної влади, центрального банку тощо;

− пошкодження завантажувальних програм (біосів) мікропроцесорів комп'ютерів і знищення баз даних операторів стільникового зв'язку, провайдерів Інтернету, відомчих комп'ютерних мереж, комп'ютерних мереж військового призначення, систем управління життєзабезпеченням, що призводить до можливості виникнення серії великих техногенних аварій та катастроф на об'єктах з критичною інформаційною інфраструктурою (атомних електростанціях, підприємствах хімічної-, нафто- і газопереробних галузей тощо). *Прикладом* стратегічної кібероперації може бути кіберінцидент з мережевим хробаком "Stuxnet" на Бушерській АЕС в Ірані.

Легальні кібероперації здійснюються представниками спецслужб з метою прихованого впливу на політику держави протиборчої сторони. Вони проводяться за такими основними напрямами:

− кібервплив на представників органів державної влади;

− кібервплив на населення;

− кібервплив на економічні та фінансові процеси в державі.

Кібервплив на представників органів державної влади проявляється в інформаційному терорі (компрометації, залякуванні, введенні в оману), який спрямовується проти патріотично налаштованих національних лідерів, їх найближчого оточення, родичів, друзів тощо та в інформаційній підтримці "агентів впливу" шляхом створення їх сприятливих умов для політичного зростання.

Кібервплив на населення здійснюється з метою формування негативної громадської думки проти органів управління державною владою, насамперед, силових структур, і патріотичних громадських організацій шляхом поширення компрометуючої інформації та панічних чуток.

Кібервплив на економічні та фінансові процеси в державі здійснюється приховано. По-перше, штучно стимулюється ажіотаж на ринку на речі першої необхідності. По-друге, приховано створюються такі умови, які у невигідному положенні для держави провокуватимуть коливання курсами валют, енергоносіїв тощо. Як правило, такий кібервплив під час легальної

кібероперації здійснюється через радіо і телевізійні супутникові або звичайні канали ЗМІ, а також електронну пошту, каналами стільникового зв'язку, соціальних мереж тощо.

Спеціальні кібероперації – це кібердії, що проводяться спеціальними підрозділами Збройних Сил з метою знищення стратегічних озброєнь протиборчої сторони.

Вони полягають у:

− прихованому проникненні у системи управління стратегічною зброєю з подальшим несанкціонованим її спрацюванням, що призводить до виникнення техногенних аварій та катастроф й знищення відповідної інфраструктури;

− блокування систем управління військами, передача у війська помилкових наказів і директив у найважливіші моменти бойових дій;

− дезорганізація орбітального угруповання протиборчої сторони (за його наявності);

− блокуванні запуску стратегічних ракет, зміні польотного завдання ракет шляхом їх перенацілювання на власні об'єкти з критичною інформаційною інфраструктурою або об'єкти іншої держави тощо.

Основні форми і способи кібердій:

1. Поширення спеціально підібраної інформації (дезінформації), в першу чергу, у соціальних Інтернет-сервісах. Її реалізація виявляється у такий спосіб:

− розсилка електронних листів;

− організація новинних груп;

− створення сайтів з елементами інтерактивної взаємодії їх відвідувачів (чати, on-line-голосування);

− розміщення інформації на приватних за змістом веб-ресурсах (блоги, соціальні мережі), в електронних версіях періодичних видань і мережевого мовлення (трансляції передач радіо- і телестанцій), або в мультимедійних архівах (Youtube) .

2. Повне або часткове наповнення інформаційних ресурсів шляхом підміни їх змісту, шляхом несанкціонованого доступу. З метою залучення уваги до суб'єкта кібервпливу та демонстрації своїх можливостей. Особлива роль при реалізації даної форми кібердій відводиться семантичним атакам, що полягають у проникненні до ресурсів сайта й подальшому непомітному розміщенні на них дезінформації. Подібним атакам піддаються найпопулярніші інформаційні сторінки, змісту яких користувачі цілком довіряють.

3. Створення "двійників" інформаційних ресурсів схожих на оригінальні – цілеспрямована реєстрація у пошукових системах, з метою перенаправлення (підміна) посилань на інші інформаційні ресурси протилежного змісту.

4. Зниження ефективності функціонування структурних елементів каналів передачі даних між елементами кібернетичних систем:

− "бомбардування" мережі електронними листами – "спам" ;

− DoS (DDoS)-атаки (атака типу "відмова в обслуговуванні");

− впровадження мережних комп'ютерних вірусів;

− розміщення інформації на приватних за змістом веб-ресурсах (блоги,

соціальні мережі), в електронних версіях періодичних видань і мережевого мовлення (трансляції передач радіо- і телестанцій), або в мультимедійних архівах (Youtube) .

5. Віддалене приховане управління ресурсами мережі:

− активація процесу прихованого управління здійснюється при використанні механізмів:

− “часових бомб” – за часом;

− “логічних бомб” – за діями, що безпосередньо здійснюються над операційною системою;

− “троянських коней” – за ключовими повідомленнями. Дозволяє створювати ботнет мережі.

6. Захист власних ресурсів – динамічний захист комп'ютерних систем та мереж від кібератак та захист соціуму від деструктивного контенту.

Динамічний захист від кібератак передбачає реалізацію процедур завчасного виявлення кіберзагроз ресурсам мережі й побудови відповідної моделі дій з урахуванням виявлених уразливостей та ужиття заходів (у тому числі й активних), спрямованих на забезпечення заданих показників захищеності. Сутність захисту від деструктивного контенту полягає в перекритті доступу до “небажаної” інформації.

Отже, до суб’єктів кібердій можна віднести:

− окремих громадян та осіб без громадянства, соціальні утворення або угруповання громадян, що мають на меті залякування суспільства, створення атмосфери напруженості з метою вирішення окремих політичних, релігійних, національних, економічних або соціальних проблем;

− держави або їх коаліції з економічними і політичними цілями.

Основними об’єктами кібердій при цьому можуть бути:

− кібернетичні системи державних урядових органів, фінансових установ, підприємств енергетичної галузі;

− системи управління повітряним рухом, рухом залізничного транспорту та підприємств критичних галузей промисловості;

− системи управління військами та зброєю;

− інші кібернетичні системи, які призначені для збирання, обробки, збереження та видачі інформації тощо, кібервпливи, які можуть призвести до порушення в них процесів управління;

− програмне та інформаційне забезпечення;

− програмно-апаратні, телекомунікаційні та інші засоби інформації та управління;

− канали зв’язку, що забезпечують циркуляцію інформаційних потоків між кібернетичними системами;

− інтелект людини та масова свідомість.

1.5. Система кібердій

У XXI столітті людство живе у той час, коли темпи науково-технічного прогресу досить динамічно змінюють усі сфери його життя. Зміни відбуваються практично в усьому – від техніки, до моральних цінностей суспільства. Цілком очевидним є факт того, що сьогодні відбувається безперервний процес адаптації людської цивілізації до власних високотехнологічних здобутків, які чинять на неї не тільки позитивний вплив, а й інколи мають негативні прояви, наслідки від яких мають планетарний характер.

Усвідомлюючи стратегічну важливість захисту від нових викликів та загроз, поява яких обумовлена високотехнологічними здобутками, в провідних країнах світу здійснюється активна робота щодо створення систем протидії таким викликам та загрозам. Наприклад, в США та ін. розвинених державах стрімкими темпами здійснюється підготовка збройних сил та приватного сектору до ведення кібероперацій, роль яких при досягненні воєнно-політичних цілей поставлених перед державою з часом тільки зростає. Інтенсивно удосконалюється категоріальний апарат у сфері боротьби в кіберпросторі, розробляється нова система боротьби в кіберпросторі – система кібердій.

Враховуючи ступінь розуміння ролі й місця кібербезпеки для України в системі національної безпеки, в державі вживається низка заходів з покращення ситуації, що склалася. На державному рівні здійснюються заходи спрямовані на усунення дефініційної невизначеності, здійснюються кроки спрямовані на налагодження належної координації між відповідними відомствами та приватним сектором та інші спеціальні заходи тощо. Але б яка б не була їх кількість, їх завжди буде недостатньо для створення ефективної системи кібербезпеки держави. Це пов’язано з низкою причин, однією з яких є відсутність в державі єдиної системи поглядів на систему кібердій в кіберпросторі, розробці якої і присвячено даний розділ.

Система кібердій – це сукупність взаємопов’язаних підсистем кіберрозвідки, кіберзахисту, кібервпливу та кіберконтррозвідки, які утворюють цілісну єдність, на яку покладаються функції із забезпечення кібербезпеки.

Метою системи кібердій є забезпечення стану кіберзахищеності.

1.5.1. Основи кіберрозвідки

Розвідка є однією з найдавніших професій. З плином часу змінювалися тільки способи та засоби її ведення. Нині розвідка перемістилася у новий вимір кіберпростір й посіла важливе місце у системі кібердій. При цьому, вона може виступати, як окремим їх видом, так і бути супроводжуючим елементом інших складових системи кібердій – кібервпливу та кіберзахисту.

Зростання ролі й місця кіберрозвідки обумовлено низкою факторів, серед яких основними можна вважати:

– постійне збільшення взаємозалежності між секторами та об’єктами з

критичною інформаційною інфраструктурою;

− постійне зростання кількості кіберзагроз кібернетичним системам управління різного рівня;

− поява принципово нових засобів і способів несанкціонованого доступу до інформації про процеси управління в кібернетичних системах тощо.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" під **кіберрозвідкою** розуміють діяльність, що здійснюється розвідувальними органами у кіберпросторі, або з його використанням.

У більш широкому сенсі під кіберрозвідкою слід розуміти таке визначення. **Кіберрозвідка –** процес добування усіма наявними технічними засобами розвідки (космічної, повітряної, радіоелектронної, мережної, програмно-комп'ютерної, розвідки систем управління тощо) й засобами розвідки з відкритих джерел (*OSINT*-розвідка) інформації наявної в кіберпросторі про протиборчу сторону та подальша її обробка, що здійснюються за єдиним задумом і планом з метою викриття процесів управління, які протікають в кібернетичних системах під час їх функціонування та формування вихідних даних для здійснення заходів кіберзахисту та кібервпливу на фізичні, соціальні, інформаційні та інші кібернетичні системи.

Або коротко, **кіберрозвідка** – сукупність заходів, спрямованих на забезпечення всебічної обізнаності щодо дій у кіберпросторі, або з його використанням.

До *основних функцій* кіберрозвідки можна віднести такі функції, як:

− постійний пошук і добування розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони, що становлять інтерес з використанням усіх наявних технічних засобів розвідки й засобів розвідки з відкритих джерел інформації з кіберпростору;

− обробка, узагальнення та аналіз добутої розвідувальної інформації;

− підготовка розвідувальної інформації на підставі проведеного аналізу для прийняття обґрунтованих управлінських рішень;

− формування вихідних даних для здійснення кібервпливу на кібернетичні системи протиборчої сторони;

− прогнозування можливих проявів кіберзагроз та їх наслідків.

Згрупувавши функції кіберрозвідки, можна виділити дві основні групи задач. Перша група задач – це задачі, що пов'язані з добуванням інформації; друга – це задачі прогнозування кіберзагроз.

Відповідно до масштабів і характеру розвідувальних завдань кіберрозвідка може бути стратегічною, оперативною та тактичною.

Стратегічна кіберрозвідка проводиться з метою підготовки та проведення стратегічних операцій та війни в цілому у "класичному розумінні" й кібероперацій та кіберкампаній у рамках системи кібердій. Стратегічною ціллю такого виду розвідки також є досягнення воєнної, політичної, промислової, технологічної та іншої переваги над протиборчою стороною за рахунок викриття процесів управління в кібернетичних системах протиборчої сторони.

Оперативна кіберрозвідка вирішує завдання розвідки в інтересах ведення спеціальних операцій в межах заданого операційного району.

Тактична кіберрозвідка здійснюється силами і засобами спеціальних підрозділів кіберрозвідки в інтересах успішного ведення кібердій у ході їх підготовки та безпосереднього ведення.

Кіберрозвідка має низку особливостей. Основними з них є такі:

− порівняно з іншими видами розвідки роль кіберрозвідки постійно зростає. При правильному підході до організації кіберрозвідки, а також раціональному застосуванні сил та засобів кіберрозвідки у мирний час можливо добувати від 35 до 95% інформації про об'єкти або суб'єкти, що становлять інтерес;

− добуваюча та обробляюча складові процесу кіберрозвідки мають взаємозалежний тісний зв'язок;

− підвищується роль знань на заключному етапі процесу кіберрозвідки, який на відміну від інших видів розвідки не завершується підготовкою розвідувальних даних для визначених органів. Заключний етап кіберрозвідки полягає у приведенні розвідувальних даних у вищий ступінь готовності до їх застосування у процесі прийняття управлінських рішень – у вигляді набутих знань;

− під час кіберрозвідки роль, місце та функції людини, як на етапі добування, так і на етапі обробки змінюються за рахунок зменшення об'єму працевитрат;

− сутність кіберрозвідки в основному зводиться на здійснення діяльності, спрямованої на досягнення або утримання переваги в кіберпросторі над протиборчою стороною;

− складність територіальної та державної ідентифікації належності суб'єкта або об'єкта кіберрозвідки, що суттєво ускладнює процес добування розвідувальної інформації та забезпечення її достовірності.

До кіберрозвідки висувається низка вимог системного характеру, таких як:

− підсистеми кіберрозвідки повинні мати розвинену інфраструктуру, що дозволить здійснювати постійний моніторинг процесів управління різної природи у системах управління різного цільового призначення та ієрархічної складності з метою досягнення синергетичного ефекту;

− підсистеми кіберрозвідки мають бути максимально автоматизованими, а звітні результати повинні подаватися у стандартизованій формі, яка доступна усім підсистемам;

− система кіберрозвідки повинна мати централізований банк даних для збереження розвідувальної інформації та добутих знань.

Кіберрозвідка включає три основні фази:

− організацію кіберрозвідки;

− ведення кіберрозвідки;

− інформаційна робота.

Організація кіберрозвідки передбачає визначення цілей і завдань розвідки, виділення необхідних сил і засобів, планування її заходів, постановку завдань виконавцям, організацію їх підготовки та інші питання. Ведення кіберрозвідки

має безпосередній зв’язок з добування розвідувальної інформації. Інформаційна робота являє собою збір, обробку розвідувальної інформації, її узагальнення та доведення до зацікавлених осіб.

Форми кіберрозвідки

Основними формами кіберрозвідки є:

− кіберрозвідка з використанням технічних засобів розвідки й засобів розвідки з відкритих джерел (*OSINT*-розвідка);

− агентурна кіберрозвідка (*HUMINT*-розвідка).

Кожна з визначених форм може бути як легальною, так і нелегальною.

Зв’язок між визначеними формами кіберрозвідки показано на рис. 1.12.

Кіберрозвідка з використанням технічних засобів розвідки – це одна з основних форм добування легальним та (або) нелегальним шляхом розвідувальної інформації з кіберпростору про процеси управління, які протікають в кібернетичних системах протиборчої сторони.

Рис.1.12. Форми кіберрозвідки та зв’язок між ними

Розвідка з відкритих джерел інформації (*OSINT*- розвідка) здійснюється з аналогічною метою, що й розвідка з використанням технічних засобів розвідки. Суттєвою відмінністю між ними лише є джерела розвідувальної інформації, для останньої якими є інформація з відкритих джерел.

Легальна кіберрозвідка – це вид діяльності, що ґрунтується на легальних способах добування розвідувальної інформації про процеси управління в кібернетичних системах й здійснюється в кіберпросторі уповноваженими органами з питань кібербезпеки.

Легальна кіберрозвідка має три основні форми добування розвідувальної інформації:

− законне придбання й аналіз усіх доступних джерел інформації;

− добування розвідувальної інформації на різного роду прийомах, зустрічах, конференціях, семінарах тощо;

− візуальне спостереження (фото-, відео-, аудіо-) та моніторінг кіберпростору з використанням технічних засобів розвідки (РЕР (*SIGINT*) тощо)).

Нелегальна кіберрозвідка здійснюється в кіберпросторі й ґрунтується на нелегальних способах збору розвідувальної інформації та здебільшого стосується добування розвідувальної інформації з обмеженим доступом, що охороняється державою або її власником.

Основними формами нелегальної кіберрозвідки є:

− копіювання, викрадання інформації з обмеженим доступом та (або) її носіїв, наприклад документації, презентацій, лептопів тощо;

− засилання та (або) проникнення агентів на об'єкти з критичною інформаційною інфраструктурою, що підлягають кіберрозвідці;

− прослуховування розмов суб'єкта кіберрозвідки.

Агентурна кіберрозвідка (*HUMINT*-розвідка) – це одна з форм добування інформації, що становить інтерес. Агентурна кіберрозвідка здійснюється за рахунок залучення людських ресурсів з обов'язковим використанням новітніх ІТ-рішень, у тому числі й інтегрованих у мережу Інтернет. Вона характеризується як усебічна й динамічна діяльність кіберагентів, спрямована на оперативний збір й передачу визначеним споживачам цільової інформації без її первинної обробки та аналізу. *Особливістю передачі визначеним споживачам цільової інформації є те, що вона передається відкритими каналами,* наприклад мережею Інтернет.

Праобразом агентурної кіберрозвідки можна вважати промисловий шпіонаж. Але агентурна кіберрозвідка, на відміну від останнього, суттєво відрізняється, як способами, так і засобами реалізації. Кіберагент, як правило, не є фаховим розвідником та не володіє специфічними навичками. Мережа кіберагентів не отримує прямих вказівок від своїх керуючих центів. Кіберагенти самостійно приймають рішення, які об'єкти та які суб'єкти мають бути розвідані.

Вперше ефективність агентурної кіберрозвідки на сучасному етапі її становлення оцінено під час проведення антитерористичної операції на сході України в 2014 році. Ведення агентурної кіберрозвідки проукраїнськими представниками суттєво сприяло ослабленню терористичних організацій та ліквідації її очільників.

Принципи кіберрозвідки

Роль та значимість кіберрозвідки для забезпечення кібербезпеки держави займає досить вагоме місце у системі національної безпеки. Наприклад, в США в межах свої компетенції для вирішення завдань кіберрозвідки задіяні усі 17 членів розвідувального співтовариства, які працюють, як окремо, так і сумісно.

Слід зауважити те, що основний акцент у здійсненні розвідувальних місій у кіберпросторі при цьому покладається на "Офіс операцій зі спеціалізованого доступу" (*ТАО* Агентства національної безпеки).

Останні збройні конфлікти та локальні війни також свідчать про те, що кіберрозвідка на сьогодні є найважливішим видом бойового забезпечення дій військ (сил), оскільки від якості виконання задач кіберрозвідки значною мірою залежить успіх виконання поставлених перед підрозділами і частинами завдань. Саме тому дотримання принципів кіберрозвідки має визначальну роль для забезпечення кібербезпеки, як для держави в цілому, так і для забезпечення дій її військ та сил зокрема.

Кіберрозвідка ґрунтується на низці *принципів*:

− цілеспрямованість;
− безперервність;
− активність;
− оперативність;
− скритність;
− достовірність;
− комплексне використання сил та засобів добування інформації.

Принцип *цілеспрямованості* кіберрозвідки полягає у веденні її за єдиним планом та задумом із зосередженням основних зусиль добуваючих органів на виконанні основних завдань по визначених об'єктах та суб'єктах розвідки.

Безперервність кіберрозвідки виявляється у постійному характері її ведення на який не впливають будь-які фактори, наприклад, погодні умови, час доби, пора року, оточуюча обстановка тощо.

Принцип *активності* кіберрозвідки зводиться до активного залучення усіх складових системи кіберрозвідки, задіяних у добуванні розвідувальної інформації, у пошуку найбільш дієвих методів та засобів її добування в умовах обстановки, що склалася. При зміні обстановки відповідно до даного принципу змінюються лише методи кіберрозвідки та засоби добування інформації.

Оперативність ведення кіберрозвідки передбачає її здатність у своєчасному добуванні розвідувальної інформації, її обробці та аналізі.

Скритність кіберрозвідки передбачає проведення розвідувальних заходів у таємниці від протиборчої сторони, що забезпечує безпеку, як добуваючих органів системи кіберрозвідки, так і прихованість фактів витоку інформації, що розвідується. Принцип скритності забезпечується вжиттям різних заходів, наприклад маскуванням, засекречуванням, легендуванням тощо.

Принцип *достовірності* кіберрозвідки полягає у добуванні нею такої інформації, обробка та аналіз якої забезпечують її правильне сприйняття.

Принцип *комплексування у використанні сил та засобів добування розвідувальної інформації* полягає у раціональному виборі та застосуванні тих способів та засобів добування розвідувальної інформації, які будуть найефективнішими у визначених умовах. Реалізація даного принципу забезпечує підвищення достовірності інформації, що добувається.

Добування розвідувальної інформації на основі описаних вище принципів може здійснюватися, як легальним, так і нелегальним шляхом. У першому випадку вивчається та обробляється уся інформація про об'єкт (суб'єкт) кіберрозвідки, що доступна з відкритих джерел – засобів масової інформації, періодичних фахових та публіцистичних видань, науково-дослідних робіт, матеріалів конференцій тощо. Вивчаються відкриті урядові джерела та звіти, угоди, доповіді тощо. У другому випадку використовуються різні методи та способи нелегального добування розвідувальної інформації – від агентурної до технічної.

Засоби і способи кіберрозвідки

Засоби кіберрозвідки поділяються на такі основні типи (рис. 1.13):

− технічні засоби;
− програмні засоби;
− апаратні засоби;
− програмно-апаратні засоби;
− засоби криптоаналізу;
− засоби кіберрозвідки з відкритих джерел (OSINT- засоби);
− засоби агентурної розвідки (HUMINT);
− засоби соціальної інженерії.

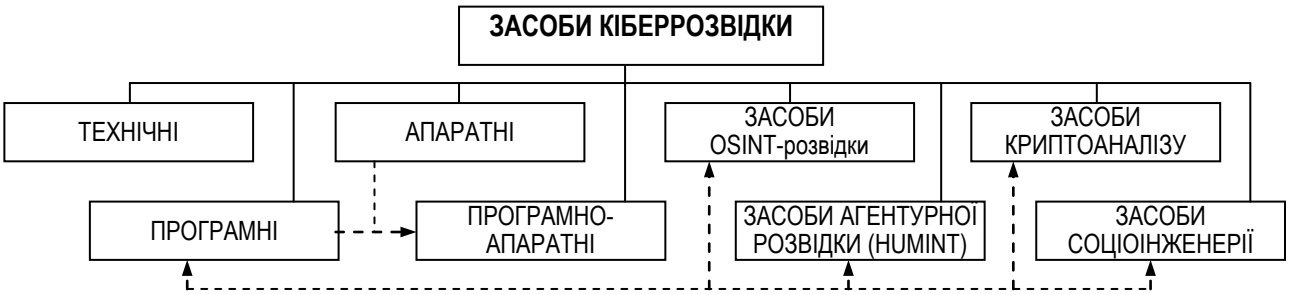

Рис. 1.13. Основні типи засобів кіберрозвідки та зв’язків між ними

Технічні засоби кіберрозвідки – це сукупність розвідувальної апаратури (апаратів, машин та виготовлених з їх використанням спеціалізованого обладнання або технічних засобів, інструментів, речовин тощо), що призначені для несанкціонованого отримання розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони шляхом контролю кіберпростору й окремих його складових, який здійснюється за рахунок приймання випромінювань різної природи, добування розвідувальної інформації з каналів зв’язку, інформаційно-телекомунікаційних систем та окремих технічних засобів оброблення інформації, подолання технічного і криптографічного захисту розвідувальної інформації, негласного спостереження за визначеними об’єктами, що становлять інтерес для розвідувальних органів як джерела розвідувальної інформації, а також забезпечення первинної обробки та передавання розвідувальної інформації визначеним споживачам.

Програмні засоби кіберрозвідки – це сукупність спеціалізованих програмних модулів, які створені з метою добування розвідувальної інформації з кіберпростору про процеси управління в кібернетичних системах протиборчої сторони.

Апаратні засоби кіберрозвідки – це сукупність спеціалізованих апаратних засобів, що забезпечують добування розвідувальної інформації шляхом дослідження апаратури, обладнання, модулів їх аналізу та випробування тощо, задіяних в управлінні кібернетичними системами протиборчої сторони з метою виявлення їх технічних характеристик та потенційних можливостей.

Програмно-апаратні засоби являють собою сукупність програмних та апаратних спеціалізованих засобів, призначення та функції яких випливають з основного призначення та функцій їх складових.

Засоби OSINT-розвідки – це сукупність, технічних, програмних, апаратних, програмно-апаратних та інших засобів, що використовуються підрозділами кіберрозвідки для добування розвідувальної інформації з відкритих та відносно відкритих джерел кіберпростору про процеси управління, що протікають у кібернетичних системах протиборчої сторони.

Засоби соціальної інженерії – засоби добування розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони, орієнтовані на її отримання від суб'єкта кіберрозвідки.

Дії розвідувальних органів з добування розвідувальних відомостей здійснюються різними способами. Під способом кіберрозвідки слід розуміти таке визначення.

Спосіб кіберрозвідки – це технологічний прийом (метод) застосування сил та засобів розвідки у цілях добування розвідувальної інформації про процеси управління в кібернетичній системі, що розвідується.

На прикладі програмних засобів кіберрозвідки розкриємо сутність відповідних способів. Так, до основних засобів кіберрозвідки можна віднести:

− засоби аналізу та подолання систем захисту;

− засоби добування розвідувальної інформації (пошукові системи) та спеціалізоване програмне забезпечення з пошуку визначеного контенту;

− комп'ютерні віруси, здатні розмножуватися, впроваджуватися в програми, передаватися за мережевими протоколами, виводити з ладу системи управління тощо;

− "троянські коні";

− засоби ведення віддалених атак;

− логічні бомби – програмні закладні пристрої, які заздалегідь впроваджують у інформаційно-керуючі центри військової або цивільної інфраструктури, щоб за сигналом або у встановлений час привести їх в дію.

Засоби аналізу та подолання систем захисту – це спеціалізовані програмні засоби та засоби подвійного призначення, що забезпечують здійснення процедур аналізу систем захисту об'єктів кіберрозвідки з подальшим їх несанкціонованим подоланням (вимкненням) або обходом відповідних механізмів захисту. Їх можна надати у вигляді двох базових груп (рис. 1.14):

1 група – засоби аналізу систем захисту;

2 група – засоби подолання систем захисту, які, у свою чергу, поділимо на чотири типи: засоби аналізу даних; засоби аналізу алгоритмів; засоби безпосереднього подолання систем захисту; засоби подолання в обхід системи захисту.

Зауважимо, що до спеціалізованих програмних засобів відносяться лише ті засоби, що призводять до відключення системи захисту (рис. 1.14) їх виділено чорним кольором, решта, – а їх більшість, мають подвійне призначення.

Рис. 1.14. Базові групи програмних засобів аналізу та подолання систем захисту

Розглянемо більш ґрунтовно спеціалізовані програмні засоби відключення систем захисту.

Засоби редагування ресурсів об’єктних модулів (*Resource Editors*) використовуються для редагування текстових, діалогових, графічних, аудіо-, відео- та ін. ресурсів, що знаходяться в області даних об’єктних модулів програмного забезпе- чення. Модифікація визначених ресурсів дозволяє відключати систему захисту.

Засоби генерації паролів та ключів (*Key Generators*), що відносяться до четвертого типу засобів подолання в обхід систем захисту, використовуються з метою генерації ключових послідовностей, що задовольняють критеріям алгоритмів, які використовуються у відповідних системах. Даний тип засобів забезпечує подолання парольних систем захисту, а також систем захисту з електронними ключами та ключовими файлами.

Серед *засобів добування розвідувальної інформації та спеціалізованого програмного забезпечення з пошуку визначеного контенту,* особлива роль відводиться пошуковим системам. Основними засобами пошуку такої інформації виступають інформаційні пошукові системи. Найбільш поширеними у світі із них є такі, як *Google* (46,2%), *Yahoo* (22,5%), *msn* (12,6%), *AOL* (5,4%), *My Way* (2,2%), *Netscape* (1,6%) та ін. (7,9%).

Спеціалізоване програмне забезпечення інформаційно-аналітичних систем призначене для пошуку в кіберпросторі інформації визначеного змісту. Основні труднощі при створенні засобів контент-моніторингу з відповідним спеціалізованим програмним забезпеченням виникають на етапі практичної реалізації змістовної частини операцій загального алгоритму роботи.

Місце контент-моніторингу у системі забезпечення кібербезпеки держави можна надати у вигляді об’ємно-просторової моделі (рис. 1.15).

Рис. 1.15. Об’ємно-просторова модель контент-моніторингу в системі забезпечення кібербезпеки

Показана на рис. 1.15 об’ємно-просторова модель в процесі кіберрозвідки дозволяє встановити зв’язки між суб’єктами та об’єктами кібербезпеки та забезпечує оцінювання рівня небезпек. Модель також дозволяє оцінювати рівень кіберзагроз на основі аналізу інформації з відкритих джерел та джерел з обмеженим доступом. Стратегія кібербезпеки визначає основні завдання, сфери та суб’єкти боротьби в кіберпросторі.

Суб’єкти протиборства у ході своєї діяльності взаємодіють із об’єктами матеріального світу (іншими суб’єктами), створюючи тим самим передумови для появи інформаційних повідомлень. Повідомлення у вигляді інформаційних документів знаходять своє відображення в ресурсах кібернетичних систем, які доступні абонентам даної системи, залежно від рівня їх повноважень. Контент-моніторинг кіберпростору в інтересах кіберрозвідки у рамках національних інтересів передбачає безперервний процес вивчення динаміки зміни кількісних та якісних характеристик повідомлень за визначеною тематикою. Аналітична обробка сукупності повідомлень дозволяє оцінити наявні загрози кібербезпеці та сформувати їх у вигляді звітів, що описують стан справ за визначеною тематикою. Дані звіти є підґрунтям для прийняття управлінських рішень суб’єктами забезпечення кібербезпеки (уповноваженими органами) формування та коригування стратегії кіберзахисту.

Застосування технології контент-моніторингу в інтересах кіберрозвідки також дозволяє забезпечувати своєчасне виявлення небезпек та встановлення рівня загроз кібербезпеці. Якісне вирішення цієї задачі передбачає побудову структури системи контент-моніторингу у вигляді підсистем, які реалізують триетапну обробку розвідувальної інформації, що включає у себе первинну, попередню та вторинну обробки (рис. 1.16).

Підсистема кіберрозвідки при первинній обробці складається з двох підсистем: підсистеми кіберрозвідки за попередньо визначеними ресурсами та підсистеми забезпечення пошуку за цільовими напрямами.

Завданням підсистеми кіберрозвідки при первинній обробці є отримання з кіберпростору даних з різних джерел та оцінювання їх інформативності. У свою чергу, підсистема кіберрозвідки для вирішення таких завдань повинна складатися з декількох груп кіберрозвідки з автоматизованими робочими місцями (АРМ). Група кіберрозвідки з АРМ за визначеними ресурсами забезпечує отримання даних з попередньо визначеного переліку джерел інформації.

Таке завдання кожною з груп вирішується за допомогою сукупності наявних у неї засобів кіберрозвідки (технічних, програмних тощо), які забезпечують доступ до визначених ресурсів.

1.5.2. Основи кіберзахисту

Невід’ємною складовою системи кібердій є підсистема кіберзахисту, призначена для реалізації заходів із забезпечення кібербезпеки. При цьому, категорія “кіберзахист” у даному випадку уживається виходячи з такого її тлумачення, яке подано в Законі України “Про основні засади забезпечення кібербезпеки України”.

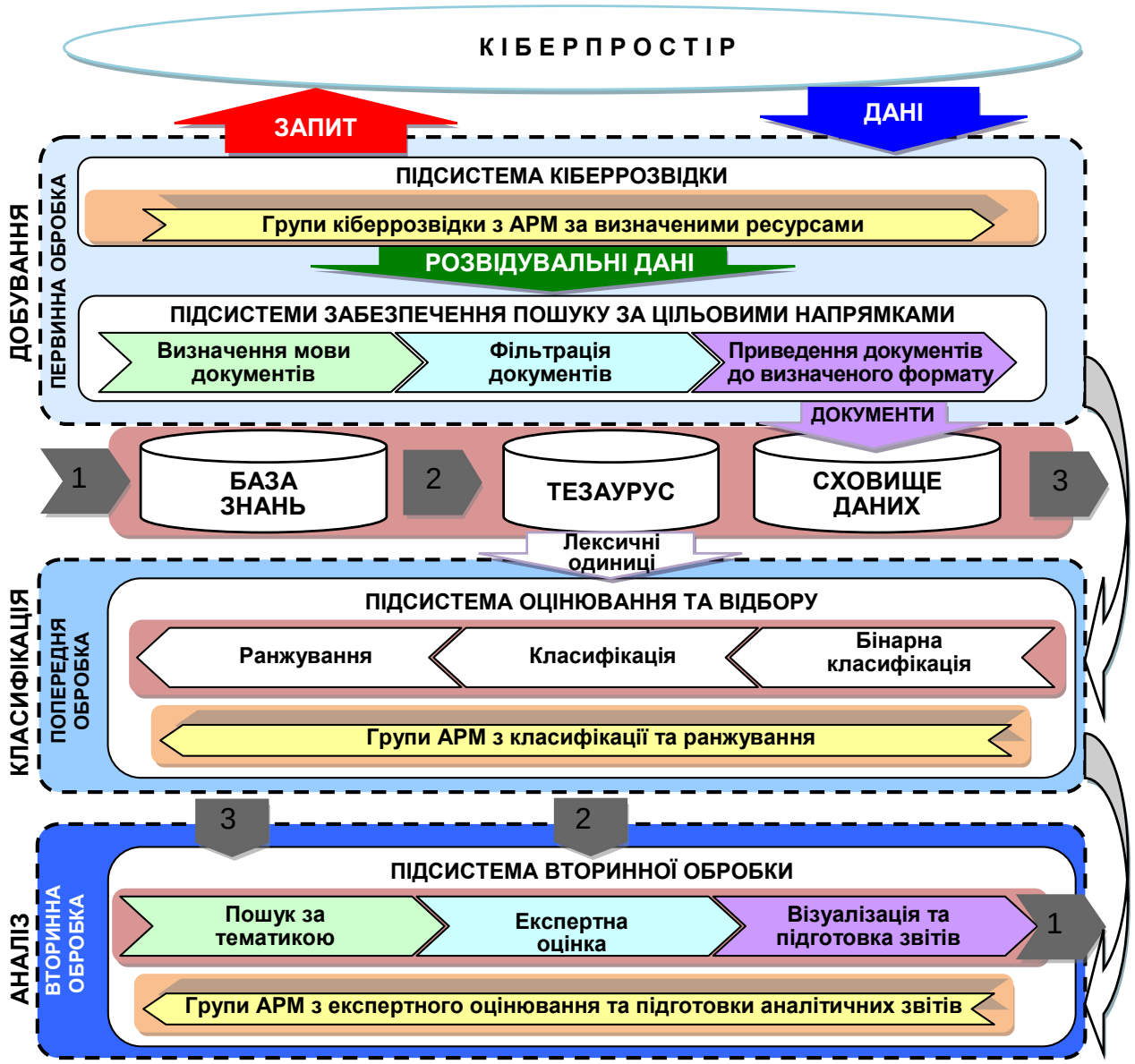

Рис. 1.16. Структура підсистеми обробки розвідувальної інформації

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від інформаційних та кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних та соціосистем.

Основними видами кіберзахисту є (рис. 1.17):

– апаратно-програмний захист;
– технічний захист інформації;
– радіоелектронний захист (радіоелектронна протидія);
– інформаційно-психологічна протидія;
– інші заходи організаційного та нормативно-правового захисту.

Рис. 1.17. Види кіберзахисту

Апаратно-програмний захист – це комплексне застосування апаратних та програмних засобів для забезпечення кіберзахисту комп'ютерної системи. Незважаючи на те, що сучасні операційні системи, такі як операційні системи лінійки *Windows, Linux* та ін. мають власні базові системи захисту, актуальність у здійсненні апаратно-програмного захисту зберігається. Це пов'язано з тим, що інформація при мережному обміні, як правило, піддається деструктивним впливам з боку протиборчої сторони.

Апаратно-програмний захист буває двох видів та містить п'ять груп.

Перший вид – це апаратний захист. Апаратний захист – це захист комп'ютерної системи з використанням технічних пристроїв. Другий вид – це програмно-математичний захист, що забезпечує захист комп'ютерної системи на основі використання програм розмежування доступу (паролів доступу, режимів доступу користувачів тощо).

Основними групами апаратно-програмного захисту є:

− системи ідентифікації (розпізнавання) й автентифікації (перевірки істинності) користувачів;

− системи шифрування даних дискового простору;

− системи шифрування даних, що передаються мережею;

− системи атентифікації електронних даних.

− засоби управління криптографічними ключами.

Технічний захист інформації в кібернетичних системах – це вид захисту, що спрямовується на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації управління. На технічний захист інформації покладаються завдання з виявлення і блокування каналів витоку інформації (радіоканал, ПЕМВ, акустичні канали, оптичні канали тощо). Ефективність вирішення задач з технічного захисту інформації передбачає наявність фахівців в області захисту інформації та їх відповідного технічного оснащення спеціальною технікою виявлення і блокування каналів витоку. Вибір спецтехніки для вирішення завдань технічного захисту інформації визначається на основі аналізу ймовірних загроз і ступеня захищеності об'єкта.

Радіоелектронний захист – це комплекс заходів щодо забезпечення стійкої роботи радіоелектронних засобів від порушення штатних режимів їх роботи.

Інформаційно-психологічна протидія – це складова інформаційно-психологічної боротьби, спрямована на власну аудиторію, яка одночасно є мішенню для пропаганди (психологічних операцій) опозиції (противника), з метою нейтралізації або зведення до мінімуму ефекту від стороннього інформаційно-психологічного впливу. Вона включає комплекс заходів, спрямованих на захист певної системи світоглядних орієнтирів, настанов, стереотипів, на основі яких ґрунтується високий морально-психологічний стан суб'єктів впливу та здатність соціуму, як такого до опору агресору. За американською класифікацією такий вид діяльності відноситься до "консолідуючої пропаганди".

Для підвищення психологічної стійкості особового складу доцільно виявляти лідерів, створювати неформальні групи військовослужбовців, які б формували відповідні стереотипи про армію противника, були б носіями високого морально-психологічного стану. Створення зазначених груп слід здійснювати завчасно, ще в ході психологічного відбору при формуванні миротворчого контингенту. При виконанні завдань в оперативному районі може виникнути необхідність призначення у кожному підрозділі відповідальних осіб, в частинах – спеціальних команд по збору і знищенню агітаційно-пропагандистських матеріалів противника. Зарубіжні фахівці вважають листівки найбільш ефективним засобом психологічного впливу на соціум, тому закриття цього каналу впливу на військовослужбовців дозволить значно знизити ефективність психологічного впливу на особовий склад.

Особлива увага при організації протидії повинна приділятися вивченню змісту, тез та аргументів друкованої та телерадіомовної пропаганди суб'єкта впливу, а також аналізу можливого негативного психологічного впливу на соціум з помітною нервово-психічною нестійкістю, високою "недовірливістю" і тривожністю, які у складних ситуаціях нерідко стають індукторами паніки.

Організаційні заходи захисту передбачають виконання таких функцій:

− визначення технологічних процесів обробки інформації;

− обґрунтування та вибір завдань захисту;

− розробку та впровадження правил реалізації заходів захисту інформації;

− визначення та встановлення обов'язків підрозділів і осіб, що беруть участь в обробці інформації;

− вибір засобів забезпечення захисту інформації;

− оснащення структурних елементів кібернетичної системи нормативними документами і засобами забезпечення захисту інформації;

− встановлення порядку впровадження засобів обробки інформації, програмних і технічних засобів захисту інформації та контролю їх ефективності;

− визначення зон безпеки інформації;

− обґрунтування структури та технології функціонування систем захисту інформації;

− розробку правил та порядку контролю функціонування системи захисту інформації;

– встановлення порядку проведення атестації технічних засобів та систем обробки інформації, систем зв'язку та передачі даних, технічних засобів та систем, що розташовані в приміщеннях, де вона циркулює, приміщень для засідань, а також усієї кібернетичної системи у цілому на відповідність вимогам безпеки інформації.

Нормативно-правовий захист – це вид захисту, що ґрунтується на низці державних указів, законів, постанов, розпоряджень та відповідних міжнародних документів.

Основні цілі кіберзахисту показано на рис. 1.18.

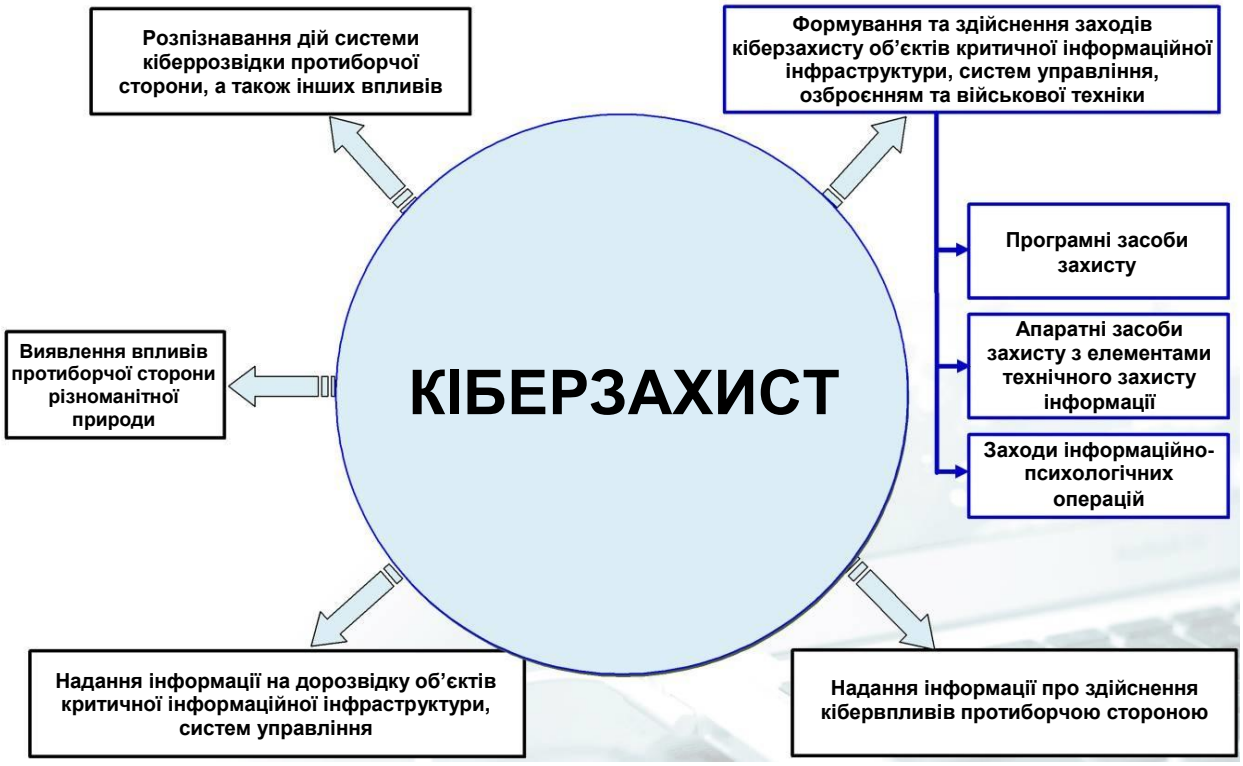

Рис. 1.18. Основні цілі кіберзахисту

Таким чином, підсистема кіберзахисту також як і підсистема кіберрозвідки, є однією з трьох ключових і невід'ємних складових системи кібербезпеки. Отже, тільки комплексна взаємодія компонентів підсистеми кібербезпеки забезпечить захист інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, систем управління об'єктів та суб'єктів з критичною інформаційною інфраструктурою, автоматизованих систем управління, гарантуватиме своєчасне виявлення, упередження та нейтралізацію спроб реалізації різноманітних кібердій зі сторони суб'єктів кібервпливу.

1.5.3. Основи кібервпливу

Зі вступом людства в епоху високотехнологічного розвитку кібервпливи дедалі частіше стають чи не найбільш дієвими механізмами контролю процесів управління, що протікають у кібернетичних системах різного цільового

призначення та різного ієрархічного рівня. Тому наслідки від проявів кібервпливів у міжнародній політиці дедалі частіше проявляються, в першу чергу, не в силовому досягненні політичних цілей, а в прихованому і зовні цілеспрямовано-керованому процесі зміни легітимних урядів, політичного, економічного та духовного підкорення окремих народів, країн територій тощо. Слід зазначити також, що кібервпливи можуть бути спрямовані на будь-які об'єкти кіберпростору, включаючи соціум, соціотехнічні системи, технічні системи (комп'ютерні системи та мережі, системи зв'язку та автоматизовані системи управління (АСУ), управляючі елементи систем озброєння і військової техніки та небезпечних і критичних об'єктів, програмне забезпечення, бази даних тощо), у вигляді інформаційних, психологічних та різноманітних фізичних деструктивних впливів. Причому останнім часом у світі досить інтенсивно розвиваються спеціальні технології психологічного кібервпливу на масову свідомість людей та технології кібервійн. Саме тому роль кібервпливів у сучасній системі протиборства дедалі все частіше стає визначальною, а у системі кібердій їм відводиться чільне місце.

Нині існує багато визначень категорій "кібервплив" та "активні дії у кіберпросторі", але остаточно визнаних та прийнятих ще й досі не існує. У міру розвитку науки і техніки з'являються все нові й нові її тлумачення, отже, маємо такі визначення.

Кібервплив – це цілеспрямований процес застосування усього наявного комплексу засобів та заходів впливу на визначені елементи кіберпростору з метою порушення процесів управління в кібернетичних системах протиборчої сторони шляхом зміни нормальних режимів їх функціонування з подальшим, або співвимірним у часі впливу взяттям їх під власне управління та контроль.

Активні дії у кіберпросторі – заходи деструктивного (руйнівного) впливу на автоматизовані системи управління, системи зв'язку, навігації й управління зброєю, мережнокомп'ютерні та соціотехнічні системи противника.

Безумовно, що кібервпливи є успішними тільки за виконання низки умов. Однією з основних умов є умова існування в сторони, що планує здійснити кібервплив повної інформаційної бази даних про об'єкти впливу за всіма сферами життєдіяльності (суспільно-політичне становище, паролі доступу до комп'ютерних систем та мереж управління збройними силами, систем управління об'єктами атомної енергетики, транспорту, банківської системи, державних органів управління тощо).

Сучасні інформаційні технології дозволяють здійснювати проникнення не лише у відкриті системи, а також у локальні закриті системи, що не мають виходу до загальних мереж. Для цього використовуються будь-які можливості доступу до них, в тому числі безпровідні засоби прийому-передачі інформації. Проникнення у локальні мережі використовується не лише для контролю за потоками інформації та її збору, а також з метою нанесення кіберударів за яких забезпечується порушення нормального функціонування у визначений час за допомогою заздалегідь вмонтованих програмних та апаратних закладок операційних систем, так званої "оболонки" комп'ютера або повного виведення зі строю його апаратних засобів – "ядра".

Об’єктами кібервпливу можуть бути органи управління та системи управління кібернетичних систем живої та неживої природи, а саме:

− технічні системи різного призначення;

− соціум;

− соціотехнічні системи.

У свою чергу, в технічних системах об’єктами кібервпливу виступатимуть АСУ озброєнням і військовою технікою, АСУ критичною інформаційною інфраструктурою (системи життєзабезпечення), АСУ технологічними процесами тощо, комп’ютерні системи з їх базами даних, програмним та апаратним забезпеченням тощо, різні види комп’ютерних систем тощо. Об’єктами кібервпливу серед соціуму є індивідуальна та групова свідомість. Соціотехнічні кібервпливи здійснюються, як на технічні системи, так і на соціотехнічні системи засобами масової комунікації – телебаченням, радіомовленням, Інтернет-мережею тощо.

Спираючись на об’єкти кібервпливу можна виділити його основні види:

− комп’ютерний вплив;

− фізичний вплив;

− радіоелектронний вплив;

− інформаційно-психологічний вплив тощо.

Таким чином, як випливає з вищесказаного – підсистема кібервпливу є ще однією невід’ємною складовою системи кібербезпеки.

Невід’ємною складовою всіх кібердій на цей час стає кіберконтррозвідка. Кіберконтррозвідку можна визначити та охарактеризувати, як особливий вид діяльності, підпорядкований вирішенню завдань забезпечення кібербезпеки та кібероборони, спрямований на адекватну протидію кіберзагрозам національній безпеці, що виникають або можуть виникнути внаслідок кіберрозвідувальної та кібердеструктивної діяльності спеціальних органів іноземних держав (розвідки, контррозвідки), недержавних розвідувальних і контррозвідувальних структур, організацій та окремих осіб. Має на меті запобігання, виявлення та припинення деструктивної діяльності з використанням кіберконтррозвідувальних (та інших) сил і засобів, форм і методів, обумовлених необхідністю своєчасного прийняття заходів, адекватних характеру та масштабам кіберзагроз національним інтересам. Тому функціонування системи кібербезпеки хоча б без однієї зі складових її компонентів, не гарантуватиме досягнення бажаного стану безпеки процесів управління в різних сферах.

Отже, спираючись на передовий світовий досвід у галузі кібербезпеки та ґрунтуючись на отриманих нових наукових результатах встановлено, що система кібердій, що складається з підсистем – кіберрозвідки, кіберзахисту, кібервпливу та кіберконтррозвідки, зі своїми складовими, на сьогодні стає ефективним регулятором процесів управління у різних сферах і на різних рівнях, виступає дієвим інструментом ведення міжнародної та регіональної політики несиловими методами. Саме тому її роль і місце у системі кібербезпеки й надалі тільки актуалізуватиметься.

1.6. Основи міжнародної співпраці з питань забезпечення кібербезпеки

1.6.1. Проблеми забезпечення кібербезпеки на міжнародному рівні

Проблема забезпечення кібербезпеки дедалі частіше стає предметом широкої дискусії не лише на національному, а й на міжнародному рівні. Це обумовлено низкою факторів, деякі з яких наведено нижче.

Фактори, що обумовлюють необхідність міжнародної співпраці у галузі забезпечення кібербезпеки:

1. Різні підходи до розуміння кібербезпеки.

Ефективне забезпечення кібербезпеки потребує єдиного загального розуміння усіх країн її значення. Кібербезпека передбачає захист від несанкціонованого доступу, маніпулювання критично важливими ресурсами і активами, наприклад, даними, і їх руйнування. Цінність таких ресурсів та активів у різних країнах є різною. Вона залежить, зокрема, від рівня розвитку і виду економічної діяльності, а також від того, що саме кожною з країн вважається її критично важливими ресурсами, які зусилля вона готова і здатна прикласти для забезпечення власної кібербезпеки.

Потреби, пріоритети і стратегії у сфері кібербезпеки найменш розвинених країн очевидно відрізняються від країн розвинених. Різноманітність позицій ключових геополітичних гравців призводить до концептуальної невизначеності із формами та методами ідентифікації кібератак відповідно до міжнародного законодавства та унеможливлює розробку адекватних заходів реагування на такі атаки. А тому вироблення єдиного бачення та плану дій щодо вирішення проблеми кібербезпеки є вкрай актуальним для більшості, якщо не для всіх, країн світу і можливе лише шляхом тісної міжнародної співпраці за новими принципами, адекватними викликам, що з’явилися.

2. Глобальний (транскордонний) характер кіберзагроз.

Питання, пов’язані з кіберзагрозами, носять глобальний характер. Але на відміну від традиційних міжнародних протиправних дій, яким, зазвичай, вдається успішно протидіяти за рахунок закриття національних кордонів, для кіберзагроз кордони є прозорими. Часові і географічні фактори, а також місцезнаходження потенційних жертв більше не є перешкодою для місця і часу здійснення кібератак. Тому, окремі країни не мають фактично ніякої змоги боротися із загрозами нового часу. Усі спроби вирішити ці проблеми на національному і регіональному рівнях виявилися недостатніми. Безперечно, виконання заходів протидії кібератакам на національному і регіональному рівнях є необхідними, проте їх недостатньо для адекватного реагування на новітні глобальні виклики.

Юридичні, технічні та інституціональні проблеми, що виникають у зв’язку з кібератаками і кіберзлочинністю, як правило, зачіпають інтереси не однієї країни і призводять до значних деструктивних наслідків, що негативно позначаються на усіх рівнях управління національних держав.

Усі спроби вирішити ці проблеми на національному і регіональному рівнях, апріорі є неефективними, оскільки кіберпростір не має меж і обмежується лише людською уявою. Тим більше, не доводиться говорити про будь-яку відповідність меж кіберпростору існуючим географічним кордонами, а тому кіберзагрози можуть виникнути де завгодно, коли завгодно, і перш ніж вони будуть усунені, завдати величезних збитків за дуже короткий проміжок часу.

3. Технічні особливості маршрутизації повідомлень.

У більшості випадків до процесів передачі даних залучається більше однієї країни. Протоколи, що для цього використовуються, засновані на принципах оптимальної маршрутизації, якщо прямі лінії тимчасово заблоковано. Навіть тоді, коли внутрішні процеси передачі в межах країни походження обмежені, дані можуть покинути країну. При цьому, зв'язок забезпечується через маршрутизатори, що знаходяться за межами цієї території, і перенаправляються назад у країну кінцевого призначення.

Крім того, багато сучасних електронних послуг засновано на зарубіжних сервісах, наприклад, постачальники послуг хостингу можуть запропонувати орендувати веб-простір в одній країні, маючи апаратні засоби в іншій.

4. Стислі терміни розслідування і реагування на кіберінциденти. Розслідування інцидентів, що мали місце у кіберпросторі, як правило,

вимагає стислих термінів виконання. Важливі для відстеження злочинів дані, як правило, дуже швидко видаляються. Стислі терміни розслідування вносять проблеми, оскільки організація традиційного режиму взаємної правової допомоги є досить тривалою. Формальні вимоги і час, необхідний для співпраці з іноземними органами правопорядку, дуже часто ускладнюють розслідування, а подекуди взагалі призводять до його недоцільності.

5. Відмінність підходів до забезпечення кібербезпеки.

Будувати співпрацю у сфері кібербезпеки на традиційних принципах взаємної правової допомоги вкрай важко. Наприклад, принцип обопільного визнання дії злочином створює значні труднощі, якщо в одній з країн, що беруть участь у розслідуванні кіберінциденту, це правопорушення не кваліфікується як злочин. Правопорушники можуть свідомо використовувати у своїх атаках такі країни, з тим щоб ускладнити розслідування.

Запобігання створенню "безпечних гаваней" є одним з головних завдань у сфері кібербезпеки. Поки існують такі "гавані" зловмисники використовуватимуть їх для кібернападів. Країни, що розвиваються, у яких ще не прийнято законодавство у сфері забезпечення кібербезпеки, можуть бути вкрай уразливими, оскільки правопорушники, як правило, вибирають саме такі країни для своїх баз.

Це може призвести до здійснення на деякі країни тиску, щоб примусити ухвалити такі закони. Одним із прикладів подібної ситуації можна навести комп'ютерний хробак "Love Bug", створений на Філіппінах ще в 2000 році. Він заразив мільйони комп'ютерів по всьому світу. Розслідування на місцевому рівні було ускладнене тим, що на той момент на Філіппінах створення і поширення шкідливих програм не переслідувалося у судовому порядку належним чином. Іншим прикладом є Нігерія, яка зазнає тиску з метою

примушування її до реагування на фінансові афери, які здійснюються по електронній пошті.

6. Відсутність належних організаційних структур.

Відсутність інституціональних структур для усунення наслідків інцидентів (наприклад, вірусних і мережевих атак, що призводять до актів шахрайства, знищення інформації і/або поширення забороненого контенту), також є серйозною проблемою при реагуванні на кібератаки.

Хоча деякі країни і регіони створили власні агентства, що займаються спостереженням і попередженням та реагуванням на інциденти у кіберпросторі, а також організаційні структури для координації діяльності з реагування на кібератаки, сучасний стан справ у сфері забезпечення кібербезпеки вимагає значно більших зусиль. Якщо кібератака здійснюється в одній країні, її руйнівні наслідки можуть протягом декількох хвилин досягти своїх жертв у країнах, між якими встановлено з'єднання. Вільний потік інформації, спільна робота і співпраця між національними організаційними структурами мають життєво важливе значення для ефективного усунення таких інцидентів і реагування на них. Ще однією областю, в якій необхідно створити організаційні структури і розробити відповідну політику, є область загальних сертифікатів ідентифікації (цифрова сертифікація). Упродовж тривалого часу автентифікація користувача вважалася найефективнішою стратегією боротьби з кіберзагрозами (розкраданням персональних даних, вивуджуванням даних та іншими видами on-line шахрайства). Строга автентифікація є найважливішим компонентом для зміцнення довіри і безпеки в умовах інформаційного суспільства. Хоча деякі країни створили організаційні структури й інфраструктуру, необхідні для надання громадянам загальних сертифікатів ідентифікації, в інших країнах такі структури ще тільки належить створити. Потрібна глобальна структура, яка дозволила б забезпечити всесвітнє визнання без урахування географічних кордонів, національних загальних сертифікатів ідентифікації, контрольованих державою.

Вирішення зазначених проблемних питань можливе тільки за умови прийняття узгодженої стратегії, в якій враховується роль усіх зацікавлених сторін, а також існуючі ініціативи у рамках міжнародної співпраці. Такі ініціативи реалізуються на міжнародному, регіональному і міждержавному рівнях (рис. 1.19).

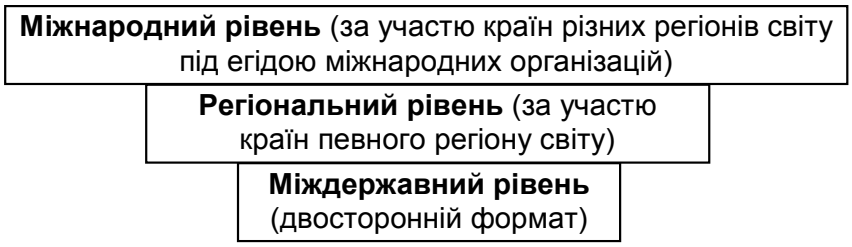

Рис. 1.19. Рівні міжнародної співпраці з питань кібербезпеки

Так, на ***міжнародному рівні*** питання кібербезпеки розглядаються у рамках:

− ООН, яка прийняла низку рішень, резолюцій та рекомендацій, що стосуються питань кібербезпеки;

− Групи восьми (G8), у структурі якої створено Підкомітет з питань високотехнологічних злочинів, що розглядає в тому числі проблеми боротьби з кіберзлочинністю;

− Ради Європи, яка ще у 1996 році створила Комітет з питань боротьби з кіберзлочинністю;

− Міжнародного союзу електрозв'язку, який реалізує власну Глобальну програму кібербезпеки.

На ***регіональному рівні*** питання кібербезпеки вирішуються у рамках:

− Європейського союзу, де до участі у зазначеному процесі залучено усі без винятку країни-члени співтовариства;

− НАТО, така співпраця стосується в основному воєнної складової кібербезпеки;

− Організації економічної співпраці і розвитку, яка з 1983 року проводить дослідження у сфері кібербезпеки, на підставі яких розробляє рекомендації щодо підвищення рівня такої безпеки;

− Азіатсько-Тихоокеанського економічного співробітництва (АТЕС), країни-учасники якого у 2002 році прийняли Стратегію кібербезпеки АТЕС та зобов'язалися всіляко сприяти одна одній у вирішенні питань забезпечення кібербезпеки;

− Співтовариства націй, де розроблено типовий закон про комп'ютери і комп'ютерні злочини, що дало змогу уникнути 1272 двосторонніх переговорів у рамках об'єднання з питань кібербезпеки;

− Ліги арабських держав і Ради співробітництва арабських держав Перської затоки, країни-члени яких задекларували необхідність відшукання спільних підходів у вирішенні проблем, пов'язаних з кібербезпекою;

− Асоціації держав Південно-Східної Азії, де планується створити систему кібербезпеки, що охоплює десять країн співтовариства, та передбачає обмін інформацією про кібератаки і технології захисту від них та проведення навчань для визначення ефективності системи;

− Організації американських держав, країни-учасниці якої вирішують спільні проблеми кібербезпеки у форматі щорічних зустрічей міністрів юстиції та генеральних прокурорів, а також за активної співпраці з Групою восьми.

На ***міждержавному рівні*** багато країн світу останнім часом значно активізували свою діяльність у напряму співпраці у сфері кібербезпеки. Підписано цілу низку двосторонніх договорів між різним країнами. Однак основним учасником двосторонньої співпраці у зазначеному напряму є Сполучені Штати Америки, що пояснюється не стільки їх позиціонуванням як світового лідера, скільки зацікавленістю у питаннях кібербезпеки з огляду на значний рівень залежності усіх сфер життєдіяльності США від кібернетичних систем.

В останні роки окрім роботи у рамках Організації Північноатлантичного договору Сполучені Штати розвивають активну двосторонню співпрацю у

сфері кібербезпеки з низкою країн. Зокрема, 19 липня 2011 року підписано Угоду з кібербезпеки між США та Індією – "Меморандум про взаєморозуміння", яка спрямована на розвиток більш тісної співпраці та взаємне інформування про кіберзагрози.

Крім того, після низки офіційних візитів у червні 2011 року підписано спільну російсько-американську заяву, присвячену питанням кібербезпеки. А у 2013 році на саміті "великої вісімки" в Ірландії відбулася зустріч Президентів Росії і США, в результаті якої прийнято спільну заяву про створення прямого каналу зв'язку між високими посадовими особами двох країн, а також оголошено про створення двосторонньої робочої групи з питань кібербезпеки у рамках інституту президентських комісій.

15 вересня того ж року міністрами оборони і закордонних справ США і Австралії підписано спільну заяву, в якій сторони погодилися "у разі кібератак, що загрожуватимуть територіальній цілісності, політичній незалежності або безпеці будь-якої з держав, Австралія і Сполучені Штати проведуть спільні консультації і вироблять адекватні заходи з протидії загрозам".

У 2013 році в ході американсько-китайського "Стратегічного діалогу з питань економіки і безпеки" між країнами було досягнуто домовленість про необхідність вироблення спільних підходів в питаннях кібербезпеки та створення робочої групи з питань стратегічної безпеки для вивчення зазначеної проблеми.

У 2011 році США та Канада досягли домовленості про розробку спільного плану дій у напрямку забезпечення кібербезпеки, яким передбачається поглибити "двосторонню співпрацю у сфері кібербезпеки для зміцнення оборони критичної інфраструктури та посилити можливості обох країн спільного й ефективного реагування на кіберінциденти". Поставлені цілі досягатимуться за рахунок реалізації спільних проектів та вирішення оперативних завдань, включаючи спільні наради із залученням представників приватного сектору та інших зацікавлених сторін, а також покращення обміну інформацією між операційними центрами у реальному масштабі часу.

У жовтні 2013 року міністри оборони США та Японії заявили про тісну співпрацю у напрямку протидії кібератакам та підписали договір про вироблення спільних підходів до обговорення заходів кібербезпеки для протидії атакам на урядові установи та інші організації, які здійснюються переважно Китаєм та Північною Кореєю.

Небезпеки, що приховуються у кіберпросторі, змушують співпрацювати між собою навіть ті країни, між якими існують певні політичні протиріччя. Зокрема, це стосується Індії та Китаю, які домовилися співпрацювати у галузі кібербезпеки на підставі єдиного бачення і підходів.

Слід зазначити, що найбільш ефективним є саме останній двосторонній формат співпраці країн у сфері кібербезпеки. Це й не дивно, адже двостороння співпраця вимагає врахування та узгодження позицій тільки двох сторін, що дозволяє оптимізувати контур такої діяльності (рис. 1.20), значно підвищуючи її результативність.

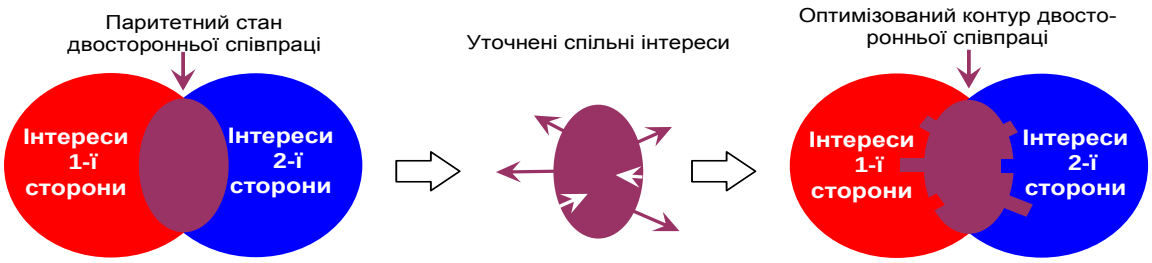

Рис. 1.20. Оптимізація контуру двосторонньої співпраці у сфері кібербезпеки

1.6.2. Діяльність Міжнародного союзу електрозв'язку щодо забезпечення кібербезпеки

Міжнародний союз електрозв'язку (МСЕ) (англ. International Telecommunication Union, ITU) є спеціалізованою установою Організації Об'єднаних Націй в області інформаційно-комунікаційних технологій (ІКТ), який розподіляє радіочастотний спектр і супутникові орбіти в глобальному масштабі, розробляє технічні стандарти, що забезпечують можливість ефективного приєднання мереж і технологій, і прагне поліпшити доступ до ІКТ для спільнот усього світу, що недостатньо обслуговуються.

МСЕ веде свою діяльність в трьох основних областях, організованих "по Секторах", робота яких здійснюється через конференції та збори:

− Сектор радіозв'язку МСЕ (МСЕ-R);
− Сектор стандартизації електрозв'язку МСЕ (МСЕ-Т);
− Сектор розвитку електрозв'язку МСЕ (МСЕ-D).

Сектор радіозв'язку МСЕ (МСЕ-R) здійснює координацію широкого і постійно зростаючого діапазону послуг радіозв'язку, а також управляє на міжна- родному рівні використанням радіочастотного спектра і супутникових орбіт.

Сектор стандартизації електрозв'язку МСЕ (МСЕ-Т) створює і переглядає понад 150 стандартів щорічно, що охоплюють всі елементи – від функціональних властивостей базових мереж до послуг наступних поколінь, таких як Інтернет-телебачення.

Сектор розвитку електрозв'язку МСЕ (МСЕ-D) пропонує програми, які допомагають вступати на ринки, що формуються, або розширювати на них свою присутність, демонструвати світове лідерство у сфері ІКТ, дізнатися як впровадити належну політику, або виконувати свій мандат, який передбачає корпоративну соціальну відповідальність

Діяльність МСЕ у галузі кібербезпеки розпочинається з Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства у 2003 році, коли Голови держав і урядів та інші світові лідери, що брали участь у Всесвітній зустрічі, а також держави – члени МСЕ, доручили МСЕ вжити конкретні заходи, спрямовані на обмеження загроз і незахищеності, пов'язаних з інформаційним суспільством. МСЕ визначили, як єдиного координатора за напрямом діяльності "Зміцнення довіри і безпеки при використанні інформаційно-комунікаційних технологій".

У 2007 році Генеральний Секретар МСЕ розробив Глобальну програму кібербезпеки (GCA – Global Cybersecurity Agenda) – механізм міжнародної співпраці по даному питанню.

З 2008 року по 2010 рік – Члени МСЕ схвалили Глобальну програму кібербезпеки у якості основного інструменту МСЕ з кібербезпеки.

Відповідно до Глобальної програми кібербезпеки кожна держава, яка співпрацює з МСЕ, повинна мати національну команду реагування на комп'ютерні інциденти (Computer Emergency Response Team – CERT). На CERT у міжнародному масштабі покладаються функції моніторингу і виявлення механізмів і Інтернет-ресурсів, що порушують норми міжнародного законодавства у сфері кібербезпеки. Також CERT вирішують завдання щодо розробки рекомендацій користувачам з організації захисту інтересів особистості і держави в інформаційній сфері, надання консультативних послуг з питань забезпечення інформаційної безпеки, прийняття повідомлень про хакерські кібератаки.

Національні команди CERT при цьому координують дії державних підрозділів комп'ютерної безпеки державних органів влади, операторів зв'язку, а також інших суб'єктів інформаційної інфраструктури з питань припинення порушень, пов'язаних з несанкціонованим втручанням в роботу інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем та мереж. Координацію діяльності таких структур на міжнародному рівні здійснює міжнародна організація FIRST (Forum of Incident Response and Security Teams) – Форум команд реагування на інциденти безпеки. На сьогодні в 66 країнах світу функціонує 305 CERT команд.

Наприклад, у США – 72 команди, в Японії та Німеччині – по 23 команди, в Литві – 5 команд, в РФ, Мексиці та Польщі – по 2 команди.

Основні завдання CERT:

− реакція на кіберзлочини;

− поширення своєчасних попереджень;

− комунікація і обмін інформацією між усіма зацікавленими;

− розробка стратегій зниження ризиків і координація заходів по реагуванню;

− обмін інформацією по інцидентах і заходах реагування;

− публікація кращих практик реагування і запобігання загрозам;

− координація міжнародної співпраці по кібербезпеці.

МСЕ було розроблено глобальний індекс кібербезпеки (GCI – Global Cybersecurity Index), який дозволяє оцінити рівень участі держав у сфері кібербезпеки, що робиться за п'ятьома сферами: законодавча база, технічна реалізація, організаційні заходи, створення потенціалу, національна і міжнародна співпраця. Щороку МСЕ проводить дослідження та публікує рівень кібербезпеки кожної держави.

Наприклад, у 2017 році проаналізовано 193 країни. Перше місце отримав Сінгапур, за ним США, Малайзія та Оман. Серед країн Європи лідирують Естонія, Франція і Норвегія. Останнє 193 місце посіла Екваторіальна Гвінея. Топ-5 пострадянських країн: Грузія – 8 місце, Російська Федерація – 10 місце, Білорусь – 39 місце, Азербайджан – 48 місце, Україна – 56 місце.

Основні публікації МСЕ:

1. Глобальна програма кібербезпеки.
2. Керівні вказівки для дітей з захисту дитини в он-лайновому середовищі.
3. Керівні вказівки для батьків, опікунів і учителів з захисту дитини в он-лайновому середовищі.
4. Керівні вказівки для галузі з захисту дитини в он-лайновому середовищі.
5. Керівні вказівки для директивних органів з захисту дитини в он-лайновому середовищі.
6. Елементи для створення глобальної культури кібербезпеки.

1.6.3. Напрями міжнародного співробітництва з питань забезпечення кібербезпеки

Основні напрями міжнародної співпраці. У цілому міжнародна співпраця передбачає заходи забезпечення кібербезпеки, які можна об'єднати за такими основними напрямами [57, 60]:

1. Нормативно-правове забезпечення:

1.1. Розроблення міжнародного правового поля у сфері кібербезпеки.

1.2. Гармонізація та узгодження національних законодавств різних країн у сфері кібербезпеки.

1.3. Узгодження законодавства у сфері кібербезпеки з існуючими міжнародними правовими нормами тощо.

2. Технічні і процедурні заходи:

2.1. Відпрацювання механізмів та процедур взаємодії різних структур на усіх рівнях.

2.2. Розроблення єдиних протоколів і стандартів безпеки.

2.3. Затвердження схем сертифікації апаратних засобів і програмного забезпечення.

2.4. Створення універсальної системи цифрової ідентифікації.

3. Створення та злагодження діяльності організаційних структур, відповідальних за забезпечення кібербезпеки:

3.1. Формування організаційних структур, відповідальних за розробку політики у сфері кібербезпеки, спостереження, оповіщення та реагування на інциденти у кіберпросторі.

3.2. Навчання та злагодження створених організаційних структур.

4. Підготовка персоналу у сфері кібербезпеки:

4.1. Сприяння у підготовці кадрів для організаційних структур кібербезпеки.

4.2. Навчання персоналу за єдиним програмами підготовки.

5. Координація діяльності учасників міжнародної співпраці:

5.1. Створення міжнародних координуючих органів з питань кібербезпеки.

5.2. Постійний обмін передовим досвідом забезпечення кібербезпеки на різних рівнях.

5.3. Спрямування розвитку міжнародної системи кібербезпеки у напряму,

адекватному еволюції викликів у цій сфері.

Заходи нормативно-правового, технічного, процедурного й організаційного забезпечення слід реалізувати на національному і регіональному рівнях, однак вони мають бути узгоджені на міжнародному рівні. Останні два напрями міжнародної співпраці у сфері кібербезпеки проходять через усі три попередні напрями.

Основні заходи міжнародної співпраці та зв'язки між ними у галузі забезпечення кібербезпеки:

Правові заходи. Розробка міжнародного законодавства з кібербезпеки. Гармонізація національних законодавств. Узгодження законодавства у сфері кібербезпеки з існуючими міжнародними правовими нормами.

Технічні та процедурні заходи. Відпрацювання механізмів та процедур взаємодії різних структур на усіх рівнях. Розробка єдиних протоколів і стандартів безпеки. Затвердження схем сертифікації апаратних засобів і програмного забезпечення.

Організаційні структури. Формування організаційних структур, відповідальних за безпеку у кіберпросторі. Навчання та злагодження створених організаційних структур.

Координація діяльності. Створення міжнародних координуючих органів з питань кібербезпеки. Постійний обмін передовим досвідом. Спрямування розвитку у міжнародній системі кібербезпеки.

Підготовка персоналу. Сприяння у підготовці кадрів для організаційних структур кібербезпеки. Навчання персоналу за єдиними програмами підготовки.

Таким чином, формування кібербезпекового сектору на міжнародному рівні, так само, як і на національному, й досі триває. Цей процес стикається з низкою проблем, обумовлених інноваційним характером кібербезпекової проблематики. На даний час ведеться активна діяльність з налагодження міжнародної співпраці з питань кібербезпеки у різних форматах. Основними напрямами такої співпраці є розробка нормативно-правового поля, технічних та процедурних основ кібербезпеки, створення організаційних структур, підготовка персоналу та координація дій зацікавлених сторін. При цьому, значна увага звертається на урахування існуючих національних і регіональних ініціатив для того, щоб уникнути дублювання функцій.

1.6.4. Міжнародне співробітництво України з питань забезпечення кібербезпеки

Цілі розвитку безпекового співробітництва ЄС і НАТО збігаються, і це базується не лише на тому факторі, що 22 країни є одночасно членами і ЄС, і НАТО, але й на бажанні взаємного заповнення поточних прогалин у безпекових можливостях один одного, зокрема у сфері кібербезпеки. Для розвитку такої співпраці, а також взаємодії зі іншими акторами, зокрема, Україною, був розроблений Рамковий документ зі спільного дипломатичного реагування ЄС на шкідливу кібердіяльність (Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities) [45].

Вагомим поштовхом для активізації зусиль у цьому напряму стало прийняття 2 квітня 2009 року організацією НАТО програмного документа під назвою "Рамки для співробітництва у питаннях кіберзахисту між НАТО та державами-партнерами". Відповідно до основних положень документа країни-партнери закликають до вжиття необхідних заходів з метою гармонізації національного законодавства у сфері кібербезпеки з відповідними міжнародними нормами (зокрема, такими як Конвенція Ради Європи з питань кіберзлочинності).

У рамках практичної реалізації зазначеного документа 6-7 травня 2009 року в Штабквартирі НАТО відбулися експертні консультації під егідою спільної робочої групи Україна-НАТО з воєнної реформи. Розгляд конкретних рекомендацій, що були напрацьовані під час експертних консультацій, відбувся 13-14 травня 2009 року у Варшаві. На засіданні досягнуто домовленості про створення Робочої підгрупи Україна-НАТО з питань кіберзахисту у форматі ad/hoc, а також розглянуто можливості запобігання загрозам кіберзлочинності та кібертероризму на найближчу перспективу у світовому масштабі.

Перше засідання робочої підгрупи Україна-НАТО за пропозицією Міжнародного секретаріату Альянсу, що корегує взаємодію у сфері кіберзахисту у форматі Консультацій експертів відбулося 11-12 лютого 2010 року у Києві. На засіданні розглянуто концептуальні підходи НАТО до побудови систем кіберзахисту, висвітлено окремі питання організації кіберзахисту в країнах Альянсу, проведено детальний огляд системи забезпечення кіберзахисту України тощо. Як результат, учасники Консультацій затвердили План роботи Робочої підгрупи Україна-НАТО та серед пріоритетних завдань визначили для України розробку рекомендацій з урахуванням досвіду держав-членів НАТО щодо вдосконалення системи захисту національної інформаційної інфраструктури від внутрішніх та зовнішніх кіберзагроз у рамках діяльності Спільної робочої групи Україна-НАТО з воєнної реформи високого рівня, а також налагодження співробітництва з міжнародними структурами з протидії кіберзагрозам з метою обміну досвідом та проведення спільних заходів. Друге засідання Робочої підгрупи Україна-НАТО за пропозицією Міжнародного секретаріату Альянсу, в рамках якої Україна отримує експертну допомогу НАТО в питаннях підготовки національної стратегії протидії кіберзагрозам, розвитку інфраструктури кіберзахисту та системи реагування на кіберзагрози, проведено у червні, а третє у жовтні 2010 року. Засідання спільної робочої групи Україна-НАТО з питань воєнної реформи у сфері кіберзахисту відбулося 8 грудня 2010 року в Брюсселі. За результатами проведених засідань було визначено напрями подальшої співпраці України з НАТО у сфері кіберзахисту, основними з яких українською стороною вважаються:

− заснування консультативних механізмів;

− обмін досвідом щодо законодавчого забезпечення і регулювання;

− створення груп реагування на кризові ситуації в електронних мережах;

− обмін досвідом та взаємодопомога у технічних аспектах захисту від кібератак;

− розробка механізмів оперативної взаємодії в кризових ситуаціях;

− налагодження системи обміну інформацією щодо моніторингу кіберпростору;

− налагодження системи оповіщення про початок кібератаки;

− обмін інформацією про технічні аспекти кібератаки;

− оперативна співпраця щодо виявлення джерел кібератаки та засобів протидії;

− співпраця щодо усунення негативних наслідків кібератаки;

− узагальнення досвіду, напрацювання технічних рішень та організаційних рекомендацій щодо запобігання кібератакам.

Важливою віхою розвитку співпраці ЄС і НАТО з кібербезпеки стало встановлення Центром передового досвіду НАТО з кібероборони у 2013 році зв'язків з Європейським оборонним агентством для обміну інформацією, проведення спільних навчань і заходів та уникання дублювання досліджень у кіберсфері. Дві структури провели низку спільних навчань, зокрема - вже згадане навчання "Кібер Коаліція" (Cyber Coalition) і навчання "Кібер Європа" (Cyber Europe), які стали платформою для спільних підходів.

Нинішня актуалізація гібридних викликів і загроз, пов'язана з агресією Росії проти України, надає додаткового поштовху поглибленню взаємодії двох організацій. В лютому 2016 року, ще до схвалення Спільної заяви ЄС-НАТО, дві організації підписали Технічну угоду про співпрацю з кібероборони за напрямами обміну інформацією, тренування, досліджень і навчання. В результаті, практична співпраця розвивається між Групою реагування на комп'ютерні надзвичайні ситуації ЄС (CERT-EU) і Центром можливостей з реагування на комп'ютерні інциденти (NCIRC), які й стали підписантами згаданої технічної угоди від імені ЄС і НАТО.

На саміті НАТО 11-12 липня 2018 року у новій штаб-квартирі в Брюсселі розширене співробітництво між ЄС і НАТО відсвяткувало свій другий рік. Співпраця між ЄС і НАТО зросла в усіх сферах, від гібридних загроз та кібербезпеки до морського співробітництва. Кібербезпека постійно присутня в їхніх офіційних документах.

В рамках Розширеної співпраці між ЄС і НАТО із залученням третіх сторін, зокрема, з кібербезпеки, на даний час існують три пілотні країни: Молдова, Туніс та Боснія і Герцеговина. Третій звіт про хід її імплементації, схвалений Радами ЄС та НАТО, визначає, що обмін інформацією, включаючи й міжштабні політичні консультації, також матимуть місце й для України.

Україна має багато кваліфікованих експертів у кіберсфері. Проте їм все ще не вистачає міжвідомчої координації та співпраці з міжнародними партнерами. Наприклад, Консультативна місія ЄС в Україні співпрацює з Кіберполіцією України, Службою безпеки України та Національним центром координації кібербезпеки при РНБО України. Тим часом, належна координація залишається важливою проблемою, оскільки вона не залежить від стратегій чи політик, які вони розробляють. Так само кошти та зусилля донорів залежать від рівня міжвідомчої координації в Україні.

Україна співпрацює з ЄС і НАТО у сфері кібербезпеки поки що сепаратно, хоча в окремих випадках, переважно на рівні практичної допомоги, дві організації здійснюють щонайменше узгодження своїх зусиль, адже ця

двостороння допомога має бути скоординована у відповідності до засад співробітництва ЄС-НАТО у сфері кібербезпеки.

В Європейській службі зовнішньої дії вважають, що комплексний характер кіберпростору вимагає спільних зусиль урядів, приватного сектору, експертного середовища, технічної спільноти, користувачів і науковців з протидії сучасним кіберзагрозам. Як повідомив представник Підрозділу координації кіберполітики, попередження конфліктів і політики безпеки Європейської служби зовнішньої дії Елоїз Діволь на міжнародній конференції "Нові формати співпраці НАТО і ЄС з Україною" 30-31 травня 2018 року у Києві, ЄС звертає увагу на необхідність адаптації країн-партнерів, включаючи Україну, до правил кібербезпеки ЄС, пріоритетними серед яких є сертифікація програмного забезпечення, процес передачі звітності, впровадження норм відповідальності за дії в кіберпросторі.

На багатосторонньому рівні ЄС керується переважно цілями, визначеними у Спільному робочому документі "Східне Партнерство – 20 очікуваних досягнень до 2020 р.: фокусуючись на головних пріоритетах та реальних результатах", де в розділі "Безпека" три із десяти груп завдань стосуються кібербезпеки, зокрема, щодо створення повноцінних діючих підрозділів боротьби з кіберзлочинністю, розвитку державно-приватного співробітництва та міжнародного співробітництва у сфері кібербезпеки. Ці завдання Україна або вже виконала, або має усі реальні шанси виконати до 2020 року. В Україні схвалена Стратегія кібербезпеки України, імплементується Конвенція про кіберзлочинність і Директива 2008/114/ЄК щодо захисту критичної інфраструктури, створені необхідні інституції, які взаємодіють з ЄС та недержавними інституціями (наприклад, CYS-Centrum і Українськими Кібервійськами).

На двосторонньому рівні Україна-ЄС кібербезпека перебуває у центрі уваги. Так, під час п'ятого засідання Ради асоціації 17 грудня 2018 р. в Брюсселі обидві сторони підкреслили необхідність подальшої співпраці у боротьбі з кібер- та гібридними загрозами в інтересах безпеки своїх громадян. У зв'язку з цим Рада асоціації привітала зобов'язання ЄС продовжувати підтримку України в галузі кібербезпеки.

У 2017-2018 роках ЄС здійснив низку заходів у рамках інструменту технічної допомоги TAIEX у трьох сферах: створення відповідної законодавчої бази в Україні; створення державно-приватного партнерства та просування організаційних аспектів національних структур кібербезпеки; підтримка технічних здібностей та навичок у державних органах, відповідальних за кібербезпеку.

ЄС допомагає Україні завдяки своїй Консультативній місії (EU Advisory Mission to Ukraine, EUAM), яка по всій Україні допомагає серед іншого у сфері протидії кіберзагрозам. На різноманітні проекти допомоги Україні у сфері кібербезпеки в КМЄС було виділено більше 2,5 млн. євро. Місія сприяє покращенню технічного оснащення українських правоохоронних органів, проводить тренінги, обміни досвідом, дискусійні панелі. До заходів залучаються фахівці Європолу та інших інституцій ЄС.

Кіберсфера є пріоритетною у розвитку співробітництва України з НАТО. Зокрема, українські експерти, які брали участь у міжнародному круглому столі "Україна-НАТО: Невійськова співпраця як спільна відповідь на гібридні загрози», організованому Центром глобалістики "Стратегія XXI" і Представництвом Фонду Конрада Аденауера в Україні 9 лютого 2017 року в м. Київ, поставили кібербезпеку на друге місце серед пріоритетних напрямів спільної Україна-НАТО протидії гібридним загрозам.

Налагоджено кіберспівпрацю між Україною й НАТО, яка щороку прописується в Річних національних програмах під егідою Комісії Україна-НАТО (РНП) в окремому розділі "Кібербезпека". Метою цієї співпраці визначено "удосконалення національної системи кібербезпеки як складової системи забезпечення інформаційної безпеки, її правових концептуальних засад та практичних механізмів протидії агресії РФ у кіберпросторі". Згідно з РНП, Україна зміцнює співробітництво державних, у тому числі правоохоронних і спеціальних органів, з приватним ІТ-сектором, що відповідає підходам і ЄС, і НАТО у сфері протидії кіберзагрозам.

Співпраці Україна-НАТО сприяє запущений у 2014 році відповідний Трастовий фонд допомоги Альянсу (Trust Fund on Cyber Defence) та Комплексний пакет допомоги НАТО, схвалений 2016 року, де кібербезпека визначена пріоритетним напрямом. Мета очолюваного Румунією Трастового фонду полягає в тому, щоб забезпечити розвиток в Україні власних груп протидії кіберзагрозам та надійних захисних технічних можливостей CSIRT1, включаючи лабораторії для розслідування кіберінцидентів. НАТО надає допомогу Україні із вдосконалення законодавства, розробки стратегії і політик, практичної підтримки у розвитку технічної інфраструктури, підготовки та напрацювання потенціалу кібероборони, що залишатиметься пріоритетом на найближчий час.

У 2014 році розпочато проект зі створення ситуаційних центрів реагування на комп'ютерні інциденти для моніторингу подій у сфері кібербезпеки, а також лабораторій для розслідування інцидентів у кіберпросторі та ліквідації їхніх наслідків. У червні 2017 року українські інституції успішно отримали відповідне обладнання, а в липні 2017 року завершився перший етап Цільового фонду, головними бенефіціарами якого були СБУ та ДССЗЗІ. У січні 2018 року був відкритий Ситуаційний центр забезпечення кібербезпеки СБУ. На цей проект НАТО виділило понад 1 млн. доларів США. Інші українські міністерства, зокрема, МЗС України, також отримують від НАТО обладнання та програмне забезпечення, необхідне для захисту інформаційної інфраструктури [45].

В Законі України "Про основні засади забезпечення кібербезпеки України" функціонування національної системи кібербезпеки забезпечується шляхом:

− вироблення й оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

− створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки

відповідно до міжнародних стандартів, зокрема, стандартів Європейського Союзу та НАТО;

− функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

− розвитку мережі команд реагування на комп'ютерні надзвичайні події;

− впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

− підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі, для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

− встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

− розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах зі зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі.

Передбачається, що в подальшому у сфері кібербезпеки НАТО приділятиме увагу розбудові можливостей України, наданні необхідного обладнання і підготовці персоналу, в результаті чого Україна повинна набути здатності захищати свою інфраструктуру від кібератак.

У майбутньому розвитку співпраці між ЄС і НАТО у сфері кібербезпеки Україна може бути в центрі уваги, якщо українське керівництво буде підтримувати темпи реформ та покращить рівень міжвідомчої координації [45].

1.7. Напрями забезпечення кібербезпеки України

1.7.1. Основні положення Стратегії кібербезпеки України

Стратегія кібербезпеки України (далі – Стратегія) введена в дію Указом Президента України від 15 березня 2016 року №96/2016.

Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення цієї мети необхідними є:

− створення національної системи кібербезпеки;

− посилення спроможностей суб'єктів Сектору безпеки і оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;

− забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та

порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, *має базуватися на принципах*:

− верховенства права і поваги до прав та свобод людини і громадянина;

− забезпечення національних інтересів України;

− відкритості, доступності, стабільності та захищеності кіберпростору;

− державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;

− пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;

− пріоритетності запобіжних заходів;

− невідворотності покарання за вчинення кіберзлочинів;

− пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

− міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях;

− забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.

Розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Стратегія кібербезпеки України базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 “Про рішення Ради національної безпеки і оборони України” від 6 травня 2015 року “Про Стратегію національної безпеки України”.”

Кіберпростір поступово перетворюється на окрему, поряд із традиційними "Земля", "Повітря", "Море" та "Космос", сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи Збройних сил провідних держав світу. З урахуванням широкого застосування сучасних інформаційних технологій у Секторі безпеки і оборони, створення єдиної автоматизованої

системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз.

Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, Сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чи опосередковано пов'язані з Російською Федерацією.

Сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет.

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

Загрози кібербезпеці актуалізуються через дію таких факторів, зокрема, як:

− невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;

− недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом від кіберзагроз;

− безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;

− недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

− недостатня ефективність суб'єктів Сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;

− недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури.

Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію та контроль діяльності суб'єктів Сектору безпеки і оборони, які забезпечують кібербезпеку України.

Основу національної системи кібербезпеки становитимуть Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

1.7.2. Сутність та завдання Національної системи забезпечення кібербезпеки України

В прийнятій Стратегії кібербезпеки України визначені суб'єкти забезпечення кібербезпеки України та основні їх завдання відповідно до компетенцій. Більш детально Національна система забезпечення кібербезпеки України розглядається в Законі України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 року.

Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі **основні завдання** (рис. 1.21):

Державна служба спеціального зв'язку та захисту інформації України:

− забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах;

− координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту;

− забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту;

− здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

− інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації);

− координує, організовує та проводить аудит захищеності комунікаційних і

технологічних систем об’єктів критичної інфраструктури на уразливість;

− забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA.

Національна поліція України:

− забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі;

− здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Служба безпеки України:

− здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі;

− здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів;

− протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави;

− розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури;

− забезпечує реагування на кіберінциденти у сфері державної безпеки.

Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції:

− здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони);

− здійснюють військову співпрацю з НАТО та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз;

− впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

Розвідувальні органи України:

− здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

Національний банк України:

− визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб’єктів переказу коштів, здійснює контроль за їх виконанням;

− створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об’єктах критичної інфраструктури у банківській системі України.

Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення й оперативної адаптації державної політики у сфері

кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури;

4) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

5) залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

6) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

8) розвитку мережі команд реагування на комп'ютерні надзвичайні події;

9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

10) забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

11) створення та забезпечення функціонування Національної телекомунікаційної мережі;

12) обміну інформацією про інциденти кібербезпеки між суб'єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі, для підвищення кваліфікації та проведення обов'язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об'єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію уразливості комунікаційних систем;

16) встановлення вимог (правил, настанов) щодо безпечного використання

мережі Інтернет та надання електронних послуг державними органами;

17) державно-приватної взаємодії у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах зі зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, Сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

23) обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

24) розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

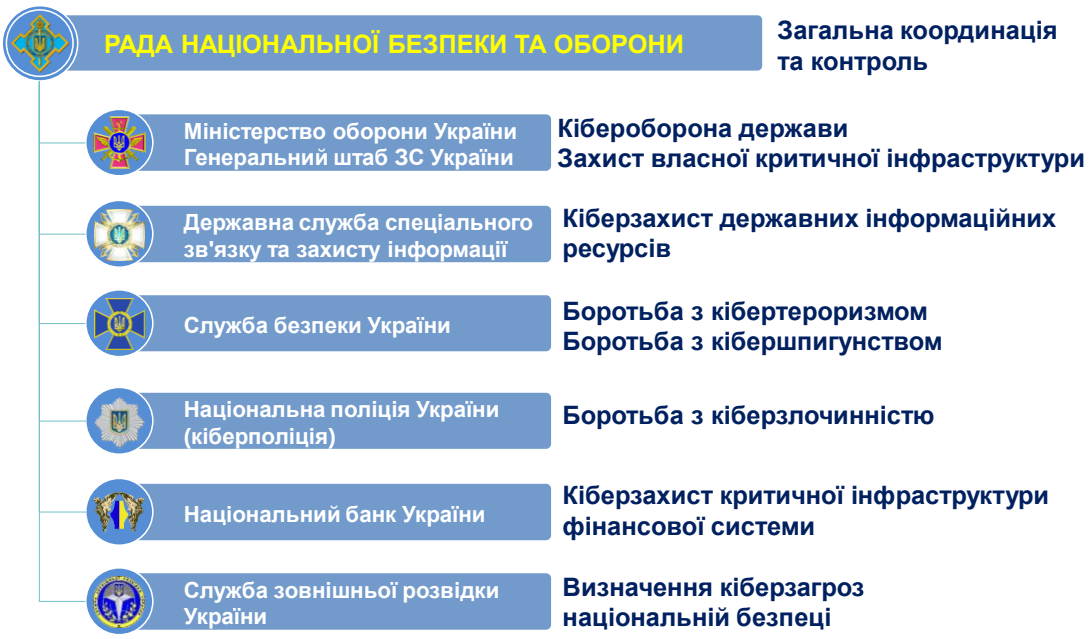

Рис.1.21 Основні завдання суб'єктів забезпечення кібербезпеки України

Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення уразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

1.7.3. Пріоритети та напрями забезпечення кібербезпеки України згідно з чинним законодавством

Пріоритети та напрями забезпечення кібербезпеки України:

Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у:

– виробленні й оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

– створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

– формуванні конкурентного середовища у сфері електронних

комунікацій, наданні послуг із захисту інформації та кіберзахисту;

− розвитку технологій кіберзахисту засобів рухомого зв'язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

− залученні експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

− підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

− проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;

− розвитку та удосконаленні системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

− розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення;

− розвитку мережі команд реагування на комп'ютерні надзвичайні події;

− створенні системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

− розвитку та вдосконаленні системи технічного і криптографічного захисту інформації;

− розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ;

− створенні умов для впровадження в Україні сучасних технологій кіберзахисту.

Кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, має полягати, насамперед, у:

− створенні та забезпеченні функціонування національної телекомунікаційної мережі – єдиної платформи захищених електронних комунікацій органів державної влади;

− упровадженні організаційно-технічної моделі національної системи кібербезпеки, оперативному реагуванні на кібератаки та кіберінциденти;

− розгортанні (відповідно до компетенції) єдиної системи ситуаційних центрів профільних органів державної влади Сектору безпеки і оборони на базі захищеної інформаційної інфраструктури;

− розбудові захищеної інтегрованої системи електронних державних реєстрів, баз даних, дата-центрів, у тому числі єдиного дата-центру резервного

збереження інформації і відомостей державних електронних інформаційних ресурсів;

− удосконаленні системи зберігання, передачі та обробки даних державних реєстрів і баз даних із застосуванням сучасних інформаційно-комунікаційних технологій (включаючи технології on-line-доступу);

− розробленні нових методів запобігання кібератакам, кіберінцидентам та поширенню інформації про них;

− розробленні вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

− підвищенні обізнаності працівників державних органів у сфері інформаційної та кібербезпеки, проведенні відповідних тренінгів, навчань.

Кіберзахист критичної інфраструктури має полягати, насамперед, у:

− комплексному вдосконаленні правової основи кіберзахисту об'єктів критичної інфраструктури, визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури;

− формуванні та забезпеченні функціонування державного реєстру об'єктів критичної інформаційної інфраструктури;

− регламентації вимог до кіберзахисту об'єктів критичної інфраструктури;

− створенні та забезпеченні функціонування власниками (розпорядниками) об'єктів критичної інфраструктури підрозділів кіберзахисту;

− установленні кваліфікаційних вимог для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз, упровадження для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам;

− налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвитку державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

− розробленні та запровадженні механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

Розвиток потенціалу Сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку, зокрема, таких заходів:

− здійснення захисту технологічних процесів на об'єктах критичної інфраструктури, в яких управління або моніторинг здійснюється за допомогою інформаційно-комунікаційних технологій, від несанкціонованого втручання у їх роботу;

− періодичне проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки;

− розроблення та впровадження протоколів спільних дій, зокрема, інформаційного обміну у режимі реального часу, суб'єктів забезпечення кібербезпеки під час виявлення кібератак та кіберінцидентів;

− проведення навчань суб'єктів Сектору безпеки і оборони щодо реагування

на кібератаки та кіберінциденти, зокрема, проведення кібернавчань Збройних Сил України, інших суб'єктів Сектору безпеки і оборони України, участь у таких навчаннях у рамках заходів колективної оборони;

− реалізація державного стратегічного планування та програмно- цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

− здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, Сектору безпеки і оборони у кіберпросторі, створення, розвиток сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватись як засіб стримування військових конфліктів та загроз у кіберпросторі (активний кіберзахист);

− створення єдиного підрозділу із забезпечення кібербезпеки та кіберзахисту Збройних Сил України на стратегічному, оперативному та тактичному рівнях;

− розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, розвідувальних органів, досягнення сумісності із відповідними підрозділами кібербезпеки та кіберзахисту держав – членів НАТО;

− сприяння розвитку системи оперативного реагування на комп'ютерні надзвичайні події;

− удосконалення системи контррозвідувального та оперативно-розшукового забезпечення кібербезпеки держави;

− розвиток та координація проведення наукових досліджень у галузі кібербезпеки та кіберзахисту для потреб національної безпеки і оборони;

− підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також розвідувально-підривної діяльності іноземних спецслужб, організацій, груп та осіб проти України у кіберпросторі;

− обмеження участі у заходах із забезпечення інформаційної та кібербезпеки будь-яких суб'єктів господарювання, які знаходяться під контролем держави-агресора, визнаної Верховною Радою України, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб'єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю у цій сфері;

− розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідне розмежування підслідності;

− розвиток системи підготовки кадрів для потреб органів Сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи.

Боротьба з кіберзлочинністю передбачатиме здійснення в установленому порядку, серед іншого, таких заходів:

− створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів;

− удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;

− запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду;

− унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік;

− врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису;

− упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю;

− підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів;

− запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів;

− підвищення кваліфікації співробітників правоохоронних органів.

1.8. Основи та особливості кібероборони держави

1.8.1. Сутність та основні завдання кібероборони держави

Тенденцією розвитку сучасних підходів до забезпечення національної безпеки у воєнній сфері, ведення збройного протиборства є активне впровадження інформаційних технологій та використання інформаційного простору (включаючи кіберпростір) для досягнення національних інтересів та цілей збройної боротьби. Поява, інституалізація та подальший розвиток інформаційного домену збройного протиборства створює нові можливості для забезпечення національної безпеки держави у воєнній і інших сферах та одночасно несе нові виклики та загрози для реалізації національних інтересів держави.

Інформаційна складова ”гібридної війни”, яку розв’язано проти України, стан забезпечення суверенітету держави в інформаційному просторі, поточна суспільно-політична та фінансово- економічна ситуація в Україні, інші фактори впливу зовнішнього та внутрішнього безпекового середовища вимагають з боку держави, в першу чергу, від Сектору безпеки і оборони України та при підтримці суспільства реалізації комплексу вичерпних заходів реагування на

загрози в кіберпросторі, інформаційної підтримки підготовки та застосування Збройних Сил України та обумовлюють необхідність пошуку та впровадження нових методів, форм та способів дій в кіберпросторі всіма складовими Сектору безпеки та оборони держави, створення ними відповідних спроможностей.

Протягом найближчої перспективи Збройні Сили України, інші суб'єкти забезпечення національної безпеки держави будуть розвиватися та функціонувати (виконувати завдання за призначенням) в умовах:

− зростання рівня загроз національній безпеці держави у воєнній сфері, які реалізуються у кіберпросторі та/або з його використанням;

− активного створення та поширення інформаційних технологій, зростання їх ролі у досягненні цілей збройного протиборства;

− розширення існуючих та появи нових функцій, завдань та повноважень суб'єктів забезпечення національної безпеки, пов'язаних з воєнною безпекою та кібербезпекою, відображених у вимогах (положеннях) нормативно-правових актів держави;

− тенденцій розвитку Збройних Сил країн світу, в першу чергу, членів НАТО щодо дій в кіберпросторі.

До основних загроз обороноздатності держави у кіберпросторі належать:

− здійснення системних і масштабних дій проти України у кіберпросторі іноземними державами (групами держав), недержавними утвореннями, у тому числі, шляхом використання спеціальних засобів активного впливу в кіберпросторі (кіберозброєнь);

− створення та застосування проти України збройних формувань та спецслужб, що спеціалізуються на веденні дій і операцій в кіберпросторі;

− застосування іншою державою або групою держав проти України збройної сили з використанням кіберпростору;

− діяльність у кіберпросторі спрямована на здійснення негативного інформаційно-психологічного впливу на особовий склад Сектору безпеки і оборони, порушення функціонування інформаційної та іншої інфраструктури держави, яка забезпечує виконання завдань оборони;

− проведення противником сучасних інформаційних та кібероперацій із застосуванням спроможностей, які він має в кіберпросторі;

− порушення функціонування та/або руйнування об'єктів критичної інформаційної інфраструктури внаслідок збройної агресії, воєнних дій, у т.ч. у кіберпросторі;

− виявлення та використання противником уразливостей інформаційних технологій та інформаційної інфраструктури з метою порушення функціонування інформаційних систем управління державою, критичною інфраструктурою, силами оборони, системами управління військами та зброєю;

− підготовка та проведення скоординованих заходів у кіберпросторі суб'єктами забезпечення кібербезпеки держави з метою запобігання виникненню воєнних конфліктів, стримування та відсічі воєнної агресії;

− створення сприятливих умов у кіберпросторі для застосування ЗС України, інших військових формувань та правоохоронних органів, їх ефективних дій в кіберпросторі, сприяння забезпеченню інформаційної безпеки держави у воєнній сфері;

– порушення функціонування інформаційної інфраструктури противника, систем (процесів) прийняття ним рішень та здійснення управління військами (силами) при одночасному захисті власного кіберпростору.

Прогноз розвитку безпекового середовища навколо України вимагає вжиття суб'єктами забезпечення національної безпеки держави комплексу невідкладних випереджувальних заходів зі створення необхідного потенціалу Сектору безпеки і оборони держави для відбиття воєнної агресії у кіберпросторі, в першу чергу, щодо підготовки та ведення дій в інтересах оборони держави, іншими словами – підготовки та ведення кібероборони.

Також Україна взяла на себе публічні зобов'язання перед НАТО та країнами-партнерами щодо впровадження сучасних підходів до кібероборони, розвитку необхідних спроможностей Сектору безпеки і оборони держави для дій в кіберпросторі та досягнення оперативної сумісності з питань забезпечення кібербезпеки з Альянсом.

Законодавство України **визначає кібероборону** як складову частину системи заходів щодо оборони держави, яка є сукупністю політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Більш точним визначенням може бути таке: кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії в інформаційному та кіберпросторі.

Закон України "Про оборону України" визначає кібероборону як активний кіберзахист та вимагає, що у разі збройної агресії проти України або загрози нападу на Україну не чекаючи офіційного оголошення стану війни органи державної влади та військового управління розпочинають воєнні дії у кіберпросторі, у т.ч. проведення заходів активного кіберзахисту, інформаційно-психологічних, спеціальних, розвідувальних операцій тощо.

Сказане вимагає формування та реалізації єдиних підходів щодо створення та функціонування системи кібероборони, які мають включати визначення її мети, цілей, принципів, напрямів, основних завдань, процедур створення та функціонування організаційних структур, підготовки та ведення дій в кіберпросторі.

Мета кібероборони полягає у плануванні та організації за єдиним замислом захисту від наявних та прогнозованих інформаційних та кібервпливів на інформаційні ресурси, системи та мережі, програмні і електронні апаратні засоби Сектору оборони держави, а також на свідомість, підсвідомість і морально-психологічний стан особового складу та всебічної протидії ним.

Основні завдання кібероборони:

– підготовка та проведення скоординованих заходів у кіберпросторі суб'єктами забезпечення кібербезпеки держави з метою запобігання виникненню воєнних конфліктів, стримування та відсічі воєнної агресії;

− створення сприятливих умов у кіберпросторі для застосування ЗС України, інших військових формувань та правоохоронних органів, їх ефективних дій в кіберпросторі, сприяння забезпеченню інформаційної безпеки держави у воєнній сфері;

− порушення функціонування інформаційної інфраструктури противника, систем (процесів) прийняття ним рішень та здійснення управління військами (силами) при одночасному захисті власного кіберпростору.

1.8.2. Стратегічні цілі системи кібероборони держави

Для завчасного проведення наведених заходів щодо підготовки та відбиття воєнної агресії у кіберпросторі створюється система кібероборони як організована сукупність суб'єктів та об'єктів кібероборони з визначеними зв'язками між ними, об'єднаних єдиним керівництвом та з підсистемою забезпечення, які реалізують комплекс визначених законодавством України дій в кіберпросторі.

Система кібероборони є одночасно:

− складовою частиною (підсистемою) системи заходів щодо оборони держави, в першу чергу щодо підготовки та застосування Збройних Сил України;

− підсистемою відомчої системи безпечного використання кіберпростору;

− підсистемою національної системи кібербезпеки.

Зазначена система кібероборони на початковому етапі створюється в Міністерстві оборони України та Збройних Силах України. В подальшому, в міру набуття необхідних відомчих спроможностей з кібероборони вона трансформується в національну систему кібероборони.

Кібероборона є основним способом застосування Збройних Сил України щодо забезпечення захисту інтересів держави у воєнній сфері в кіберпросторі та створення сприятливих умов для застосування Збройних Сил України, інших складових Сектору безпеки і оборони в інформаційному (кібер) домені збройного протиборства, яка доповнюється іншими заходами суб'єктів забезпечення кібербезпеки держави відповідно до їх компетенції.

Основним змістом ведення кібероборони є сукупність узгоджених і взаємопов'язаних за метою, завданнями, об'єктами, місцем та часом одночасних і послідовних заходів впливу в кіберпросторі, які готуються та проводяться за єдиним замислом і планом силами та засобами Збройних Сил України із залученням необхідних можливостей інформаційної інфраструктури та ресурсів держави у взаємодії з військовими формуваннями та правоохоронними органами, іншими суб'єктами забезпечення кібербезпеки держави відповідно до їх компетенції щодо запобігання, захисту, стримування, попередження, реагування та мінімізації наслідків від кібервпливу противника.

Дії Міністерства оборони України та Збройних Сил України в кіберпросторі розглядаються у якості узгодженої системи, в якій кожен суб'єкт підготовки та ведення кібероборони виконує свої завдання притаманними йому способами та прийомами, одночасно шляхом інтеграції в єдину систему підвищує ефективність функціонування системи кібероборони в інтересах

досягнення цілей, які визначені перед Міністерством оборони України та Збройними Силами України, виконання військами (силами) завдань за призначенням.

Заходи підготовки та ведення кібероборони в МО України та ЗС України проводяться в єдиній системі загальнодержавних заходів оборони держави та забезпечення її кібербезпеки, у взаємодії з іншими центральними органами виконавчої влади держави, суб'єктами Сектору безпеки і оборони держави, засобами масової інформації, громадськими організаціями, іншими суб'єктами інформаційних відносин.

Кібероборона може вестися в мирний час та в умовах особливого періоду, з введенням правового режиму воєнного стану, правового режиму надзвичайного стану, під час проведення Операції Об'єднаних сил, участі в проведенні антитерористичної операції, а також у випадку залучення підрозділів ЗС України до участі в міжнародних операціях з підтримання миру та безпеки. Головною відмінністю заходів щодо підготовки та ведення кібероборони держави в умовах мирного часу порівняно з особливим періодом є низка обмежень щодо проведення заходів активного кіберзахисту. Діяльність Міністерства оборони України та Збройних Сил України щодо досягнення мети реалізації Стратегії на період до 2022 року передбачає визначення стратегічних цілей, які охоплюють два основні напрями:

– створення та розвитку необхідних та достатніх спроможностей Міністерства оборони України та Збройних Сил України для ефективних дій в інформаційному (кібер) просторі та досягнення оперативної сумісності з НАТО з наведеного напряму;

– практичного виконання поточних заходів щодо реагування на дії противника в кіберпросторі, підготовки та ведення Збройними Силами України кібероборони в повсякденній діяльності, під час підготовки та застосування, у тому числі їх участі в проведенні Операції Об'єднаних сил, антитерористичної операції, а також у випадку залучення підрозділів (персоналу) ЗС України до участі в міжнародних операціях з підтримки миру та безпеки.

Виходячи із вимог, які визначені Законом України "Про основні засади забезпечення кібербезпеки України" та Указом президента України від "Про стратегію кібербезпеки України", стратегічні цілі та основні завдання для їх досягнення щодо створення та розвитку спроможностей Міністерства оборони України та Збройних Сил України полягають у наступному:

Примітка. При визначенні та деталізації стратегічних цілей використана адаптована методика Збройних Сил країн – членів НАТО "DOTMPL-A", яка включає наступі складові "D" – доктрини, "O" – організаційні структури, "T" – підготовка,"M" – матеріально-технічна база, "P" – персонал,"L" – керівництво, "A" – практичні дії.

Стратегічна ціль № 1. Завчасне та всебічне нормативно-правове регулювання діяльності з кібероборони, розроблення концепцій, доктрин, програм.

Основні завдання щодо її досягнення:

− визначення переліку положень у сфері кібероборони, які потребують нормативно-правового урегулювання;

− проведення наукових досліджень щодо розроблення та обґрунтування теоретичних засад нормативно-правового забезпечення діяльності у сфері кібероборони;

− створення та розвиток вітчизняної термінологічної бази у сфері кібероборони;

− організація розроблення та імплементація концепцій, доктрин, програм, планів;

− відображення питань, що стосуються протидії кіберзагрозам у воєнній сфері, відбиття воєнній агресії у кіберпросторі, підготовки, ведення та забезпечення кібероборони, керівництва кібероборoною та її складовими в нормативно-правових актах держави з питань національної безпеки, відомчих нормативних документах;

− розроблення, періодичний перегляд, уточнення та переопрацювання відомчих керівних, плануючих та розпорядчих документів з кібероборони;

− розроблення та імплементація індикаторів та порядку оцінки діяльності суб'єктів кібероборони та стану об'єктів кібероборони;

− розроблення та реалізація процедур інтеграції, взаємної сумісності з нормативними документами НАТО з питань кібербезпеки та дій в кіберпросторі;

− приведення національних і військових стандартів за напрямом кібероборони у відповідність до міжнародних норм та стандартів, що застосовуються в Європейському Союзі та НАТО.

Стратегічна ціль № 2. Випереджувальний розвиток організаційних структур в інтересах виконання завдань кібероборони.

Основні завдання щодо її досягнення:

− розвиток бойового складу Збройних Сил України для виконання завдань кібероборони шляхом створення нових та реорганізації існуючих органів військового управління, військових частин (підрозділів у їх складі);

− створення (визначення) у складі Генерального штабу Збройних Сил України підрозділу, відповідального за організацію та планування кібероборони;

− розвиток у складі розвідувального органу Міністерства оборони України, інших органів управління військової розвідки підрозділів з завданнями здійснення розвідувальної діяльності щодо виявлення загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

− розвиток центрів (підрозділів) захисту інформації та забезпечення кібербезпеки в інформаційно-телекомунікаційній системі Збройних Сил України;

− створення та функціонування принципово нових інноваційних організаційних одиниць у складі органів управління та військ (сил) за напрямом кібербезпеки, у т.ч. експериментальних, навчально-бойових, випробувальних, впроваджувальних тощо;

− створення підрозділів активного кіберзахисту, у т.ч. для виконання завдань пошуку уразливостей (тестування) власних інформаційно-телекомунікаційних систем, об'єктів інформаційної інфраструктури, імітації дій

противника в кіберпросторі під час заходів підготовки військ (сил) тощо;

− створення підрозділів (мобільних груп реагування) для забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури у воєнній сфері;

− розвиток спроможностей щодо виконання завдань у кіберпросторі підрозділів, відповідальних за протидію іноземним технічним розвідкам;

− організаційне виокремлення та інтеграція сил та засобів Збройних Сил України, основною сферою застосування яких є інформаційний (кібер) простір в окремий рід військ шляхом формування Командування інформаційного та кіберпростору Збройних Сил України;

− розвиток спроможностей Сил спеціальних операцій Збройних Сил України для проведення спеціальних та інформаційно-психологічних операцій в кіберпросторі та з використанням кіберпростору;

− розвиток організаційних та інших спроможностей Військової служби правопорядку у Збройних Силах України (після реформування – військової поліції) щодо проведення правоохоронних заходів в інтересах підготовки, ведення та забезпечення кібероборони;

− збереження та розвиток підрозділів військових навчальних закладів та науково-дослідних установ Збройних Сил України, які здійснюють підготовку фахівців та наукові дослідження в інтересах кібероборони та інших заходів забезпечення кібербезпеки держави;

− сприяння розвитку спроможностей суб'єктів забезпечення кібербезпеки держави щодо їх участі у виконанні завдань кібероборони;

− розвиток мобілізаційної компоненти кібероборони шляхом використання складових (можливостей) мобілізації, військової служби в резерві, оперативного резерву, визначення мобілізаційних завдань тощо.

Стратегічна ціль № 3. Всебічна підготовка органів військового управління, військ (сил) до виконання завдань кібероборони.

Основні завдання щодо її досягнення:

− розроблення та впровадження системи підготовки органів військового управління, військ (сил) до виконання завдань кібероборони;

− опанування сучасними формами та способами виконання завдань щодо кібероборони (дій в кіберпросторі) загальновійськовими (видовими, міжвидовими тощо) органами військового управління всіх рівнів, військами (силами), родами військ;

− участь органів військового управління та підрозділів Збройних Сил України у проведенні навчань щодо захисту критичної інформаційної інфраструктури держави;

− участь органів військового управління та підрозділів Збройних Сил України у міжнародних навчаннях з кібероборони та забезпечення кібербезпеки.

Стратегічна ціль № 4. Створення та розвиток матеріально-технічної основи кібероборони.

Основні завдання щодо її досягнення:

− підготовка території держави та її інформаційної інфраструктури до кібероборони (в рамках системи заходів підготовки території держави до оборони);

− створення (залучення) необхідної інформаційної інфраструктури держави всіх форм власності для її використання в інтересах кібероборони та періодичне проведення її огляду;

− забезпечення інтеграції та взаємосумісності інформаційно-телекомунікаційних систем, програмно-технічних засобів систем управління військами та зброєю Збройних Сил України з аналогічними системами інших суб'єктів оборони та забезпечення кібербезпеки держави;

− проведення науково-дослідних та дослідно-конструкторських робіт щодо створення сучасних зразків зброї, програмно-технічних та інших засобів в інтересах виконання завдань кібероборони, забезпечення ними відповідних підрозділів у необхідній кількості;

− створення Єдиної автоматизованої системи управління Збройних Сил України з урахуванням забезпечення її кібербезпеки на необхідному рівні;

− залучення можливостей структур громадянського суспільства (громадських організацій) до виконання завдань у сфері забезпечення кібероборони України (на добровільних засадах);

− розширення співробітництва між державним і приватним секторами, залучення інноваційного потенціалу приватних компаній до наукових досліджень і розробки рішень у сфері забезпечення кібероборони.

Стратегічна ціль № 5. Формування і розвиток людського капіталу як головного фактора успішного виконання завдань кібероборони.

Основні завдання щодо її досягнення:

− створення привабливих умов для проходження військової служби в органах військового управління та підрозділах, на які покладаються виконання завдань кібероборони;

− пошук та залучення до військової служби у відповідних підрозділах обдарованої (талановитої) молоді);

− впровадження сучасних підходів до управління військовою кар'єрою на рівні підходів (стандартів, кращих практик) Збройних Сил країн – членів НАТО, у тому числі механізмів нестандартних індивідуальних підходів до найбільш цінних фахівців;

− створення дієвої системи безперервної підготовки (навчання) та професійного вдосконалення протягом усієї кар'єри для фахівців з питань кібероборони та відповідного кадрового менеджменту в цій галузі;

− запровадження механізмів мотивації особового складу, який займає ключові посади в підрозділах, має унікальні професійні якості та здійснює значний персональний внесок в успішне виконання завдань за призначенням, у т.ч. шляхом підвищення штатно-посадових категорій посад, пільгового обчислення терміну військової служби, додаткового грошового забезпечення (виплати грошової винагороди), надання додаткової відпустки, позачергового забезпечення службовим житлом тощо;

− надання за кошти державного бюджету можливостей щодо розвитку фахівців, у т.ч. шляхом навчання на базі цивільних навчальних закладів, стажування на базі провідних вітчизняних та зарубіжних ІТ-компаній, участі в конференціях, семінарах,інших заходах професійного розвитку.

Стратегічна ціль № 6. Набуття спроможностей та здійснення ефективного керівництво кібероборoною.

Основні завдання щодо її досягнення:

− зміна парадигми мислення та дій керівників (командирів) в сторону набуття ними ментальної готовності та спроможностей виконання завдань (дій) в кіберпрострі та через кіберпростір;

− визначення (встановлення) цілей, що планується досягти в кіберпросторі в інтересах досягнення мети оборони держави (застосування Збройних Сил України);

− визначення порядку керівництва підготовкою та веденням кібероборони;

− інтеграція заходів щодо підготовки та ведення кібероборони в діяльність органів військового управління всіх рівнів як складової частини керівництва підготовкою та застосуванням військ (сил) Збройних Сил України;

− визначення переліку завдань з кібероборони, способів їх виконання та необхідних ресурсів;

− завчасне визначення об’єктів дій в кіберпросторі (ведення кібероборони), шляхів та способів отримання доступу до них та можливостей здійснення впливу;

− завчасне визначення порядку, встановлення та підтримання взаємодії з суб’єктами кібероборони;

− впровадження механізмів та процедур спільного застосування Збройних Сил України, інших суб’єктів забезпечення кібербезпеки держави в інтересах ефективного виконання завдань кібероборони.

Детально зміст заходів щодо досягнення стратегічних цілей № 1-6 розкривається в планах Міністерства оборони України та Збройних Сил України щодо реалізації даної Стратегії та відповідних документах оборонного планування.

Стратегічна ціль № 7. Ефективне виконання поточних заходів щодо випереджувального реагування на дії противника в кіберпросторі, підготовки та ведення Збройними Силами України кібероборони.

Основні завдання щодо її досягнення:

− моніторинг кіберпростору, завчасне виявлення загроз;

− здійснення розвідувальної діяльності щодо виявлення загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

− підтримання сил та засобів для дій в кіберпросторі в готовності до виконання завдань за призначенням, адекватне нарощування їх готовності в залежності від рівня загроз та ступенів реагування на них;

− несення бойового чергування визначених сил та засобів кібероборони;

− проведення поточних заходів підготовки та ведення кібероборони відповідно до компетенції (завдань) органів військового управління всіх рівнів, військових частин, організацій та установ Міністерства оборони України та Збройних Сил України;

− проведення оперативно-розшукових, контррозвідувальних та інших правоохоронних заходів в інтересах кібероборони;

− випереджувальна перевірка на уразливість від кібервпливу об’єктів

кібероборони, об’єктів критичної інформаційної інфраструктури;

− проведення інформаційно-аналітичної діяльності та прогнозування розвитку обстановки у воєнній сфері, пов’язаній з кіберзагрозами та кіберпростором;

− розвиток технологій кіберзахисту засобів рухомого зв'язку, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

− участь у забезпеченні кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура);

− активний кіберзахист власної інформаційної інфраструктури;

− всебічна підготовка до проведення заходів кібероборони;

− створення, впровадження у суб’єктів кібероборони інформаційно-технологічних систем, програмно-апаратних комплексів, засобів кіберзахисту, кібервпливу, підготовка відповідних фахівців, формування та розиток відповідних підрозділів;

− впровадження дієвої системи захисту інформаційно-телекомунікаційних систем, об’єктів інформаційної діяльності суб’єктів оборони держави від кібервпливу (кібератак);

− здійснення поточних заходів військової співпраці з Європейським Союзом і НАТО, пов’язаної з безпекою кіберпростору та спільним захистом від кіберзагроз воєнного характеру;

− розвиток міжнародного співробітництва у сфері забезпечення кібероборони, підтримка міжнародних ініціатив, які відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО для посилення спроможностей України у сфері забезпечення кібероборони, забезпечення участі в заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ;

− випереджувальне та/або оперативне реагування на проведення противником заходів у кіберпросторі та через кіберпростір, мінімізація результатів їх впливу. За необхідності – безпосереднє здійснення заходів кібервпливу та інших заходів в кіберпросторі та через кіберпростір, координація їх проведення та уточнення за необхідності;

− використання потенціалу державно-приватного партнерства, громадських організацій для виконання завдань у сфері забезпечення кібероборони.

Детально зміст заходів щодо досягнення стратегічної цілі № 7 розкривається в плануючих документах Міністерства оборони України та Генерального штабу Збройних Сил України щодо стратегічного застосування Збройних Сил України.

Фінансовими джерелами реалізації заходів Стратегії є видатки Державного бюджету України, допомога від країн-партнерів, кошти від благодійної допомоги та інші ресурси, які не заборонені законодавством України.

Світовий досвід показує, що ефективне вирішення будь-якими військами задач за призначенням та забезпечення ними найбільш повного використання

потенціалу озброєння та військової техніки (ОВТ) можливе лише за умови їх об’єднання в єдиній структурі (відповідно до простору де вони діють або ОВТ, яке застосовують) та наявності раціональної системи управління від стратегічного до тактичного рівня.

У провідних країнах світу при формуванні систем кібербезпеки та кібероборони основною тенденцією стало створення нового виду Збройних Сил – Кіберсил (Кібервійськ) з відповідними кіберкомандуваннями, шляхом об’єднання в єдиній структурі, що відповідає за кібероборону, органів військового управління, сил і засобів, які мають відношення до кіберпростору, з реформуванням, перерозподілом функцій та перепідпорядкуванням військових частин зі зміною, за необхідності, напрямів їх діяльності, корегування наукової та освітньої діяльності наукових центрів та закладів освіти, включно утворення нових структурних підрозділів, закладів освіти, військових частин та підрозділів різних напрямів діяльності для виконання спільних заходів кіберрозвідки, кіберзахисту, активних дій в кіберпросторі, відповідно до мети, завдань, доцільних форм та способів забезпечення кібербезпеки у воєнній сфері (табл. 1.2).

Таким чином, кібероборона – це окрема, особлива, специфічна складова кібербезпеки держави, що має різнопланові повсякденні, поточні та бойові (спеціальні) завдання і функції. Тому, необхідно створювати єдину систему кібероборони під єдиним командуванням, всі складові якої діють узгоджено за єдиним замислом і планом. Відсутність зв’язків між розрізненими елементами знижує ефективність їх застосування. Натомість їх наявність – додає нові спроможності щодо ураження противника, ступінь якого може бути багатократно збільшений за рахунок ланцюгових ефектів кібердій.

Таблиця 1.2

Зведені дані щодо кіберсил (кібервійськ) окремих держав світу

Показники (індикатори)	США	ФРН	Велика Британія	Франція	Польща	Угорщина	Ізраїль	РФ	Україна
Наявність національної Стратегії (доктрини) кібероборони (кібербезпеки). Рік видання діючої	2018	2016	2018	2018	2018	2018	2015	2015	2016
Складові частини (функціональні елементи) Кіберсил	РЕР, РЕБ ІПсО зв'язок та ІС, крипто,	РЕР, РЕБ ІПсО зв'язок та ІС, крипто, гео-інформ забезп	РЕР, РЕБ ІПсО зв'язок та ІС крипто	РЕР, РЕБ ІПсО зв'язок та ІС, крипто	РЕБ, зв'язок та ІС, крипто	РЕБ, зв'язок та ІС, крипто	РЕР, РЕБ ІПсО зв'язок та ІС, крипто	ІПсО	-
Наявність сил кібероборони, як окремого виду ЗС	+	+	+	+	+	+	+	+	-
Чисельність, тис/ % від чисельності ЗС	50/ 2,5%	13,5/ 6%	2/ 1,5%	4/ 1,5%	1/ 1%	1/ 0,4%	> 3/ 5,5%	1/ 0,1%	-
Наявність органу управління (кіберкомандування)	+	+	+	+	+	+	+	+	-
Роки формування,	2009-2019	2017-2021	2017-2021	2015-2019	2018-2021	2019- 2022	2018-2021	2016 -…	-
Рік набуття спроможностей	2018	2021	2021	2018	2021	2020	2021	2015	?
Спосіб формування: на базі існуючих + нова структура	+	+	+	+	+	+	+	-	-
Наявність інтегрованого освітньо-наукового, дослідно-випробувального міжвидового, міжвідомчого військового технологічного закладу вищої освіти (*- цив.)	+	+	+	+	+	+	+*	+	-

Питання самоконтролю

1. Сутність кібербезпеки інформаційного суспільства.
2. Кібербезпека як складова міжнародної, регіональної та національної безпеки.
3. Кіберінциденти: передумови скоєння та наслідки.
4. Загрози у сфері кібербезпеки.
5. Зміст кіберзагроз.
6. Класифікація та ознаки кіберзагроз.
7. Основні характеристики кіберзагроз.
8. Дії у кіберпросторі та їх особливості.
9. Сутність, цілі та задачі кібердій.
10. Класифікація форм і способів дій у кіберпросторі.
11. Суб'єкти та об'єкти кібердій.
12. Система кібердій.
13. Основи кіберрозвідки.
14. Основи кіберзахисту.
15. Основи кібервпливу.
16. Основи міжнародної співпраці з питань забезпечення кібербезпеки.
17. Проблеми забезпечення кібербезпеки на міжнародному рівні.
18. Діяльність Міжнародного союзу електрозв'язку щодо забезпечення кібербезпеки.
19. Напрями міжнародного співробітництва з питань забезпечення кібербезпеки.
20. Напрями забезпечення кібербезпеки України.
21. Основні положення Стратегії кібербезпеки України .
22. Сутність та завдання Національної системи забезпечення кібербезпеки України.
23. Пріоритети та напрями забезпечення кібербезпеки України згідно з чинним законодавством.
24. Основи та особливості кібероборони держави.
25. Сутність та основні завдання кібероборони держави.
26. Стратегічні цілі системи кібероборони держави.

Інформаційні джерела

1. Українські технології асиметричного протиборства: збірник наукових поглядів; за ред. В. Бадрака та Д. Козлова. 2020. К.: ЦДАКР та ОПК. 192 с.
2. Сунь-Цзи. Мистецтво війни; переклад Г.Латника. К.:Арій, 2014. 128 с.
3. William S. Lind, Colonel Keith Nightengale (USA), Captain John F. Schmitt (USMC), Colonel Joseph W. Sutton (USA), Lieutenant Colonel Gary I. Wilson (USMCR) (October 1989). "The Changing Face of War: Into the Fourth Generation". *Marine Corps Gazette* pp. 22–26. URL: https://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html.
4. Слипченко В. И. Войны нового поколения: дистанционные и бесконтактные. М.: Издат. дом “Гран-Пресс”, 2004. 382 с.
5. Слипченко В. И. Войны шестого поколения: оружие и военное искусство будущего. М.: ВЕЧЕ, 2002. 384 с.
6. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского язика. М.: Логос, Наука. 1997. 794 с.
7. Salomon J. What is Technology? The Issue of its origins and definitions // *Historiy of technology*. 1984/ Vol. 1. P. 113-156.
8. Большой энциклопедический словарь. М.: Изд. дом “ОНИКС 21 век”. 2001. 1798 с.
9. Военный энциклопедический словарь. М.: Воениздат, 1983.
10. Военный энциклопедический словарь. М.: Изд. дом “ОНИКС 21 век”. 2002. 1432 с.
11. Стратегія розвитку сфери інноваційної діяльності на період до 2030 року/Розпорядження Кабінету міністрів України від 10 липня 2019 р. № 526-р.
12. Пальчук М.М. Деякі погляди на перспективи подальшого розвитку Збройних Сил України // Наука і оборона. 2001. № 4. С. 28-34.
13. Основи кібернетичної безпеки: монографія / Ю. Г. Даник, Р. В. Грищук; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ. 2016. 636 с.
14. Даник Ю. Г., Пермяков О. Ю. Сучасні інформаційні технології в забезпеченні національної безпеки і оборони: реалії та тенденції розвитку// *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. № 1(31). С. 159–176.
15. Даник Ю.Г. Парадигма високотехнологічності в сучасному воєнному мистецтві // Труди університету.- Київ: Національна академія оборони України. 2009. № 2(92). С.26-34.
16. Телелим В.М., Даник Ю.Г., Чмельов В.О. Основні аспекти стратегії превентивної оборони та її реалізації // Наука і оборона. 2010. № 2. С.15-23.
17. Белозёров В.К. Превентивная политика или превентивные удары? Безопасность Евразии. 2006. № 1.
18. Свечин А. А. Эволюция военного искусства. М.: Академический проект; Жуковский : Кучково поле, 2002.
19. Свечин А.А. Стратегия / Вступ. ст. И.С. Даниленко. Жуковский. М.: Кучково поле. 2003. С. 116.
20. Дьяконов М. Оборонная дипломатия (новые задачи вооруженных сил

Запада в современных условиях)// Зарубежное военное обозрение. 2001. № 5.
21. Перри У. Дж., Картер Э. Б. Превентивная оборона: Новая стратегия безопасности США; пер. с англ. М.: Наука. 2003. 230 с.
22. Китайская военная стратегия: перевод В. В. Малявина. М.: ООО "Издательство АСТ". 2004. 432 с.
23. Основи стратегії національної безпеки та оборони держави: підручник / Дузь-Крятченко О.П., Даник Ю.Г., Лісіцин Е.М., Рось.А.О., Телелим В.М. та ін. К.: НАОУ. 2015.
24. Кэмбел Д., Стоунхаус Дж., Хьюстон Б. Стратегический менеджмент: учебник. М. : ООО Изд-во Проспект. 2003. 336 с.
25. Дружинін В. В., Конторов Д. С. Вопросы военной системотехніки. М.: Воениздат. 1997. 224 с.
26. Вентцель Е. С. Исследование операций: Задачи, принципы, методология. М.: Наука, 1998.
27. Политов В. Доктрина маршала Огаркова. Умное производство. URL: http://www.umpro.ru/index.php?page_id=17&art_id_1=292&group_id_4=49.
28. The d-n-i echo: The Essence of Winning and Losing, by John R. Boyd, 1996 URL: https://danford.net/boyd/essence.htm.
29. Bryant D.J. Critique, Explore, Compare and Adapt (CECA): A New Model for Command Decisionmaking. Defence R&D Toronto Technical Report, DFDC, Toronto TR. 2003. 63 p.
30. Deptula, David A. Effects-Based Operations: Change in the Nature of Warfare, Arlington, VA: Aerospace Education Foundation. 2001. 40 p.
31. The Implementation of Network-Centric Warfare. URL: http://www.iwar.org.uk/rma/resources/ncw/implementation-of-NCW.pdf.
32. Начальник Генерального штаба Вооруженных Сил РФ генерал армии Валерий Герасимов выступил на общем собрании Академии воєнних наук. 04.03.2019. http://redstar.ru/vektory- razvitiya-voennoj-strategii/?attempt=l.
33. Данько Ю. А. Астротурфінг як інструмент віртуальної маніпуляції та політичної пропаганди в умовах інформаційної доби // Сучасне суспільство. 2015. Вип.2(1). С. 38-49. URL: http://nbuv.gov.ua/UJRN/cuc_2015_2(1)__6.
34. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 09 Jul. 2016 - Press Release (2016) 100 Issued on 09 Jul. 2016 Last updated: 29 Mar. 2017 10:55 URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en
35. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. Женева: МСЕ, 2010. С. 55. URL: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru.
36. JP 3-12 Cyberspace Operations, 8 June 2018. URL: https://www.jcs.mil/Portals/ 36/Documents/Doctrine/pubs/jp3_12.pdf.
37. DOD Dictionary of Military and Associated Terms. As of January 2019. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
38. Isaac R. Porche III, Christopher Paul (2013) Redefining Information Warfare Boundaries for an Army in a Wireless World. RAND Corporation. 176 p.

URL: https://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf.

39. Про основні засади забезпечення кібербезпеки України: Закон України (зі змінами) від 05.10.2017 р. № 2163-VIII. Дата оновлення: 08.07.2018. URL: https://zakon.rada.gov.ua/laws/show/ 2163-19.

40. Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2011. URL: http://www.state.gov/secretary/rm/2011/05/163523.htm

41. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ. 2015. 288 с.

42. Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. National security a minority staff report prepared for the use of the committee on foreign relations United States Senate one hundred fifteenth congress second session January 10. 2018. URL: http://www.gpoaccess.gov/congress/index.html.

43. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

44. Начальник Генштабу британського війська: Британія щодня веде війну з Росією. URL: https://www.radiosvoboda.org/a/30217370.html.

45. Співробітництво Україна – ЄС - НАТО з протидії гібридним загрозам у кіберсфері. Аналітичний документ. 2019. К.: Центр глобалістики "Стратегія XXI". 28 с.

46. Danyk Y., Maliarchuk T., Briggs Ch. Hybrid War: High-tech, Information and Cyber Conflicts. Connections: The Quarterly Journal. 2017. Vol. 16, no. 2. pp. 5-24.

47. Alexander Kosenkov. Cyber Conflicts as a New Global Threat. Future Internet, 2016,8, 45. doi:10.3390/fi8030045. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2988455.

48. Про Доктрину інформаційної безпеки України: Указ президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017.

49. Про Стратегію національної безпеки України: Указ Президента України від 26.05.2015 р. № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015.

50. Про Стратегію кібербезпеки України: Указ Президента України від 15.03.2016 р. №96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016.

51. Про Стратегічний оборонний бюлетень України: Указ Президента України від 6.06.2016 р. № 240/2016. URL: https://zakon.rada.gov.ua/laws/show/n0006525-16.

52. Про захист інформації в інформаційно- телекомунікаційних системах: Закон України (зі змінами) від 5.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр.

53. Cybersecurity a generic reference curriculum (2016). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-

curriculum.pdf.

54. Про боротьбу з тероризмом: Закон України (зі змінами) від 20.03.2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15.

55. National Cyber Security Strategy Good Practice Guide (2016). URL: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

56. Присяжнюк М. М., Цифра Є. І., Особливості забезпечення кібербезпеки // Реєстрація, зберігання та обробка даних. 2017. Т. 19. № 2. С. 61-68.

57. Guide to developing a national cybersecurity strategy. (2018). URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

58. Понимание киберпреступности: Руководство для развивающихся стран. (2009). URL: https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf.

59. Шрайдер Ф., Викс Б., Винклер Т. Кибербезопасность: дорога, которую надо пройти. (2013) / URL: https://www.dcaf.ch/sites/default/files/publications/documents/Horizon_4_Cyber_Road_Ahead_RUS.pdf.

60. Global Cybersecurity Agenda. (2008). URL: https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf.

61. AJP-3.10 Allied Joint Doctrine for Information Operations. Edition A Version 1. DECEMBER 2015.

62. Спільна доктрина Збройних Сил США JP 3-13.2 “MISO (PsyOps)”.

63. Графічний навчальний посібник (graphic training aid - GTA) GTA 33-01-001United States Army John F. Kennedy Special Warfare Center and School (USAJFKSWCS).

64. Венесуела залишилася без електрики: URL: https://glavcom.ua/world/observe/venesuela-zalishilasya-bez-elektriki-575648.html

65. Блэкаут в Венесуэле - Хуан Гуайдо решил ввести режим ЧП URL: https://vesti-ukr.com/mir/328311-blekaut-v-venesuele-khuan-huajdo-reshil-vvesti-rezhim-chp

66. США расширили санкции против Венесуэлы. URL: https://www.facenews.ua/news/2019/443568/.

Даник Ю.Г., Вдовенко С.Г. Ланцюгові ефекти в кібердіях: Збірник наукових праць ВІ КНУ імені Тараса Шевченка. Вип. 64. 2019. С. 71-90. http://mil.univ.kiev.ua/files/253_320018412.pdf

Розділ 2 ТЕХНОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ

Розглянуті в першому розділі основні заходи забезпечення кібербезпеки та кібероборони показали, що у загальному сенсі, вони охоплюють потреби людини, суспільства та держави в інформаційному та кіберпросторі, які не можна виокремити один від одного.

Тому, в якості методологічної основи дослідження кібербезпеки соціотехнічних систем необхідно застосовувати так званий системний підхід або системний аналіз. Системний підхід виступає як засіб методологічного аналізу кібербезпеки, застосування якого дозволяє досягти найбільш глибокого осмислення явищ, виділити складові елементи системи, побачити їх взаємозв'язки і взаємозалежність структурних і функціональних компонентів. Системний підхід у дослідженнях кібербезпеки є головним принципом і методом дослідження.

Отже, процеси управління, що пов’язані з інформацією (зберігання, розповсюдження, обробка тощо), необхідно розглядати як питання кібербезпеки інформаційної складової в кіберпросторі. Якщо це стосується виконання будь-яких дій по відношенню до об’єктів інфраструктури, то це кібербезпека критичної інфраструктури або критичної системи в енергетичній, економічній та інших сферах. Якщо це пов’язано з роботою автономних систем (система озброєння, банківська система), то це кібербезпека таких систем.

На даний час питання забезпечення кібербезпеки поки що розглядаються окремо для різних систем. У цьому розділі будуть розглянуті лише технологічні аспекти забезпечення кібербезпеки в інформаційно-телекомунікаційних системах.

2.1. Характеристика основних завдань управління кібербезпекою

Відповідно до чинного законодавства України [1, 2] серед пріоритетів державної політики у сфері кібербезпеки є формування умов для забезпечення кіберзахисту інформаційної інфраструктури України, передусім – об’єктів критичної інформаційної інфраструктури держави.

Під **об’єктом критичної інформаційної інфраструктури** розуміється комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине стале функціонування такого об’єкта критичної інфраструктури [2].

До **об’єкта критичної інфраструктури** або критично важливого об’єкта інфраструктури, згідно з [2], відносяться підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з

технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Постановою Кабінету Міністрів України 19 червня 2019 року № 518 були затверджені Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [3]. Ці Загальні вимоги визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури, що є обов'язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури.

Також були введені наступні терміни:

− *критичні бізнес/операційні процеси об'єкта критичної інфраструктури* – процеси організації функціонування об'єктів критичної інфраструктури, реалізація загроз на які призводить до виведення з ладу або порушення функціонування самого об'єкта критичної інфраструктури та відповідно справляє негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіює майнову шкоду та/або становить загрозу для суспільства, життя і здоров'я людей; для організації функціонування цього процесу можуть використовуватися декілька інформаційно-телекомунікаційних систем;

− *система інформаційної безпеки* – сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, запобігання порушенню режиму функціонування та/або недоступності служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, порушенню функціонування компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; забезпечення спостережності за діями користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та функціонуванням засобів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

− *політика інформаційної безпеки* – політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки.

Впровадження організаційних та технічних заходів з кіберзахисту на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які визначені в [3], повинні забезпечувати:

− формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки;

− управління доступом користувачів та адміністраторів до об’єктів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

− ідентифікацію та автентифікацію користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

− реєстрацію подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит;

− мережний захист компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

− доступність та відмовостійкість компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

− визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

− визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

− визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Процес впровадження кібербезпеки на об’єктах критичної інфраструктури за Загальними вимогами [3] можна представити моделлю PDCA (англ. *Plan-Do-Check-Act* – планування – дія – перевірка – коригування), відомий як цикл Демінга *(Deming Cycle)*. Ця модель знайшла застосування в нормах ISO, таких як: ISO 9001 – Система управління якістю; ISO 14001 – Системи управління навколишнім середовищем; OHSAS 18001 – Система управління безпекою і гігієною праці; ISO 27001 – Система управління інформаційною безпекою; ISO 17025 – Загальні вимоги, що стосуються компетенції дослідних та калібрувальних лабораторій.

Розглянемо застосування моделі PDCA для процесів Системи управління інформаційною безпекою (СУІБ) [4, 5]:

− Plan (планування) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;

− Do (дія) – етап реалізації та впровадження відповідних заходів;

− Check (перевірка) – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;

− Act (поліпшення) – виконання превентивних і коригуючих дій.

Враховуючи зазначене процес, впровадження кібербезпеки за Загальними вимогами буде мати наступний вигляд (рис. 2.1) [6].

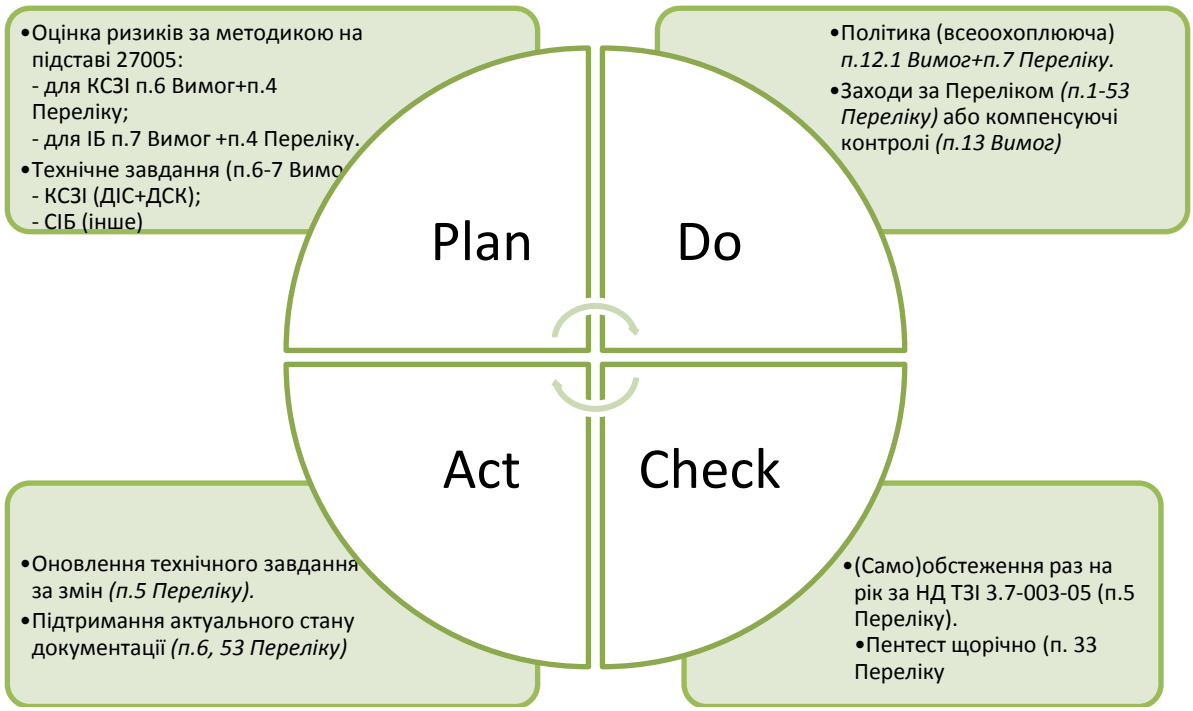

Рис. 2.1. Процес впровадження кібербезпеки за Загальними вимогами

Згідно з міжнародними стандартами ISO/IEC 27001, 27005 [4, 5], управління інформаційною безпекою (кібербезпекою) – це циклічний процес, який складається з:

– усвідомлення необхідності захисту інформації та забезпечення живучості інформаційно-телекомунікаційної системи;

– збору та аналізу інформації про стан забезпечення кібербезпеки в інформаційно-телекомунікаційній системі;

– оцінки інформаційних ризиків;

– планування заходів по усуненню (зменшенню, нейтралізації) ризиків;

– реалізації відповідних механізмів контролю;

– розподілу ролей та відповідальності;

– навчання та мотивації персоналу;

– оперативної роботи по реалізації заходів безпеки;

– моніторингу функціонування механізмів контролю, оцінки їхньої ефективності та визначення відповідних коригуючих заходів.

В цьому ж стандарті визначені **принципи управління** інформаційною безпекою:

– комплексний підхід – управління повинно охоплювати всі елементи і підсистеми ІТС та враховувати всі ризикоутворюючі фактори;

– відповідність призначенню та завданням застосування Збройних Сил (організації);

– високий рівень керованості (можливість змінювати налаштування та режими функціонування в реальному часі);

– адекватність (релевантність, повнота, достовірність) інформації, яка використовується для управління;

– ефективність – оптимальний баланс між реалізованим ступенем кібербезпеки та затратами;

– безперервність управління;

– замкнений цикл планування, впровадження, перевірки, аудиту і коригування.

Удосконалену схему процесу управління кібербезпекою в загальному вигляді побудувати таким чином (рис. 2.2):

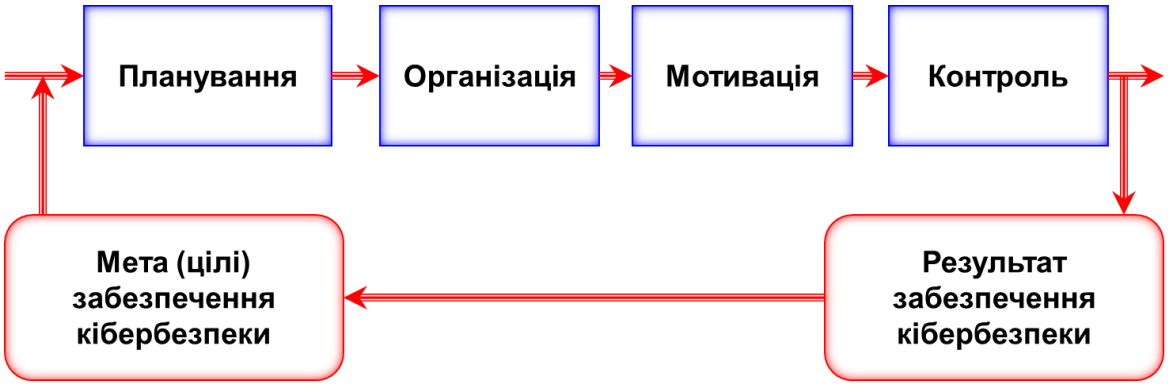

Рис. 2.2. Схема процесу управління кібербезпекою

Основними процедурами управління кібербезпекою в цьому випадку можуть бути:

На етапі *планування*:

– проектування захищених інформаційно-телекомунікаційних систем;

– розробка політики безпеки;

– планування заходів безпеки;

– вибір засобів забезпечення безпеки;

– планування застосування сил забезпечення кібербезпеки.

На етапі *організації*:

– реалізація захищених інформаційно-телекомунікаційних систем;

– реалізація політики безпеки;

– проведення заходів безпеки;

– застосування сил забезпечення кібербезпеки.

На етапі *мотивації*:

– управління особовим складом сил забезпечення кібербезпеки;

– підготовка особового складу;

– проведення навчань по забезпеченню кібербезпеки.

На етапі *контролю*:

– контроль проведених заходів;

– аудит кібербезпеки;

– розслідування кіберінцидентів;

– прийняття рішення на коригування заходів забезпечення кібербезпеки.

2.2. Характеристика сучасних кібератак на інформаційно-телекомунікаційні системи та інформаційні ресурси в умовах ведення кібервійни

2.2.1. Сутність та класифікація кібератак на інформаційно-телекомунікаційні системи та інформаційні ресурси

Основною загрозою об'єктам інформаційної інфраструктури – інформаційно-телекомунікаційним (інформаційним, телекомунікаційним) системам є кібератаки.

Згідно з Законом України "Про захист інформації в інформаційно-телекомунікаційних системах" розглянемо деякі визначення:

− *інформаційна (автоматизована) система* – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

− *телекомунікаційна система* – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

− *інформаційно-телекомунікаційна система* – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" [7] розглянемо деякі визначення:

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей:

− порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів;

− порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем;

− використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Кіберінцидент – подія або низка несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого

управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Інститут AV-TEST щодня реєструє понад 350 000 нових шкідливих програм (шкідливих програм) та потенційно небажаних програм (PUA – potentially unwanted application), кількість нових штамів вірусів перевищує 140 млн. в рік. Вони розглядаються і класифікуються за своїми характеристиками і зберігаються. Програми візуалізації потім перетворюють результати в діаграми, які можна оновлювати і створювати поточну статистику шкідливих програм. На рис 2.3 показана діаграма зростання кількості шкідливого програмного забезпечення, на які немає готових засобів та механізмів реагування.

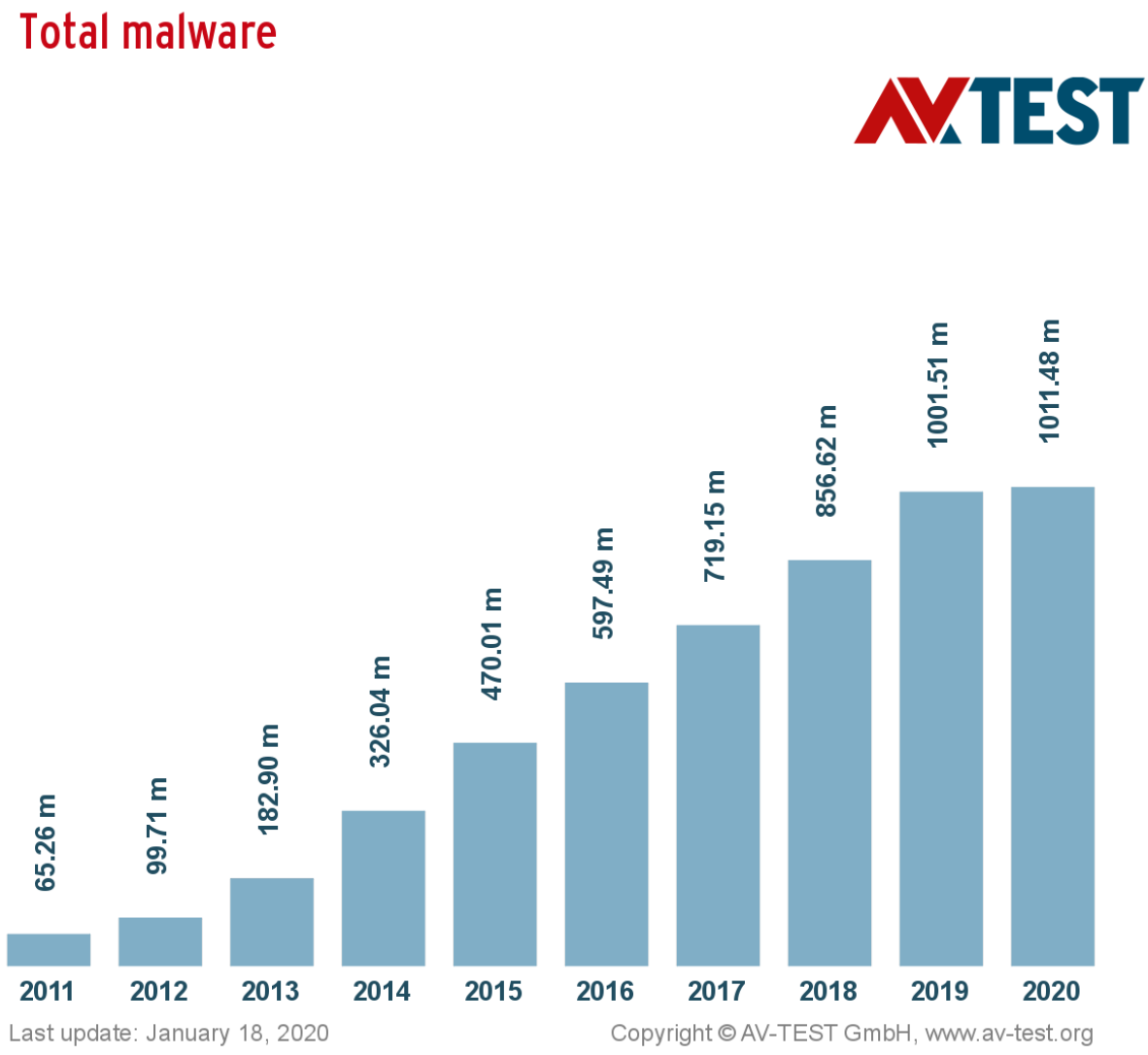

Рис. 2.3. Діаграма зростання кількості шкідливого програмного забезпечення

Якщо прирівнювати кібератаку до інформаційно-технічного впливу, то можна скористатися наступною класифікацією [8, 9].

Перш за все, слід розглянути класифікацію кібератак за характеристиками захищеності інформації.

Так, кібератаки можуть порушувати:

Конфіденційність інформації – властивість інформації, яка полягає в тому,

що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації та видалення.

Доступність інформації – властивість інформаційного ресурсу, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу. Суть властивості полягає в тому, що потрібний інформаційний ресурс знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Спостережність інформаційно-телекомунікаційної системи – ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою.

Усі кібератаки можна здійснити за допомогою:

− технічних засобів (шпигунське устаткування (key-логери, аналізатори бездротових пакетів), апаратні закладки, генератори та боєприпаси електромагнітного імпульсу тощо);

− програмних засобів (бот-мережі, трояни, віруси, хробаки, експлойти, руткіти, бекдори, програми підбору паролів, шпигунські програми, сніфери).

− За характером кібератаки бувають:

− пасивні;

− умовно-пасивні;

− активні.

Пасивна дія не чинить безпосереднього впливу на роботу ІТС, але може порушити її політику безпеки.

Активні дії мають за мету нанесення прямого збитку ІТС, полягають в порушенні конфіденційності, цілісності і доступності інформації, а також виводять зі строю комп’ютерні телекомунікації і здійснюють психологічні впливи на користувачів ІТС.

Умовно-пасивні дії мають за мету підготовку до активної дії. Вони спрямовані на ведення комп’ютерної розвідки і подолання системи захисту ІТС.

Можна навести ще достатню кількість різних класифікацій, але основною є класифікація кібератак за метою здійснення впливу. Так можна окремо розглядати інформаційно-технічні впливи, які проводяться з метою:

− виведення з ладу об’єктів інформаційної інфраструктури та інформаційно-телекомунікаційних систем;

− блокування доступу до інформаційних ресурсів;

− прослуховування інформаційних каналів;

− несанкціонованого доступу до інформаційних ресурсів;

− контролю інформаційного простору.

Загальноприйнятою сьогодні є наступна класифікація кібератак:

− віддалене проникнення (remote penetration);
− локальне проникнення (local penetration);
− атака на відмову в обслуговуванні (denial of service);
− мережні сканери (network scanners);
− сканери уразливостей (vulnerability scanners);
− зламувачі паролів (password crackers);
− аналізатори протоколів (sniffers);
− спам e-mail (Mailbombing);
− перехоплення каналу зв’язку (Man-in-the-Middle).

Деякі розглянемо більш детально.

DoS (від англ. Denial of Service – відмова в обслуговуванні) – атака, що має своєю метою змусити сервер не відповідати на запити. Такий вид атаки не передбачає отримання деякої секретної інформації, але іноді буває підмогою в ініціалізації інших атак. Наприклад, деякі програми через помилки у своєму коді можуть викликати виняткові ситуації, і при відключенні сервісів здатні виконувати код, наданий зловмисником, або атаки лавинного типу, коли сервер не може обробити величезну кількість вхідних пакетів.

DDoS (від англ. Distributed Denial of Service – розподілена DoS) – підтип DoS атаки, має ту саму мету що і DoS, але що проводяться не з одного комп’ютера, а з декількох комп'ютерів у мережі. У даних типів атак використовується або виникнення помилок, що призводять до відмови сервісу, або спрацьовування захисту, що приводить до блокування роботи сервісу, а в результаті також до відмови в обслуговуванні. DDoS використовується там, де звичайний DoS неефективний. Для цього кілька комп'ютерів об’єднуються, і кожен виробляє DoS-атаку на систему жертви. Разом це називається DDoS-атака.

Аналізатори протоколів (sniffers) – досить поширений вид атаки, заснований на роботі мережної карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. В такому режимі всі пакети, отримані мережною картою, пересилаються на обробку спеціальному додатку, званому сніффером. В результаті зловмисник може отримати значну кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці пакети проходили. Найбільшою небезпекою такої атаки є отримання самої інформації, наприклад, логінів і паролів співробітників, які можна використовувати для незаконного проникнення у систему під виглядом звичайного співробітника компанії.

Mailbombing вважається найстарішим методом атак, хоча суть його проста і примітивна: значна кількість поштових повідомлень роблять неможливими роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Для цієї мети було розроблено безліч програм, і навіть недосвідчений користувач міг зробити атаку, вказавши всього лише e-mail жертви, текст повідомлення, і кількість необхідних повідомлень. Такі програми дозволяють ховати реальний IP-адрес відправника, використовуючи для розсилки анонімний поштовий сервер. Цю атаку складно запобігти, тому що навіть поштові фільтри провайдерів не можуть визначити реального відправника спаму. Провайдер

може обмежити кількість листів від одного відправника, але адреса відправника і тема часто генеруються випадковим чином.

Man-in-the-Middle – вид атаки, коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. При отриманні доступу на такому рівні зловмисник може модифікувати інформацію потрібним йому чином, щоб досягти своєї мети. Мета такої атаки – незаконне отримання, крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі. Такі атаки вкрай складно відстежити, оскільки зазвичай зловмисник знаходиться всередині організації.

Всі розглянуті підходи до класифікації кібератак характеризують їх загальні риси, однак недостатньо деталізовані і не враховують особливостей функціонування самої інформаційно-телекомунікаційної системи. Тому ми розглянемо узагальнений підхід до класифікації кібератак.

В основі даного підходу до класифікації кібератак лежить базова еталонна модель взаємодії відкритих систем OSI (рис. 2.4).

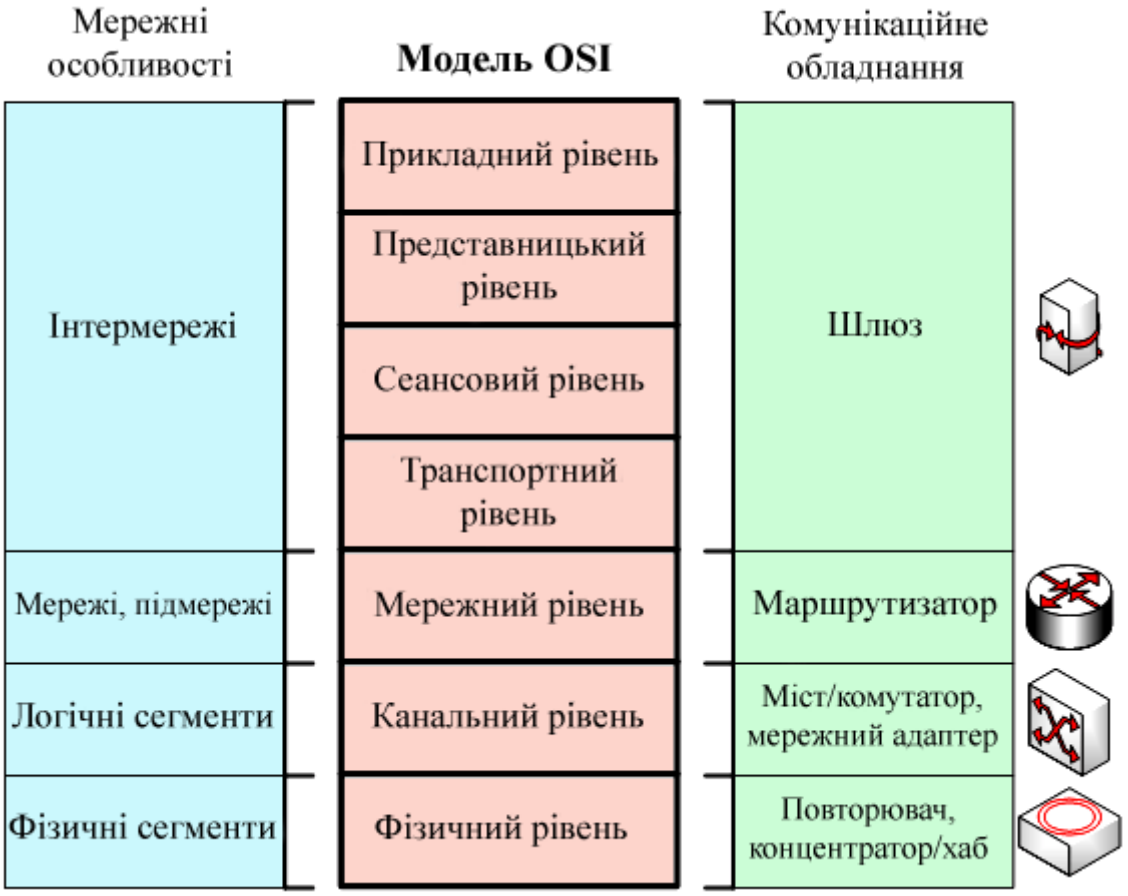

Рис. 2.4. Зв’язок рівнів моделі OSI, мережних структур та пристроїв комунікацій

Модель OSI (EMBBC) (базова еталонна модель взаємодії відкритих систем, англ. *Open Systems Interconnection Basic Reference Model*, 1978 р.) – абстрактна мережна модель для комунікацій і розробки мережних протоколів. Представляє рівневий підхід до мережі. Кожен рівень обслуговує свою частину

процесу взаємодії. Завдяки такій структурі спільна робота мережного обладнання й програмного забезпечення стає набагато простішою, прозорішою й зрозумілішою.

Модель складається з семи рівнів, розташованих вертикально один над іншим. Кожен рівень може взаємодіяти тільки зі своїми сусідами й виконувати відведені тільки йому функції.

Прикладний рівень (Application layer). Верхній (сьомий) рівень моделі, забезпечує взаємодію мережі й користувача. Рівень дозволяє додаткам користувача доступ до мережних служб, таким як обробник запитів до баз даних, доступ до файлів, пересиланню електронної пошти. Також відповідає за передачу службової інформації, надає додаткам інформацію про помилки й формує запити до рівня подання.

Представницький рівень (Presentation layer). Цей рівень відповідає за перетворення протоколів і кодування/декодування даних. Запити додатків, отримані з прикладного рівня, він перетворить у формат для передачі по мережі, а отримані з мережі дані перетворить у формат, зрозумілий додаткам.

На цьому рівні може здійснюватися стиснення/розпакування або кодування/декодування даних, а також перенапрямок запитів іншому мережному ресурсу, якщо вони не можуть бути оброблені локально.

Сеансовий рівень (Session layer). Відповідає за підтримку сеансу зв’язку, дозволяючи додаткам взаємодіяти між собою тривалий час. Рівень керує створенням/завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди неактивності додатків. Синхронізація передачі забезпечується розміщенням у потік даних контрольних точок, починаючи з яких відновлюється процес при порушенні взаємодії.

Транспортний рівень (Transport layer). Четвертий рівень моделі OSI, призначений для доставлення даних без помилок, втрат і дублювання в тій послідовності, у якій вони були передані. При цьому немає значення, які дані передаються, звідки й куди, тобто він визначає сам механізм передачі. Блоки даних він розділяє на фрагменти, розмір яких залежить від протоколу, короткі об’єднує в один, довгі розбиває. Протоколи цього рівня призначені для взаємодії типу точка-точка.

Мережний рівень (Network layer). Третій рівень мережної моделі OSI, призначений для визначення шляху передачі даних. Відповідає за трансляцію логічних адрес й імен у фізичні, визначення найкоротших маршрутів, комутацію й маршрутизацію пакетів, відстеження неполадок і заторів у мережі. На цьому рівні працює такий мережний пристрій, як маршрутизатор.

Канальний рівень (Data Link layer). Цей рівень призначений для забезпечення взаємодії мереж на фізичному рівні й контролю за помилками, які можуть виникнути. Отримані з фізичного рівня дані він упаковує в кадри даних, перевіряє на цілісність, якщо потрібно виправляє помилки й відправляє на мережний рівень. Канальний рівень може взаємодіяти з одним або декількома фізичними рівнями, контролюючи й управляючи цією взаємодією. Специфікація IEEE 802 розділяє цей рівень на 2 підрівні – MAC (Media Access

Control) регулює доступ до поділюваного фізичного середовища, LLC (Logical Link Control) забезпечує обслуговування мережного рівня. На цьому рівні працюють комутатори, мости й мережні адаптери.

MAC-підрівень забезпечує коректне спільне використання загального середовища, надаючи його в розпорядження тієї або іншої станції мережі. Також додає адресну інформацію до фрейма, позначає початок і кінець фрейма.

LLC-рівень відповідає за достовірну передачу кадрів даних між вузлами, а також реалізовує функції інтерфейсу з мережним рівнем за допомогою фреймування кадрів. Також здійснює ідентифікування протоколу мережного рівня.

У програмуванні цей рівень представляє драйвер мережної карти, в операційних системах є програмний інтерфейс взаємодії канального й мережного рівня між собою, це не новий рівень, а просто реалізація моделі для конкретної ОС. Приклади таких інтерфейсів: NDIS, ODI.

Фізичний рівень (Physical layer). Найнижчий рівень моделі, призначений безпосередньо для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів через середовище передавання та їхній прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів. Інакше кажучи, здійснює інтерфейс між мережним носієм і мережним пристроєм. На цьому рівні працюють концентратори й повторювачі (ретранслятори) сигналу. Фізичний рівень визначає електричні, процедурні і функціональні специфікації для середовища передачі даних, в тому числі розніми, розпаювання і призначення контактів, рівні напруги, синхронізацію зміни напруги, кодування сигналу.

Цей рівень приймає кадр даних від канального рівня, кодує його в послідовність сигналів, які потім передаються у лінію зв'язку. Передача кадру даних через лінію зв'язку вимагає від фізичного рівня визначення таких елементів: тип середовища передавання (дротовий або бездротовий, мідний кабель або оптичне волокно) і відповідних конекторів; як повинні бути подані біти даних у середовищі передавання; як кодувати дані; якими повинні бути схеми приймача і передавача.

Фізичним рівнем в лінію зв’язку кадр даних (фрейм) не передається як єдине ціле. Кадр подається як послідовність сигналів, що передаються один за одним.

У сучасних мережах використовуються три основних типи середовища передавання: мідний кабель, оптичне волокно та бездротове середовище передавання. Тип сигналу, за допомогою якого здійснюється передавання даних, залежить від типу середовища передавання. Для мідного кабелю сигнали, що подають біти даних, є електричними імпульсами, для оптичного волокна – імпульсами світла. У випадку використання бездротових з’єднань сигнали є радіохвилями (електромагнітними хвилями).

Коли пристрій, що працює на фізичному рівні кодує біти кадру в сигнали для конкретного середовища передавання, він має розрізняти кадри. Тобто позначати, де закінчується один кадр і починається інший. Інакше мережні пристрої, що здійснюють прийом сигналів, не зможуть визначити, коли кадр

буде отриманий повністю. Відомо, що початок і кінець кадру позначається на канальному рівні, але в багатьох технологіях фізичний рівень також може додати спеціальні сигнали, що використовуються тільки для позначення початку і кінця кадру даних.

Технології фізичного рівня визначаються стандартами, що розробляються такими організаціями: The International Organization for Standardization (ISO), The Institute of Electrical and Electronics Engineers (IEEE), The American National Standards Institute (ANSI), The International Telecommunication Union (ITU), The Electronics Industry Alliance/Telecommunications Industry Association (EIA/TIA) та інші. Дані стандарти охоплюють чотири області, що належать фізичному рівню: фізичні та електричні властивості середовища передавання; механічні властивості (матеріали, розміри, розпаювання контактів конекторів); кодування (подання бітів сигналами); визначення сигналів для управління інформацією. Всі компоненти апаратного забезпечення такі, як мережні карти (Network interface card, NIC), інтерфейси і конектори, матеріали кабелів та їх конструкція визначаються стандартами фізичного рівня. Можна зазначити, що функції фізичного рівня вбудовані у мережне обладнання (hardware).

Основними функціями фізичного рівня є: фізичні компоненти, кодування даних, передавання даних. Фізичні компоненти – електронне обладнання, середовище передавання і конектори, через які передаються сигнали, подані бітами даних.

Кодування є процесом, за допомогою якого потік бітів даних перетворюється у певний код. Кодування здійснюється над групою бітів. Це необхідно для того, щоб забезпечити створення передбачуваної комбінації кодів, яка буде правильно розпізнаватися, як передавачем, так і приймачем.

Використання передбачуваної комбінації кодів допомагає розрізняти біти даних від бітів, що використовуються для управління, а також забезпечує краще виявлення помилок у середовищі передавання. При створенні кодів даних, методи кодування фізичного рівня також забезпечують створення кодів управління, що допомагають, наприклад, визначати початок і кінець кадру.

Відповідно до моделі OSI та мети кібератаки можна класифікувати наступним чином:

1. Можливою метою кібератаки визначити:

− проведення технічної комп’ютерної розвідки;

− використання шкідливого програмного забезпечення;

− викрадення, знищення або модифікацію інформації:

− відмову в обслуговуванні;

− зміну напряму трафіка.

2. Для кожного типу кібератак визначати рівень моделі OSI та обладнання, на якому вона найбільше проявляється;

Деталізувати кожний тип кібератак за способами реалізації. Тоді, всі кібератаки можна надати у вигляді табл. 2.1 [12].

Таблиця 2.1

Узагальнена класифікації кібератак

Тип кібератаки	Спосіб реалізації кібератаки	Область виявлення кібератаки
1. Технічна комп'ютерна розвідка		
1.1. Аналіз мережного трафіка	1.1.1. Аналіз пакетів даних на канальному рівні	Канал зв'язку
	1.1.2. Аналіз пакетів даних на мережному рівні	
1.2. Сканування комп'ютерної мережі та визначення її уразливостей	1.2.1. Сканування пакетом TCP з прапорцем SYN (Синхронізація (Synchronize) використовується для встановлення з'єднання між хостами)	Комутатори, маршрутизатори, ПЕОМ, сервери
	1.2.2. Сканування пакетом TCP з прапорцем FIN (Фініш (Finish) вказує на завершення з'єднання)	
	1.2.3. Сканування пакетом TCP з прапорцем ACK (Підтвердження (Acknowledge) успішності отримання TCP-сегмента)	
	1.2.4. Сканування пакетом TCP з прапорцем NULL	
	1.2.5. Сканування пакетом UDP (один з найпростіших протоколів транспортного рівня моделі OSI, який виконує обмін повідомленнями без підтвердження та гарантії доставки)	
	1.2.6. Сканування пакетом ICMP (використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних)	
1.3. Сканування протоколів передачі даних	1.3.1. Сканування за протоколом RIP (один із найрозповсюдженіших протоколів маршрутизації в невеликих комп'ютерних мережах, який дозволяє маршрутизаторам динамічно оновлювати маршрутну інформацію (напрямок і дальність в хопах (процесах передачі мережних пакетів між хостами мережі), отримуючи її від сусідніх маршрутизаторів)	Комутатори, маршрутизатори, ПЕОМ, сервери
	1.3.2. Сканування по протоколу OSPF (протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху алгоритм Дейкстри)	
	1.3.3. Сканування за протоколом SNMP (протокол керування мережами зв'язку на основі архітектури TCP/IP)	
	1.3.4. Сканування за протоколом HTTP (протокол передачі гіпертекстових документів)	
	1.3.5. Сканування за протоколом DNS (ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережного пристрою) в IP-адресу)	

Тип кібератаки	Спосіб реалізації кібератаки	Область виявлення кібератаки
	1.3.6. Сканування за протоколом TELNET (мережний протокол для реалізації текстового інтерфейсу по мережі)	
	1.3.7. Сканування за протоколом POP3 (протокол, що використовується клієнтом для доступу до повідомлень електронної пошти на сервері)	
	1.3.8. Сканування за протоколом NNTP (основний і єдиний протокол, за допомогою якого користувачі можуть підключатися до news-серверів і брати участь у дискусіях)	
	1.3.9. Сканування за протоколом FINGER (протокол для отримання інформації про користувачів локальних та віддалених комп'ютерів)	
	1.3.10. Сканування за протоколом FTP (протокол передачі файлів)	
	1.3.11. Сканування за протоколом TFTP (простий, покроково синхронізований протокол передачі файлів, який дозволяє клієнтам зчитувати або записувати файли сервера)	
	1.3.12. Сканування за протоколом RLOGIN (забезпечує віртуальний термінал з віддаленою відповіддю та з локально керованим потоком і з належним скиданням буферів виходу)	
	1.3.13. Сканування за протоколом IDENT (призначений для ідентифікації користувача, який встановлює TCP-з'єднання)	
	1.3.14. Сканування за протоколом IMAP (мережний протокол прикладного рівня для доступу до електронної пошти)	
	1.3.15. Сканування за протоколом RPC (протокол, що дозволяє програмі, запущеній на одному комп'ютері, бути викликаною на іншому комп'ютері без написання безпосередньо коду для цієї операції)	
2. Використання шкідливого програмного забезпечення		
2.1. Локальне проникнення в комп'ютерну мережу	2.1.1. Ransomware (спливаюче вікно з повідомленням, що Ваш комп'ютер заблокований і що Ви не зможете отримати до нього доступ, якщо не заплатите)	ПЕОМ, сервери
	2.1.2. Rootkit (програма або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі. Це такий спеціальний модуль ядра, який хакер встановлює на зламаній ним комп'ютерній системі відразу після отримання прав суперкористувача. Цей набір, як правило, включає всілякі утиліти для «замітання слідів»	

Тип кібератаки	Спосіб реалізації кібератаки	Область виявлення кібератаки
	вторгнення у систему, сніфери, сканери, кейлоггери, «троянські» програми, що заміщають основні утиліти)	
	2.1.3. Троянський кінь (шкідлива програма, яка видає себе за безпечний та корисний застосунок, для того аби переконати жертв встановити її на комп'ютер)	
	2.1.4. Spyware (моніторинговий програмний продукт, що встановлений і вживається без належного сповіщення користувача, його згоди і контролю з боку користувача, тобто несанкціоновано встановлений)	
2.2. Віддалене проникнення в комп'ютерну мережу	2.2.1. Knobe (Kernel Hook Bypassing Engine, програма, яка до перевірки антивірусом є абсолютно безпечною. Після перевірки код програми замінюється іншим)	ПЕОМ, сервери, маршрутизатори
	2.2.2. Засоби віддаленого адміністрування	
	2.2.3. BrowserHijackers (програми, які замінюють початкову сторінку, сторінку, яка запитується, результати пошуку, дані про помилку іншими сторінками, які користувач не запитував)	
	2.2.4. Bot-коди (програми, які призначені для автоматизації контролю параметрів і адміністрування каналів IRC (Internet Relay Chat)	
3. Викрадення, знищення або модифікація інформації		
3.1. Злам паролів	3.1.1. Комп'ютерні віруси, призначені для зміни системних файлів	ПЕОМ, сервери, комутатори, маршрутизатори
	3.1.2. Апаратні закладки	
	3.1.3. Метод перебору даних у системних файлах SAM та SYSTEM	
	3.1.4. Програми для скидання паролів	
	3.1.5. Програми зламу паролів	
	3.1.6. Програмні закладки	
3.2. Введення хибної інформації, модифікація інформації, знищення інформації та програмного забезпечення	3.2.1. Апаратні закладки	ПЕОМ, сервери
	3.2.2. Програмні закладки	
	3.2.3. Засоби віддаленого адміністрування	
	3.2.4. Комп'ютерні віруси	
	3.2.5. Викрадення інформації сервісними утилітами	
4. Відмова в обслуговуванні		
4.1. Локальна відмова в обслуговуванні	4.1.1. "Важкий пакет" (передача великого файла)	Комутатори, маршрутизатори, ПЕОМ, сервери
	4.1.2. Mac-flooding (підміна MAC-адреси відправника та/або отримувача інформації на комутаторі)	
	4.1.3. Форк-бомба (програма, яка без кінця створює власні копії)	

Тип кібератаки	Спосіб реалізації кібератаки	Область виявлення кібератаки
4.2. Віддалена відмова в обслуговуванні	4.2.1. Smurf (ICMP-флуд)	
	4.2.2. Fraggle (UDP-флуд)	
	4.2.3. SYN-flooding	
	4.2.4.XML-бомба (XML-документ, в якому: дуже багато байтів, символів, елементів, вкладень, атрибутів, імен, тегів тощо)	
4.3. Спам	4.3.1. Розсилка значної кількості пакетів	ПЕОМ, сервери
4.4. Логічне відключення абонентів	4.4.1. Перехоплення IP	ПЕОМ
5. Зміна напряму трафіка		
5.1. Логічна підміна сервера	5.1.1. Запити за протоколом RIP	Маршрутизатори, ПЕОМ, сервери
	5.1.2. Запити за протоколом OSPF	
5.2. Зміна напряму (перенаправлення) пакетів даних	5.2.1. Запити за протоколом SNMP	
	5.2.2. Запити за протоколом BGP (як протокол міждоменної маршрутизації використовується усіма Інтернет-провайдерами, а також великими компаніями та організаціями, які мають власні публічні номери автономних систем (ASN) та користуються послугами більш ніж одного Інтернет-провайдера (мултіхомінг[en]) або мають прямі IP-з'єднання з багатьма іншими великими компаніям, що також мають власні публічні номери автономних систем, без використання послуг Інтернет-провайдерів)	
	5.2.3. Запити за протоколом SAP (протокол, за яким файлові сервери і сервери друку анонсують свої адреси та відкриті служби)	
	5.2.4. Запити за протоколом ARP (мережний протокол, призначений для перетворення IP-адрес (адрес мережного рівня) в MAC-адреси (адреси канального рівня) в мережах TCP/IP)	
	5.2.5. Запити за протоколом DNS	
	5.2.6. Передача раніше підготовленої хибної відповіді	

2.2.2. Характеристика APT-кібератак як основної форми боротьби в кіберпросторі

Загрози інформаційній безпеці, як відомо, змінюються. Традиційні загрози захищеності інформаційних систем з часом набули більш небезпечних, підступних та ефективних в дії типів – Advanced Persistent Threat (APT). Ці загрози потребують особливої уваги.

APT-кібератака (розвинена стала загроза або постійна загроза підвищеної складності) – різновид складних кібератак з метою отримання несанкціонованого доступу до інформаційних систем жертви та встановлення прихованого доступу до неї з метою використання або контролю в майбутньому.

Розвинена (англ. *advanced*) – здатна обійти наявні системи захисту (мережні екрани, антивіруси, різні фільтри тощо); зловмисник здатен знаходити нові уразливості або створювати нові зразки шкідливого програмного забезпечення.

Стала (англ. *persistent*) – здатна залишатись непоміченою для систем виявлення загроз (антивіруси, системи виявлення вторгнень тощо); зловмисник спрямований на досягнення мети, може мати відповідний наказ від замовника.

Загроза (англ. *threat*) – здатна завдати певну шкоду; зловмисник добре організований, має необхідні засоби, мотивацію.

Хоча APT-атаки – тип загроз, що швидко розвивається, він вже голосно проявив себе та впливає на світову індустрію інформаційної безпеки. Основні характеристики найбільш відомих APT-кібератак надані в табл. 2.2.

Прикладами APT-кібератак, які відбулися відносно нещодавно, стали:

1. Злам 18 березня 2011 року систем RSA SecurID, які використовували двофакторну автентифікацію та за допомогою токенів, включаючи дані, які використовувались компанією для генерації одноразових паролів.

2. Операція “Аврора” 2011 року, в рамках якої було вкрадено сенситивну інформацію, таку як інтелектуальна власність (програмні коди власності Google, Adobe та інших широковідомих компаній). Під час цього використовувались техніки високої складності та доброї скоординованості.

3. У 2014 році APT CERT-UA зафіксовано дві атаки на органи державної влади України, які мають усі ознаки APT [11].

За даними фахівців, середній прямий збиток від кожної APT-кібератаки для організацій становить 5,5 млн. у.о., які витрачаються на реагування та усунення наслідків.

Найчастіше джерелами APT-кібератаки є установи, що фінансуються з державних бюджетів та мають цілі, що виходять далеко за межі простої крадіжки: військова розвідка; економічний саботаж; технічний шпіонаж; фінансові махінації; політичні маніпуляції.

Життєвий цикл APT-кібератаки можна надати наступним чином:

Підготовка:
– виявлення цілей;
– збір інформації;
– розробка стратегії кібератаки;
– створення стендової моделі цілей;
– розробка інструментів кібератаки.

Проникнення:
– обхід стандартних засобів захисту;
– експлуатація уразливостей;
– соціальна інженерія;
– комбіновані техніки проникнення;
– інвентаризація мережі.

Розповсюдження:
– закріплення;
– розповсюдження;
– оновлення;
– пошук ключової інформації і методів досягнення мети атаки.

Таблиця 2.2

Характеристики основних відомих APT-кібератак

	Agent.btz	**STUXNET**	**"Красный октябрь"**	**Black Energy**	**Carbanak**	**Equation**
Перший прояв	2007	2007	2007	2010	2013	2002
Виявлена	2008	червень 2010	січень 2013	грудень 2013	2014	2014
Неактивна	з 2009	з 2012	з 2013	Активна	Активна	Активна
Тип	мережний хробак	мережний хробак	комплексна платформа для кібератак	комплексна платформа для кібератак	бекдор	комплексна платформа для кібератак
Операційна система	Windows	промислові системи SCADA	Windows, Windows Mobile	Windows, Linux, Cisco, IOS	Windows	Windows
Кількість жертв	50001-100000	100001-300000	1001-500	500-1000	11-100	500-1000
Спосіб розповсюдження	USB-накопичувачі, саморозповсюдження (хробак)	USB-накопичувачі, зараження файлів, саморозповсюдження в локальних мережах	соціальна інженерія, експлоїти	соціальна інженерія, USB-накопичувачі, зараження файлів, саморозповсюдження в локальних мережах	соціальна інженерія, експлоїти	USB-накопичувачі, експлоїти, саморозповсюдження, фізичні засоби (CD-ROM)
Мета	кібершпіонаж, крадіжка інформації	кіберсаботаж, диверсія	кібершпіонаж	кібершпіонаж, “відмова в обслуговуванні”, крадіжка даних, диверсія	крадіжка грошей, стеження (за рахунками, клієнтами тощо)	кібершпіонаж, крадіжка грошей, стеження (за людьми)
Спрямованість	військові відомства, дипломатичні організації, посольства	підприємства ядерної енергетики (збагачення урану)	урядові установи, посольства, енергетичні та нафтогазові компанії, військові відомства, торгівля	урядові установи, посольства, енергетичні та нафтогазові компанії, військові відомства, фінансові установи	фінансові установи та організації, банки	політичні діячі, активісти, енергетика, фінансові установи та організації, банки, урядові установи, військові відомства

Закінчення табл. 2.2

	Agent.btz	STUXNET	"Красный октябрь"	Black Energy	Carbanak	Equation
Особливості	сканування комп'ютерів на наявність даних і відкритих бекдорів з наступною відправкою необхідних даних через бекдори на командно-контрольний сервер	4 різні уразливості "нульового дня", файли драйверів Stuxnet мали реальні цифрові підписи Realtek та IMicron	швидка адаптація до різних системних конфігурацій, завдання від командних серверів передавались у вигляді одноразових бібліотек PE DLL, які після виконання в пам'яті, відразу знищувались	завдання з командних серверів відправлялись у вигляді плагінів для Windows та, навіть, для CISCO (tcl-скрипти), а також для архітектур ARM/MIPS	Результатив-ність понад 1 млрд. доларів зі 100 фінансових установ, за один "рейд" виводиться не більше 10000 доларів	можливість заражати заводське програмне забезпечення жорстких дисків, імітація роботи шкідливого програмного забезпечення, «ізолювання» жертв
Атаковані країни	США, РФ, Іспанія, Італія, Казахстан, Німеччина, Польща, Латвія, Литва, Великобританія, Україна та ще 100 країн	Іран	Східна Європа, країни СНД та Центральна Азія, деякі країни Західної Європи та Північної Америки	РФ, Україна, Польща, Білорусія, Азейбарджан, Киргизія, Казахстан, Іран, Ізраїль	РФ, США, Німеччина, КНР, Україна, Канада, Тайвань, Гонконг, Іспанія, Норвегія, Індія,Франція, Пакистан, Польща та ін.	Іран, РФ, Пакистан, Афганістан, Індія, КНР, Сирія, Малі, Ліван, Йомен

Досягнення мети: – крадіжка ключової інформації;
– зміна даних;
– маніпуляція з процесами;
– скриття слідів;
– встановлення "точки повернення".

Майже кожна APT-кібератака має наступні етапи:

1. Розвідка (data gathering, reconnaissance).

Виявлення слабких місць у захисті організації (DNS-запити до домену організації, сканування портів та уразливостей сервісів).

2. Початкове втручання (initial entry).

Виявлені уразливості експлуатуються для закріплення в мережі, для чого використовуються складні техніки (spearfishing, соціальна інженерія тощо).

3. Розширення повноважень (escalation of privileges).

Подальша експлуатація, хакери працюють над отриманням якомога більшого контролю над системами та над додатковими системами, встановлюють "бекдори" (backdoor), які спрощують повторний доступ в систему.

4. Подальша експлуатація (continuous exploitation).

Нападники отримують можливість постійної та безперешкодної ідентифікації, компрометації та використання конфіденційних даних.

Способами розвідки, які найчастіше використовуються при проведенні APT-кібератак, є:

− **інсайд** – отримання інформації від нещодавно звільнених, або діючих співробітників компанії (установи);

− **відкриті джерела** – списки співробітників, адреси електронної пошти, телефонні довідники, графіки та розпорядки роботи підрозділів компанії тощо;

− **соціальна інженерія.**

Основними засобами проникнення APT-кібератак вважаються:

Експлоїт – комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують уразливості в програмному забезпеченні та використовуються для кібератаки – це такі: Adobe PDF, Adobe Flash, Microsoft Office та Internet Explorer. Експлоїти доставляються через електронну пошту, веб-сайти та USB-пристрої.

Валідатор – комп'ютерна програма для збору та перевірки інформації з заражених хостів і передачі її (в зашифрованому вигляді) в центр управління, де суб'єкт кібератаки, на продовження атаки.

Downloader – комп'ютерна програма для швидкого зараження хоста. Доставляється за допомогою фішингу або через фішингові веб-сайти. При запуску загружає основний шкідливий модуль Payload або Dropper.

Dropper – "троянська" комп'ютерна програма для доставки (через прихо-ване автозавантаження) модуля Payload на комп'ютер жертви. Доставляється через електронну пошту, веб-сайти, експлоїти та валідатори. Звичайно, вмонтовує свій власний код в код самого активного процесу, який працює на комп'ютері жертви, безпосередньо в оперативній пам'яті. Основний шкідливий модуль payload може виконувати функції:

− клавіатурного шпигуна;
− здійснення знімків екрана;
− віддалений доступ;
− розповсюдження в локальній мережі та на комп'ютері жертви;
− взаємодія з командним центром та оновлення;
− шифрування;
− очищення слідів активності, самознищення;
− доступ (читання) електронної пошти;
− пошук інформації на комп'ютері жертви.

Цей модуль створюється з багаторівневим шифруванням для захисту від систем виявлення кібератак та скриття інформації про хакерів.

Особливості APT-кібератаки:

1. Етапи 3 та 4 можуть проводитись роками, що значно ускладнює їх детектування.

2. Типові заходи та засоби із захисту телекомунікаційних мереж та інформаційно-телекомунікаційних систем не діють проти APT-кібератак з достатньою ефективністю, оскільки:

а) об'єкти APT-кібератак – це чітко визначені організації, телекомунікаційна інфраструктура, технічні рішення тощо. Таким чином, атаки APT мають невеликий розголос та рідко викликають суспільний резонанс. Часто об'єкти атак бояться розголосу того, що вони стали жертвами APT-кібератаки в незалежності від того до державного, приватного чи комерційного сектору вони належать;

b) суб'єктами APT-кібератак використовуються найновітніші хакерські техніки та технології, ціна яких зазвичай – велика для більшості звичайних комп'ютерних зловмисників. Атакуюча сторона не зупиняється при здійсненні APT-кібератаки, зіткнувшись з ситуацією, коли об'єкт атаки має досить надійний захист (це зазвичай робиться у разі "рядових" комп'ютерних злочинів);

c) типові пристрої та технології захисту, що використовуються у телекомунікаціях, можуть лише затримати час проведення етапу 2, проте не ефективні на етапах 3 та 4;

d) для захисту від APT-кібератак ефективні проактивні та комплексні методики захисту, які дозволяють виявляти та попереджувати етап 2 та подальші етапи. APT-кібератака може змінювати характеристики, дозволяючи обходити навіть дуже надійні мережні пристрої захисту.

Рекомендації CERT-UA щодо протидії APT-кібератакам.

Успішна стратегія захисту від APT-кібератак повинна включати традиційні організацію периметра захисту і заходи з забезпечення безпеки інфраструктури. Таким чином, організація повинна бути спроможною до наступних **організаційних заходів**:

− максимально ускладнити початкове втручання (добрий приклад - забороняюча політика безпеки за принципом "заборонено все, що не дозволено");

− знизити потенційні ризики при розширенні повноважень (наприклад, при компрометації автентифікаційних даних);

− обмежити шкоду, яка може бути нанесена при компрометації акантів організації;

− детектувати підозрілу активність та розвідку уразливих місць;

− збирати інформацію від/для розслідувань, яка необхідна для визначення наслідків APT-кібератак та їх усунення.

Конкретні **технічні заходи**, які рекомендуються CERT-UA щодо протидії APT:

− розмежування повноважень та управління обліковими записами при доступі до програмних та технічних ресурсів організації;

− мінімальні повноваження для облікових записів;

− контроль та запис сесій (особливо, адміністративних);

− захищеність серверного забезпечення;

− реалізація політики безпеки у форс-мажорних/нестандартних ситуаціях та політики безпеки при реагуванні на зовнішні для організації загрози;

− реалізація безпеки систем та середовищ віртуалізації;

− управління ідентифікацією та авторизацією (багатофакторна автентифікація);

− впровадження елементів/політики управління даними.

На схемі (рис. 2.5), що визначає етапність APT-кібератак, перелічені вище заходи зображено у тій частині, в якій вони можуть бути корисними на різних етапах протидії атаці APT.

Рис. 2.5. Рекомендовані заходи протидії APT-кібератакам на різних етапах

Конкретні поради CERT-UA щодо протидії APT-кібератакам [11].

Для **розмежування повноважень та управління обліковими записами при доступі до програмних та технічних ресурсів організації** необхідно:

− безпечно зберігати зашифровані парольні дані;

− управляти складністю паролів (ввести мінімальні довжини, зробити обов'язковими спеціальні символи та різні регістри в паролях, регулярно змінювати паролі);

− обмежити доступ до адміністративних облікових записів;

− заборонити збереження автентифікаційних даних з використанням можливостей автоматичної автентифікації (веб-браузери, клієнти електронної пошти, електронні платіжні системи тощо);

− обмежити кількість осіб, які мають доступ до привілейованих облікових записів (наприклад, шляхом створення облікового запису "для нагальної потреби");

− заборонити використання фіксованих паролів у скриптах.

Для **мінімальних повноважень для облікових записів** необхідно:

− не повинно надаватись доступу за принципом "все або нічого". Натомість повинно бути реалізовано схему, за якою для виконання певних завдань певні користувачі повинні шляхом авторизації та автентифікації отримати визначені для цього ролі. Наприклад:

Системні адміністратори – їм дозволяється оновлення програмного забезпечення, конфігураційні зміни та встановлення нового програмного забезпечення, але не дозволяється змінювати налаштування безпеки або переглядати журнальні файли.

Адміністратори безпеки – їм дозволяється оновлювати або змінювати налаштування та конфігурації, а також переглядати журнальні файли, але не дозволяється встановлювати програмне/апаратне забезпечення або здійснювати доступ до сенситивних даних.

Аудитори – мають можливість перевіряти налаштування безпеки та переглядати журнальні файли, але не мають можливості здійснювати будь-які зміни у системах організації.

Для **контролю та запису сесій (особливо, адміністративних)** необхідно:

− щоб було зрозумілим чином та легко визначити "хто, що і коли робив";

− впровадити аналітичний інструментарій з метою пошуку та виявлення загроз та уразливостей замість перегляду гігабайтів журнальних файлів;

− відмічати будь-які команди, які вводяться користувачами;

− поєднувати аномальну активність з особою, яка її породжує.

Для захищеності серверного забезпечення необхідно:

− використовувати мережний екран (програмний і/або апаратний), який контролює з'єднання, блокує пакети даних та небезпечні (не довірені) протоколи;

− впровадити політику для дозволених програмних пакетів (тобто, визначити, що можна встановлювати на серверах, а що - ні);

− визначити специфічні для сенситивних програмних пакетів та критично важливих для організації завдань;

− заборонити внесення змін до журнальних файлів;

− здійснювати моніторинг цілісності ключових файлів;

− контролювати доступ до файлів та директорій, сервісів, фізичний доступ тощо.

Для **реалізації політики безпеки у форс-мажорних/нестандартних ситуаціях та політики безпеки при реагуванні на зовнішні для організації загрози** необхідно:

− використовувати утиліти та засоби моніторингу та захисту файлів для можливості адміністраторів детектувати спроби атакуючих зламати мережі;

− модифікувати імена стандартних системних команд та адрес, таким чином щоб вони були не стандартні. Стандартні системні команди та адреси повинні викликати сигнал про загрозу.

Для **реалізації безпеки систем та середовищ віртуалізації** необхідно:

− застосовувати принцип мінімальних повноважень та привілеїв для аканту гіпервізора;

− здійснювати моніторинг на журналювання усіх дій (подій), які відбуваються на рівні гіпервізора;

− зробити більш захищеними віртуальні машини шляхом активації можливостей з підтримки автоматизації процесів віртуалізації (наприклад, для версії Platinum Edition системи віртуалізації XenServer існує можливість адміністраторам створювати політики автоматичного створення знімків копій віртуальних машин, їх архівування та збереження на визначених сховищах).

Для **управління ідентифікацією та авторизацією** необхідно:

− позбавляти повноважень (та забороняти доступ до інформації, яка в них циркулює й обробляється) в програмно-апаратних рішеннях/системах персон, які полишили організацію;

− регулярно перевіряти та видаляти не використовувані та не актуальні облікові записи;

− за можливості, реалізовувати більше одного методу автентифікації при доступі до ресурсів/інформації. Як варіант, використовувати програмну двофакторну автентифікацію з автентифікаційними даними, що відрізняються для кожного пристрою/програмного продукту;

− використовувати різні методи автентифікації для різних сценаріїв (наприклад, при доступі з зовнішніх для організації мереж сценарій автентифікації може включати автентифікацію за токеном, а також потребувати введення захисного коду (captcha) для захисту від підбору автенифікаційних даних з використанням ботів);

− використовувати механізми захисту від різних технік APT (різноманітні затримки при негативних спробах автентифікації, ідентифікація пристроїв, геолокація, білі/ сірі/чорні списки, індивідуальні реакції на певні загрози APT-кібератак тощо);

− реалізувати вимоги щодо певного (зазвичай, більш жорсткого) порядку проходження етапів автентифікації у разі, якщо в її результаті користувачу повинно бути надано більш широкі повноваження.

Для **впровадження політики управління** даними необхідно:

− класифікувати відповідно до ступеня важливості інформацію, яка циркулює та обробляється в організації, після чого визначити технології та методи її захисту;

− контролювати передавання даних між частинами організації (філіями) та/або іншими організаціями (наприклад, відслідковувати шляхи слідування електронної пошти та жорстких дисків тощо).

2.3. Технологічні аспекти захисту інформації в інформаційно-телекомунікаційних системах

2.3.1. Технологічні рішення щодо ідентифікації, автентифікації та авторизації користувачів інформаційно-телекомунікаційної системи

Реалізація конкретних моделей захисту від несанкціонованого доступу повинна спиратися на відповідні адміністративні (процедурні) заходи і технічні засоби, спрямовані, в першу чергу, на ідентифікацію й автентифікацію користувачів автоматизованої системи.

Ідентифікація користувачів АС полягає в установленні і закріпленні за кожним з них унікального ідентифікатора у вигляді номера, шифру, коду тощо. Це пов’язано із тим, що традиційний ідентифікатор виду “прізвище –ім’я – по батькові” не завжди може бути використаний в конкретній АС. Для цілей ідентифікації в різних автоматизованих системах широко, наприклад, застосовуються так званий персональний ідентифікаційний номер (PIN), соціальний безпечний номер (SSN), особистий номер, код безпеки тощо. Такі ідентифікатори використовуються при побудові різних систем розмежування доступу і захисту інформації.

Відповідно до Закону України “Про електронні довірчі послуги” [12] *автентифікація* – електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних. Автентифікація полягає в перевірці достовірності користувача за пред’явлений їм ідентифікатор, наприклад, при вході у систему. Така перевірка повинна виключати фальсифікацію користувачів у системі і їх компрометацію. Без перевірки достовірності втрачається сенс у самій ідентифікації користувачів і застосуванні засобів розмежування доступу, побудованих на базі особистих ідентифікаторів. Відсутність надійних засобів перевірки достовірності користувачів може істотно утруднити реалізацію принципу персональної відповідальності, про який говорилося вище.

Перевірка достовірності (автентифікація) може проводитися різними методами і засобами. Нині в автоматизованих системах використовуються три основні способи автентифікації за наступними ознаками:

1) паролю або особистому ідентифікуючому номеру (користувач “знає”);

2) деякому предмету, який є у користувача (користувач “має”);

3) яким-небудь фізіологічним ознакам, властивим конкретним особам (користувач “є”).

Перший спосіб реалізують програмні засоби автентифікації, що вживаються в більшості операційних систем, систем управління базами даних, моніторів телеобробки, мережних пакетів. Суть цього способу полягає в тому, що кожному зареєстрованому користувачеві видається персональний пароль, який він повинен тримати в таємниці і вводити в автоматизовану систему при кожному зверненні до неї. Спеціальна програма порівнює введений пароль з еталоном, що зберігається в пам’яті, і при збігу паролів запит користувача приймається до виконання.

Простота цього способу очевидна, але очевидні також і його явні недоліки: пароль може бути підібраний перебором можливих комбінацій, а майстерний зловмисник може проникнути в ту область пам’яті, де зберігаються еталонні паролі. В процесі завантаження цією ОС можна було легко проглянути паролі усіх користувачів. Безпечніші системи здійснюють зберігання списків паролів у зашифрованому виді. В той самий час перехоплення навіть зашифрованого пароля дозволяє при його використанні отримати несанкціонований доступ до видаленої ПЕОМ.

До заходів підвищення безпеки парольних систем автентифікації, окрім згаданого зберігання списків паролів в зашифрованому виді, може бути віднесене скорочення термінів дії паролів аж до застосування паролів одноразового використання. Останнім часом для цілей автентифікації широко використовується так званий метод “запит-відповідь”, який дозволяє не лише автентифікувати користувача, але і дає можливість користувачеві здійснювати автентифікацію системи, з якою він працює. Це має принципове значення при роботі в мережі, оскільки використання підставної ПЕОМ, ОС або програми є одним зі шляхів несанкціонованого отримання повідомлень або паролів законних користувачів. Слід зазначити, що необхідність такої взаємної автентифікації підтверджена міжнародним стандартом по взаємодії відкритих систем.

Різновидом першого способу автентифікації є і так зване пізнання в діалоговому режимі, здійснюване за наступною схемою. У файлах механізмів захисту завчасно створюються записи, що персоніфікують, що містять, користувача дані (дата народження, зростання, вага, імена і дати народження рідних і близьких, і тому подібне) або досить великий і впорядкований набір паролів. При зверненні користувача програма захисту пропонує йому назвати деякі дані з наявного запису, які порівнюються з тими, що зберігаються у файлі. За результатами порівняння приймається рішення про допуск. Для підвищення надійності пізнання запрошені у користувача дані можуть вибиратися кожного разу різні.

Другий спосіб автентифікації здійснюється через застосування так званої карти ідентифікації (КІ), на яку наносяться дані, що персоніфікують користувача: персональний ідентифікаційний номер, спеціальний шифр або код тощо. Ці дані заносяться на картку в зашифрованому виді, причому ключ

шифрування може бути додатковим ідентифікуючим параметром, оскільки він може бути відомий тільки користувачеві, вводиться ним кожного разу при зверненні до системи і знищується відразу ж після використання.

Інформація, що знаходиться на карті, може бути записана і зчитана різними способами або комбінацією декількох способів. Наприклад, КІ поміщається у зчитувачі, джерело світла освітлює мікрокристалічну точкову матрицю, встановлену на карті. Оскільки тільки неполяризовані елементи матриці будуть прозорі для світла, то буде прочитаний відповідний код, що містить інформацію про конкретного користувача.

Ще одним типом КІ є інформаційна картка з нанесеним особливим способом із застосуванням фосфору на її поверхню декількома рядами знаків, букв тощо. Зчитування даних з пристрою в цьому випадку є двома електродами, один з яких прозорий.

Картка поміщається між електродами, і при подачі на них напруги, електрони, що збуджуються між ізолюючим шаром (основою картки) і шаром фосфору, викликають світіння останнього. Таким чином, інформаційні знаки можуть бути лічені тільки спеціальним способом, що виключає візуальне розпізнавання інформації.

Іншим типом КІ є електронна ідентифікуюча карта, побудована на інтегральній мікросхемі. У цієї карти на короткій стороні друкованої плати розташовуються котушки індуктивності, через які передається електроживлення на плату і здійснюється обмін кодованою інформацією з пристроєм, що пізнає. Інтегральна схема містить арифметичний блок, а також постійний і оперативний пристрої, що запам’ятовують.

На поверхню карти може також наноситися покриття, що дозволяє бачити зображення або текст тільки в інфрачервоному або ультрафіолетовому діапазоні. Над текстом або зображенням можна розмістити рідкокристалічну матрицю, прозору тільки за певної орієнтації кристалів.

Найбільше поширення серед пристроїв автентифікації за типом “користувач має” отримали індивідуальні магнітні карти. Популярність таких пристроїв пояснюється універсальністю їх застосування (не лише в автоматизованих системах), відносно низькою вартістю і високою точністю, вони легко комплектуються з терміналом і персональною ПЕОМ. Оскільки зчитувачі цих пристроїв ідентифікують не особу, а магнітну карту, то вони комплектуються спеціальною, часто цифровою клавіатурою для введення власником карти свого шифру, пароля. Для захисту карт від несанкціонованого зчитування і підробки, як і в попередніх випадках, застосовуються спеціальні фізичні і криптографічні методи.

Для пізнання компонентів обробки даних, тобто ПЕОМ, ОС, програм функціональної обробки, масивів даних (таке пізнання особливе актуально при роботі в мережі ПЕОМ) використовуються спеціальні апаратні блоки-приставки, що є пристроями, які генерують індивідуальні сигнали. З метою попередження перехоплення цих сигналів і наступного їх зловмисного використання вони можуть передаватися в зашифрованому виді, причому періодично може мінятися не лише ключ шифрування, але і використовуваний спосіб (алгоритм) криптографічного перетворення.

Усього зростаючого значення останнім часом починають набувати системи розпізнання користувачів за фізіологічними ознаками. Тільки за такого підходу дійсно встановлюється, що користувач, що претендує на доступ до термінала, саме той, за кого себе видає. При використанні цього класу засобів автентифікації виникає проблема "соціальної прийнятності": процедура автентифікації не повинна принижувати людську гідність, створювати дискомфорт, просто бути занадто морочливою і займати багато часу.

Існує досить фізіологічних ознак, що однозначно вказують на конкретну людину. До них відносяться: відбитки ніг і рук, зуби, ферменти, динаміка дихання, риси обличчя і таке інше. Для автентифікації термінальних користувачів автоматизованих систем найбільш прийнятними вважаються відбитки пальців, геометрія руки, голос, особистий підпис.

Автентифікація за відбитками пальців. Встановлення особи за відбитками пальців – старий і перевірений прийом. Нині існують два можливі способи використання цього прийому для автентифікації термінального користувача:

− безпосереднє порівняння зображень відбитків пальців, отриманих за допомогою оптичних пристроїв, з відбитками з архіву;

− порівняння характерних деталей відбитка в цифровому виді, які отримують в процесі сканування зображень відбитка.

На сьогодні розроблені спеціальні чутливі матеріали, що забезпечують отримання відбитків без використання фарби, засновані на здатності речовин змінювати свої відбивні характеристики залежно від температури предметів, що прикладаються.

При безпосередньому порівнянні зображень відбитків пристрій Автентифікації визначає оптичне співвідношення двох зображень і виробляє сигнал, що визначає міру збігу відбитків. Порівняння відбитків зазвичай виконується безпосередньо на місці установки пристрою. Передача зображення відбитка по каналах зв'язку не застосовується через її складність, високу вартість і необхідність додаткового захисту цих каналів.

Значного поширення набув спосіб, побудований на порівнянні деталей відбитків (метод співвідношення борозенок на відбитках). При цьому користувач вводить з клавіатури ідентифікуючу інформацію, за якою пристрій автентифікації проводить пошук необхідного списку деталей відбитка в архіві. Після цього він поміщає палець на оптичне віконце пристрою, і починається процес сканування, в результаті якого обчислюються координати 12 точок, що визначають відносне розташування борозенок відбитка. Об'єм інформації при цьому складає близько 100 байт на відбиток. Порівняння виробляється в ЕОМ за спеціальними алгоритмами. Проте недоліком цього способу є те, що практично неможливо забезпечити точне центрування і стабільну пластичність пальця, тому неможливо отримати і точне положення борозенок, внаслідок чого оцінка відповідності має ймовірнісний характер.

Одним із прикладів пристрою автентифікації за відбитками пальців може служити американська система Fingerprint. Ця система складається з центрального пристрою управління і пристроїв для зняття відбитків пальців. Користувач вводить свій ідентифікуючий номер, поміщає палець в спеціальну

щілину, і пристрій виробляє оптичне сканування шкіри. До складу пристрою входять лазерна оптична система, апаратура обробки сигналів і мікропроцесор з програмами побудови “образу” відбитка пальця. Рельєф шкіри прочитується пристроєм майже безпомилково. Для занесення еталона відбитка одного пальця вимагається від 3 до 5 хвилин, необхідний об’єм пам’яті 256 байт.

Автентифікація за формою кисті руки. Принцип дії таких пристроїв автентифікації заснований на тому, що на руку випробовуваному направляють яскраве світло й аналізують освітленість чутливих елементів, яка залежить від довжини пальців, закругленості їх кінчиків і прозорості шкіри. Вихідна інформація від кожного фоторезистора перетвориться в цифровий код. Ідентифікуюча інформація може зберігатися централізований в головній ПЕОМ. Перевагою подібних систем є велике число аналізованих параметрів, що зменшує вірогідність помилки.

Автентифікація за допомогою автоматичного аналізу підпису. Відомо, що почерк кожної людини строго індивідуальний, ще більше індивідуальний її підпис. Вона стає надзвичайно стилізованою і з часом набуває характеру умовного рефлексу. Нині існують два принципово різних способи аналізу підпису: візуальне сканування і дослідження динамічних характеристик руху руки при виконанні підпису (прискорення, швидкості, тиски, тривалість пауз). Вважається, що другий спосіб прийнятніший, оскільки очевидно, що два підписи однієї і тієї ж людини не можуть бути абсолютно ідентичними. З іншого боку, маючи оригінал підпису, можна навчитися повторювати її практично точно.

При другому способі автентифікації передбачається застосування спеціальних вимірювальних авторучок з датчиками, чутливими до вказаних вище динамічних характеристик руху. Ці параметри унікальні для кожної людини, їх неможливо підробити. У авторучку вбудований двомірний датчик прискорення, що дозволяє вимірювати характеристики на площині, а також датчик тиску, фіксувальний параметри вертикальної сили. Фахівці вважають, що системами встановлення достовірності підпису при меншій вартості і більше соціальною прийнятністю не поступається за надійністю пристроям, що звіряють відбитки пальців.

Автентифікація за характером голосу. На думку ряду фахівців, найбільш надійними засобами автентифікації користувачів є засоби верифікації за голосом. Це напрям дуже перспективний тому, що для автентифікації можуть бути використані телефонні канали зв’язку, а алгоритм пізнання може бути реалізований в центральній ПЕОМ. Можна виділити три основні напрями реалізації цього способу автентифікації:

− аналіз короткочасних сегментів мови (тривалістю до 20 мс) – вибирається серія коротких фрагментів, обробляється, складається статистичний образ, який і порівнюється з еталоном;

− контурний аналіз мови – з фрагмента мови виділяється декілька характеристик, наприклад, висота тону, для них визначається характеристична функція, яка порівнюється з еталонною;

– статистична оцінка голосу – мова повинна звучати достатньо довго (близько 12 с), упродовж усього цього періоду збирається інформація про декілька параметрів голосу, на основі якої створюється цифровий образ і порівнюється з еталоном.

Слова, які вимовляє користувач, вибираються за принципом найбільшої різноманітності звуків і заздалегідь виводяться на екран дисплея у випадковій послідовності, що виключає підробки, у тому числі використання магнітофонного запису.

Основними характеристиками пристроїв автентифікації є:

1) частота помилкового заперечення законного користувача;
2) частота помилкового визнання стороннього;
3) середній час напрацювання на відмову;
4) число обслуговуваних користувачів;
5) вартість;
6) об’єм інформації, циркулюючої між зчитувачем і блоком порівняння;
7) прийнятність з боку користувачів.

Дослідження і випробування пристроїв автентифікації різних типів показали, що частота помилкового заперечення дещо перевищує частоту помилкового визнання і складає величину, що не перевищує 1-2%.

Головним висновком, що виходить з досвіду створення пристроїв автентифікації, є те, що отримання високої точності пізнання користувача можливо тільки при поєднанні різних методів.

Необхідно зазначити, що усі розглянуті методи автентифікації, у разі не підтвердження достовірності, повинні здійснювати тимчасову затримку перед обслуговуванням наступного запиту. Це необхідно для зниження загрози підбору ідентифікуючих ознак (особливо паролів) в автоматичному режимі. При цьому, усі спроби неуспіхів діставання доступу повинні реєструватися з метою забезпечення ефективного нагляду (контролю) за безпекою системи.

2.3.2. Особливості функціонування систем виявлення і попередження кіберзагроз та оцінки кіберризиків

Одним із важливих засобів захисту від кібератак є системи виявлення атак (СВА) – програмні або апаратні засоби, які призначені для виявлення фактів неавторизованого доступу у комп’ютерну систему або мережу, або несанкціонованого керування ними. Проте, незважаючи на той факт, що у теперішній час питанням побудови СВА присвячено значну кількість наукових робіт, головне питання – ефективне застосування СВА для побудови системи кіберзахисту, залишається невирішеним.

У свою чергу, це обумовлює актуальність подальших досліджень, які полягають у підвищенні ефективності застосування СВА на основі розробки та впровадження нових методів виявлення кібератак.

Аналіз останніх досліджень і публікацій показує, що методи виявлення атак у сучасних СВА недостатньо повно опрацьовані з точки зору стійкості, адаптованості та верифікації, а також достатньо складно оцінити їхні власти-

вості такі, як обчислювальна складність, коректність, завершуваність та ін.

На теперішній час, методи виявлення атак класифікують як методи виявлення аномалій та методи виявлення зловживань, причому до другого класу відносять більшу частку сучасних комерційних СВА. Вони застосовують, так звані, сигнатурні методи, основним недоліком яких є низька ефективність (адаптивність) виявлення невідомих атак. Це є проблемою щодо їх застосування в інформаційних системах (ІС) органів військового управління (ОВУ), незважаючи на той факт, що сигнатурні методи виявлення атак мають такі достоїнства, як низька обчислювальна складність та відносно невелика вартість розгортання та застосування [13].

Найбільш поширеними методами даного класу є:

− сигнатурні методи (дозволяють скласти алфавіт з подій, що спостерігаються у системі, та описати множину сигнатур атак у вигляді регулярних виразів у побудованому алфавіті);

− методи аналізу систем станів (процес виявлення атаки являє собою побудову графу станів системи та переходів між ними, а також пошук відомих шляхів, що є неприпустимими);

− графи сценаріїв атак (на вхід системі верифікації надходить кінцева модель системи, яка захищається, та деяке формальне правило коректності, яке виконується тільки для дозволеної поведінки системи та яке розділяє усю множину її поведінок на два класи: допустимої поведінки, для якого правило виконується, та недопустимої, у протилежному випадку);

− нейронні мережі (для виявлення атак, нейронні мережі навчаються на прикладах атак кожного класу, а у подальшому, застосовуються для розпізнавання приналежності поведінки системи до одного з класів атак);

− імунні мережі (є механізмом класифікації, але на відміну від нейронних мереж, дозволяють отримувати механізми для протидії невідомим атакам);

− метод опорних векторів (Support Vector Machines, SVM) (дозволяє побудувати функцію, яка вирішує задачу класифікації, при цьому, для виявлення атак формується вектор ознак, а далі – здійснюється навчання та побудова класифікатора, в результаті чого отримана функція здійснює класифікацію векторів-ознак і, таким чином, розпізнає до якого класу відноситься поточна дія програмного забезпечення чи користувача: правомірного чи забороненого);

− експертні системи (дозволяють описувати функціонування системи у вигляді множини фактів і правил виводу для прийняття рішення про наявність або відсутність атаки);

− методи, засновані на специфікаціях (в основу покладено опис обмежень на заборонену поведінку об’єктів у системі, яка захищається, у вигляді специфікацій атак, наприклад, обмежень на завантаженість ресурсів, списку заборонених операцій та їх послідовностей, часу доби, протягом якого мають застосовуватися ті чи інші обмеження та ін.);

− Multivariate Adaptive Regression Splines (MARS) (оперують у багатовимірному просторі ознак, де поведінка мережних об’єктів відображується у послідовності векторів даного простору, причому задача

виявлення атаки полягає у побудові оптимальної апроксимації поведінки за заданою історією у вигляді навчальної множини векторів, при цьому, у якості апроксимуючої функції застосовуються сплайни зі змінним числом вершин).

З іншого боку, існує значна кількість наукових досліджень у галузі виявлення аномалій, проте в реальних СВА вони застосовуються дуже рідко, внаслідок значної кількості хибних спрацьовувань.

До основних методів виявлення аномалій можна віднести:

− статистичний аналіз (ґрунтується на побудові статистичного профілю поведінки системи протягом деякого періоду навчання, за якого поведінка системи вважається нормальною, причому для кожного параметра функціонування системи будується інтервал припустимих значень із застосуванням деякого відомого закону розподілу);

− кластерний аналіз (полягає у розбитті множини векторів-властивостей системи, які спостерігаються на кластерах, серед яких виділяють кластери нормальної поведінки);

− нейронні мережі (для виявлення аномалій нейронна мережа навчається протягом деякого інтервалу часу, коли поведінка системи вважається нормальною, а після навчання нейронна мережа запускається у режимі розпізнавання);

− експертні системи (інформація про нормальну поведінку надаєтья у вигляді правил та фактів);

− біометрія поведінки (ґрунтується на результатах спостереження клавіатурного почерку та використання комп'ютерної миши, а також гіпотези про відмінність почерку роботи з інтерфейсами вводу-виводу для різних користувачів);

− імунні мережі та SVM (також застосовуються для методів виявлення аномалій).

Крім того, проведений аналіз показує, що у теперішній час найбільш поширеними критеріями для оцінки методів виявлення атак є:

− рівень спостереження за системою (на рівні операційної системи окремого вузла мережі, на рівні мережної взаємодії об'єктів на вузлах мережі, на рівні окремих додатків вузла мережі, комбінування різних рівнів тощо);

− верифікація методу (наприклад, кваліфікованим адміністратором з безпеки або експертом);

− адаптивність методу (оперативне реагування на невідомі атаки);

− стійкість методу (навчений в одній мережі аналізатор може бути стійким у межах даної мережі проте нестійким в інших мережах);

− обчислювальна складність методу (логарифмічна, лінійна, квадратична та ін.).

Результати порівняльного аналізу методів виявлення атак показують, що для більшості методів виявлення аномалій характерним недоліком є слабка верифікованість та слабка стійкість. З іншого боку, основним достоїнством цих методів є адаптивність та здатність виявляти раніше невідомі атаки.

Таким чином, жоден з наведених методів не є одночасно адаптивним, стійким та верифікованим, маючи при цьому припустиму обчислювальну

складність.

У свою чергу, для порівняльного аналізу СВА застосовують наступні критерії:

− класи атак, що виявляються (внутрішні або зовнішні);

− вузлові або мережні;

− спрямовані на ресурси користувачів, системні ресурси, ресурси СКБД, обчислювальні ресурси або ресурси захисту;

− спрямовані на збір інформації, отримання прав користувачів ресурсів або їхніх адміністраторів;

− порушення цілісності ресурсу або його працездатності; розподілений або нерозподілений характер);

− рівень спостереження за системою (аналогічно до методів);

− за методом виявлення атаки (метод виявлення зловживань або аномалій);

− адаптивність до невідомих атак (здатність виявляти невідомі типи атак); масштабованість (можливість додавання нових ресурсів мережі, які аналізуються, нових вузлів, каналів передачі даних, а також можливість керування єдиною розподіленою системою виявлення атак);

− відкритість (можливості системи для інтеграції в неї інших методів виявлення атак та компонентів сторонніх розробників, а також з іншими системами захисту інформації);

− формування зворотної реакції на атаку (наявність у системі вбудованих механізмів у відповідь на атаку); захищеність (ступінь захищеності СВА від атак).

Аналіз наведених критеріїв класифікації показує, що найбільш ефективною можна вважати СВА, яка:

− є повною (покриває всі класи атак);

− дозволяє аналізувати поведінку ІС, яка захищається, на всіх рівнях (мережному, вузловому, окремих додатків тощо);

− є адаптивною до всіх типів атак;

− масштабується для різних класів ІС (від локальних до корпоративних);

− є відкритою; має вбудовані механізми реагування на атаки;

− є захищеною від атак на свої компоненти.

Проте аналіз відомих на сьогоднішній день СВА з відкритим кодом за наведеними критеріями показує, що жодна із них повною мірою не відповідає сформульованим критеріям, зокрема завдяки відсутньої адаптації до невідомих типів атак та неможливості аналізувати поведінку ІС на всіх рівнях одночасно.

Таким чином, проведений аналіз методів і СВА дозволяє зробити висновок про відсутність у теперішній час СВА, яка б була адаптивною до невідомих атак. Незважаючи на те, що існує значна кількість методів виявлення аномалій, їхня слабка стійкість, неверифікація, значна кількість хибних спрацьовувань, вузька спеціалізація та дослідницький характер, не дозволяють широко використовувати їх в ІС ОВУ.

Для усунення даних недоліків є доцільним проведення низки наукових досліджень щодо розробки адаптивної СВА, в основу функціонування якої необхідно покласти методи, які б при низькій (близькій до лінійної)

обчислювальній складності, стійкості та верифікації мали б низькій рівень хибних спрацьовувань.

Крім того, можна зробити висновок про те, що постійна тенденція у галузі захисту ІС щодо переходу від розробки механізмів виявлення атак до їхнього запобігання, з урахуванням постійного підвищення пропускної здатності каналів зв'язку, пред'являє підвищені вимоги до обчислювальної складності алгоритмів виявлення атак.

Результати дослідження сучасних СВА з відкритим кодом (Snort, Bro, OSSEC, Prelude) показують, що основними елементами, які входять до їхньої структури, є підсистема збору інформації, що використовується для збору первинної інформації про систему, яка захищається; підсистема аналізу (виявлення), що здійснює пошук атак та вторгнень у систему, яка захищається; підсистема подання даних (користувацький інтерфейс), який дає змогу адміністраторові безпеки спостерігати за станом системи.

Ураховуючи сучасні тенденції в галузі інформаційних технологій, можна зробити висновок, що слабким місцем даних СВА є відсутність підсистеми, що дозволяє адміністратору безпеки здійснювати оперативну аналітичну обробку даних (Online Analytical Processing, OLAP) та підсистеми, яка дозволяє знаходити неочевидні, об'єктивні та корисні на практиці закономірності (Data Mining), а також підсистеми візуального аналізу даних.

Підсистема оперативного аналізу даних повинна складатися з модулів збору даних про стан системи з первинних джерел і накопичення їх у сховищі даних (Data Warehouse) СВА та модуля аналізу даних, накопичених у сховищі даних, який дає змогу адміністраторові безпеки здійснювати гнучкий логічний та статистичний аналіз, а також забезпечуватиме йому багатовимірне концептуальне подання даних.

Підсистема інтелектуального аналізу даних повинна виконувати функції знаходження у Сховищі Даних СВА неочевидних, об'єктивних та корисних на практиці закономірностей, які не виявляються стандартними методами обробки інформації або експертним шляхом, більшою мірою відповідають дійсності, ніж думка експертів, яка є суб'єктивною, та мають конкретне практичне застосування. Основною метою введення даної підсистеми у структуру СВА є формування нових знань про процес функціонування системи та кібератаки (донавчання системи) шляхом виявлення порушень (побудови моделей атак для їхньої подальшої класифікації) або виявлення аномалій (побудови моделей нормальної роботи системи для пошуку аномалій в її роботі) з подальшим накопиченням їх у базі знань системи.

Підсистема візуального аналізу даних являє собою подальший розвиток підсистеми подання даних СВА та повинна виконувати функції пошуку прихованих закономірностей у даних, що накопичуються системою, шляхом збігу можливостей сучасних засобів обчислювальної техніки з творчим та гнучким мисленням людини. Це досягається завдяки поданню великих обсягів даних у формі, яка дозволяє людині побачити те, що важко виділити алгоритмічним шляхом. Візуальний аналіз даних є корисним тоді, коли мало відомо про самі дані, а цілі дослідження є нечіткими.

У цьому випадку адміністратор безпеки системи безпосередньо працює з даними, які подають у вигляді візуальних образів та які він може розглядати різнобічно, під будь-якими кутами та має можливість отримувати додаткову інформацію, яка допомагає йому більш чітко формулювати цілі аналізу.

Лише часткова практична реалізація запропонованих у доповіді рішень на базі СВА Snort, Bro, OSSEC та Prelude уже дозволяє зробити висновок про підвищення ефективності роботи адміністратора безпеки щодо прийняття ним оперативних й обґрунтованих рішень на виявлення та протидію кібератакам не менш ніж на 15 – 18% [13].

Перспективними напрямами подальших наукових досліджень у галузі розробки систем виявлення кібератак можна вважати:

− розробку моделей ідентифікації атак (у тому числі, на основі теорії нечітких множин та нечіткого логічного виводу);

− розробку методів збору, узгодження, очищення, верифікації вхідних даних та завантаження їх у централізоване Сховище Даних СВА;

− розробку методики вибору моделей подання знань у базі знань СВА;

− розробку методів і методик добування та формування знань у базі знань СВА;

− розробку моделей і методів та візуального аналізу даних;

− розробку методики оцінки ефективності роботи СВА.

2.3.3. Антивірусний захист інформаційно-телекомунікаційної системи

Антивірусний захист відноситься до основних завдань системи захисту інформації та забезпечення кібербезпеки в інформаційно-телекомунікаційних системах (ІТС). Система антивірусного захисту в ІТС призначена для запобігання несанкціонованим діям з використанням комп’ютерних вірусів у ІТС, визначення найменувань та версій антивірусного програмного забезпечення, правил та порядку інсталяції, конфігурації та експлуатації антивірусних програмних засобів і контролю за їх функціонуванням, забезпечення та впровадження антивірусних оновлень, а також контролю стану антивірусного захисту.

Система антивірусного захисту в ІТС складається з системи застосування антивірусних програмних засобів та системи антивірусних оновлень.

Керівництво системою антивірусного захисту в ІТС здійснюється уповноваженим органом із захисту інформації та кібербезпеки в ІТС.

Організація виконання основних завдань системи антивірусного захисту в ІТС покладається на визначений виконавчий підрозділ системи захисту інформації та кібербезпеки в ІТС.

До функцій з антивірусного захисту уповноваженого органу із захисту інформації та кібербезпеки в ІТС і виконавчого підрозділу системи захисту інформації та кібербезпеки в ІТС відносяться: організація заходів з антивірусного захисту та керівництво системою антивірусного захисту в ІТС, здійснення оперативного керівництва уповноваженими підрозділами,

підрозділами та службами захисту інформації, кібербезпеки, службами захисту інформації та кібербезпеки в ІТС, визначення вимог та потреб у галузі антивірусного захисту, погодження документації закупівель товарів, робіт чи послуг з антивірусного захисту в організації, класифікація інцидентів антивірусного захисту, проведення експертизи, впровадження та контроль засобів і заходів з антивірусного захисту в ІТС.

Технічні та організаційні вимоги до антивірусного захисту захищеної системи обміну інформацією визначаються наказами та розпорядженнями керівника уповноваженого органу із захисту інформації та кібербезпеки в ІТС.

Відповідно до Інструкції про порядок організації антивірусного захисту в інформаційно-телекомунікаційних системах:

− **антивірусний захист** – діяльність, спрямована на запобігання несанкціонованим діям з використанням комп'ютерних вірусів, їх копій, модифікацій щодо інформації у системі;

− **антивірусна програма** – програмне забезпечення, яке призначене для захисту об'єктів/ресурсів ІТС від ушкодження комп'ютерними вірусами.

Можна також дати наступне визначення антивірусної програми:

Антивірусна програма (антивірус) – програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файла вірусом.

Існує величезна кількість різних антивірусних програмних комплексів. Вони відрізняються, як за ціновими параметрами, так і за функціональністю. Крім того, на різних тестах можна отримати різні результати для різних антивірусних програм.

Найбільш відомими та популярними ресурсами, призначеним для порівняння різних антивірусів є https://www.virusbulletin.com/ та https://www.av-test.org/en/.

Якщо розглянути результати порівняння різних антивірусних програмних комплексів за основними тестами, то можна визначити два основні параметри для кожної антивірусної програми:

− результативність проактивного захисту;

− результативність реактивного захисту.

Реактивний захист – це захист від відомих загроз із використанням знань про ділянки коду та інших унікальних особливостях шкідливих програм. Для того щоб такий захист працював успішно, антивірусна програма повинна мати найсвіжіші бази вірусних сигнатур.

Кожен, хто користувався антивірусом, зустрічався з таким явищем, як оновлення антивірусних баз. Для чого це потрібно? Відповідь проста – антивіруси працюють за принципом розпізнавання зловмисного коду, використовуючи при цьому дані з антивірусних сигнатур, які зберігаються у вірусних базах.

Щодня у світі з'являються десятки тисяч нових шкідливих програм. І найчастіше, єдине, що захищає комп'ютер користувача від всіх цих загроз – це робоча антивірусна програма.

Як правило, вірусні бази провідних продуктів містять величезну кількість записів.

Коли вірусологи антивірусної компанії виявляють новий вірус, вони декодують його і виявляють ділянки шкідливого коду, фрагменти якого потім додають в антивірусні сигнатури, користуючись якими антивірус може визначати в заражених файлах віруси.

Після виявлення шкідливої програми або файла зараженого вірусом, антивірусна програма може (залежно від вибору користувача):

− спробувати вилікувати заражений файл – видалити з нього шкідливі ділянки коду;

− помістити інфікований файл в карантин. Якщо це цінний файл і містить важливу інформацію, то його можна помістити в папку карантину. Пізніше його можна спробувати вилікувати «вручну» самостійно або ж звернутися за допомогою до фахівців;

− видалити інфікований файл. Якщо файл вилікувати не вдалося, то єдиним виходом залишається його видалення;

− нічого не робити. Якщо Ви впевнені, що антивірус помилково визнав цей файл шкідливим, то можна не робити над файлом ніяких дій і додати його у виключення.

Повноцінні антивіруси, як правило, захищають комп’ютер постійно. Тобто, запускаються разом із запуском операційної системи (саме тому після встановлення антивірусної програми завантаження ОС стає трохи довшим, ніж зазвичай), контролюють оперативну пам’ять і файлову систему комп’ютера, а також перевіряють на наявність вірусів кожну програму, що запускається.

Для того, щоб порівняти різні антивірусні програмні комплекси на реактивний захист формується тестова вибірка відомих вірусів і різні антивіруси перевіряються на:

− повноту виявлення вірусів (чим більша – тим кращий антивірусний програмний комплекс);

− швидкість виявлення вірусів (чим більша – тим кращий антивірусний програмний комплекс);

− навантаження на операційну систему в режимі перевірки (чим менша – тим кращий антивірусний програмний комплекс);

− коректність лікування/знешкодження/додавання винятків.

Проактивний захист – це захист від невідомих вірусів, заснований на знанні особливостей коду та поведінки, характерних для шкідливого програмного забезпечення. Проактивний захист особливо ефективний від модифікованих вірусів, заснованих на вже існуючих загрозах.

На відміну від сигнатурних технологій, вони попереджають, а не виявляють вже відоме зловмисне програмне забезпечення в системі. При цьому проактивний захист намагається блокувати потенційно небезпечну активність програми.

Основними технологіями проактивного захисту є:

− евристичний аналіз – тобто аналіз програмного коду невідомої програми шляхом його емуляції та покрокової перевірки кожної команди, порівнюючи

отримані результати з відомими сигнатурами шкідливого програмного забезпечення;

− емуляція коду;

− аналіз поведінки невідомої програми;

− “пісочниця”;

− віртуалізація робочого простору.

Реалізація всіх (крім евристичного аналізу) технологій проактивного захисту потребує створення віртуального простору, в якому невідома програма запускається на виконання. За результатами роботи програми або її характерною поведінкою приймається рішення про її “шкідливість”.

Параметри оцінки проактивного захисту аналогічні до реактивного. Але, до них додається такий параметр, як кількість хибних спрацювань (чим менша – тим кращий антивірусний програмний комплекс).

Також, важливими параметрами сучасних антивірусів є ергономічність (зручність у використанні), простота налаштування, регулярність та повнота оновлень антивірусних баз і, звичайно, ціна антивірусного програмного комплексу.

Тобто повний перелік основних параметрів антивірусного програмного комплексу буде мати наступний вигляд:

− повнота виявлення вірусів;

− швидкість виявлення вірусів;

− навантаження на операційну систему в режимі перевірки;

− коректність лікування/знешкодження/додавання винятків;

− кількість хибних спрацювань;

− ергономічність (зручність у використанні);

− простота налаштування;

− регулярність та повнота оновлень антивірусних баз;

− ціна.

Принцип вибору антивірусного програмного продукту для його реалізації в ІТС військового призначення можна сформулювати наступним чином: *антивірусний програмний комплекс повинен мати найвищі показники реактивного та проактивного захисту, бути простим у налаштуванні, зручним у використанні, регулярно оновлюватись та мати найнижчу можливу ціну.*

Крім того, вибір необхідно здійснювати з урахуванням вимог Інструкції про порядок організації антивірусного захисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України.

На автоматизованих робочих місцях та серверах автоматизованих систем забороняється використання зовнішніх машинних носіїв інформації без проведення їх перевірки на наявність комп’ютерних вірусів за допомогою антивірусної програми.

Інсталяція антивірусних оновлень у функціонуючі АРМ або сервери проводиться не рідше одного разу на тиждень.

За допомогою антивірусної програми не рідше разу на місяць проводиться

повна перевірка (сканування) функціонуючої в цьому місяці ПЕОМ на наявність комп'ютерних вірусів.

У разі неможливості знищення комп'ютерного вірусу наявними антивірусними програмними засобами з актуальними антивірусними оновленнями, доступ до комп'ютерного вірусу повинен бути тимчасово блокований засобами антивірусного програмного засобу або операційної системи. Крім того, будь-який антивірусний програмний засіб має бути обов'язково сертифікованим. Сьогодні в мережі Інтернет існують спеціальні ресурси, на яких можна протестувати антивірусні програми.

2.3.4. Використання брандмауерів (firewall) для контролю та фільтрації трафіка в інформаційно-телекомунікаційних системах

Брандмауери забезпечують безпеку при здійсненні електронного обміну інформацією з іншими взаємодіючими інформаційно-телекомунікаційними системами і зовнішніми мережами, розмежування доступу між сегментами корпоративної мережі, а також захист від проникнення і втручання в роботу ІС порушників із зовнішніх систем.

Брандмауер (firewall) – спеціалізований програмний або апаратний (або програмно-апаратний) засіб, що дозволяє розділити мережу на дві або більше частин і реалізувати набір правил, що визначають умови проходження мережевих пакетів з однієї частини в іншу.

Брандмауери, встановлені в точках з'єднання з мережею Інтернет, забезпечують захист зовнішнього периметра мережі підприємства і захист власних Internet-серверів, відкритих для загального користування, від несанкціонованого доступу.

Механізми захисту брандмауерів, які реалізовуються :

− фільтрація мережного трафіка;
− шифрування (створення VPN);
− трансляція адрес;
− автентифікація (додаткова);
− протидія деяким мережним атакам (найбільш поширеним);
− управління списками доступу на маршрутизаторах (необов'язково).

Основна функція брандмауера – фільтрація мережного трафіка. Вона може здійснюватися на будь-якому рівні моделі OSI. Критеріями може бути інформація з різних рівнів: адреси відправника/одержувача, номера портів, вміст поля даних.

Приналежність брандмауера до того або іншого типу визначається рівнем моделі OSI, інформація з якого є критерієм фільтрації.

Розглянемо основні типи брандмауера.

Пакетні фільтри здійснюють аналіз інформації мережного і транспортного рівнів моделі OSI. Це мережні адреси (наприклад, IP) відправника та отримувача пакета номера портів відправника й отримувача, прапори протоколу TCP, опції IP, типи ICMP. Зазвичай пакетні фільтри організовуються засобами маршрутизаторів. Часто використовуються штатні засоби операційних систем.

Шлюзи рівня з'єднання. Цей і наступний тип брандмауера заснований на використанні так званого принципу посередництва, тобто запит приймається брандмауером, аналізується і тільки потім перенаправляється реальному серверу. Перш ніж дозволити встановлення з'єднання TCP між комп'ютерами внутрішньої і зовнішньої мережі, посередники рівня з'єднання спочатку як мінімум реєструють клієнта. При цьому неважливо, з якого боку цей клієнт знаходиться. При позитивному результаті реєстрації між зовнішнім і внутрішнім комп'ютерами організовується віртуальний канал, по якому пакети передаються між мережами.

Найбільш відомим прикладом шлюзу рівня з'єднання можна вважати шлюз з перетворенням IP-адрес (Network Address Translation, NAT).

Шлюзи прикладного рівня. Шлюзи прикладного рівня (application - level proxy), що часто називаються proxy-серверами, контролюють і фільтрують інформацію на прикладному рівні моделі OSI. Вони розрізняються по протоколах прикладного рівня, що підтримуються. Найчастіше підтримуються служби Web (HTTP), ftp, SMTP, POP3 I MAP, NNTP, Gopher, Telnet, DNS, RealAudio/RealVideo. Коли клієнт внутрішньої мережі звертається, наприклад, до сервера Web, то його запит потрапляє до посередника Web (чи перехоплюється ним). Останній встановлює зв'язок з сервером від імені клієнта, а отриману інформацію передає клієнтові. Для зовнішнього сервера посередник виступає клієнтом, а для внутрішнього клієнта – в якості сервера Web. Аналогічно посередник може працювати і у разі зовнішнього клієнта і внутрішнього сервера.

Технології Proxy і Stateful inspection. У розглянутих вище типах брандмауера, що припускають посередництво при встановленні з'єднання (шлюзах рівня з'єднання і прикладного), реалізована так звана технологія Proxy. Ця технологія значно поширена і застосовується в таких відомих моделях брандмауера, як Microsoft Proxy Server і CyberGuard Firewall .

Проте для вироблення остаточних рішень про дозвіл того або іншого з'єднання для служб TCP/IP (тобто пропустити, заборонити, Автентифікувати, зробити запис про це в журналі), брандмауер повинен вміти отримувати, зберігати, витягати і маніпулювати інформацією з усіх рівнів мережної семирівневої моделі та з інших додатків.

Недостатньо тільки переглядати окремі пакети. Інформація про стан, береться з тих з'єднань, що мали місце раніше та інших додатків, використовується для ухвалення остаточного рішення про поточну спробу встановлення з'єднання. Залежно від типу пакета, що перевіряється, для ухвалення рішення важливими можуть бути, як поточний стан з'єднання, якому він належить (отримане з його історії), так і стан додатка, що його використовує.

Таким чином, для забезпечення найвищого рівня безпеки брандмауер повинен вміти зчитувати, аналізувати і використати наступну інформацію:

− інформацію про з'єднання – інформацію з усіх семи рівнів моделі;

− стан з'єднання – стан, отриманий з попередніх пакетів;

– стан додатка – інформація про стан, отримана з інших додатків. Наприклад, коли-небудь авторизованому користувачеві був дозволений доступ через firewall тільки для дозволених типів мережних протоколів.

Крім того, брандмауер повинен уміти виконувати дії над інформацією, що передається, залежно від усіх вищевикладених факторів.

Stateful Inspection – технологія нового покоління, задовольняє усім вимогам до безпеки, наведеним вище.

Технологія інспекції пакетів з урахуванням стану протоколу на сьогодні є найбільш передовим методом контролю трафіка (вона розроблена і запатентована компанією Check Point Software Technologies).

Ця технологія дозволяє контролювати дані аж до рівня додатків, не вимагаючи при цьому окремого процесу-посередника (proxy) для кожного протоколу, що захищається, або мережної служби. В результаті досягаються високі показники продуктивності, висока гнучкість рішень і можливість швидко і досить просто адаптувати систему під нові потреби.

Ґрунтуючись на технології інспекції пакетів з урахуванням стану протоколу, брандмауер забезпечує найвищий рівень безпеки. Метод stateful inspection забезпечує збір інформації з пакетів даних, як комунікаційного, так і прикладного рівнів, що досягається збереженням і накопиченням її в спеціальних контекстних таблицях, які динамічно оновлюються. Такий підхід забезпечує максимально можливий рівень безпеки, контролюючи з'єднання на рівнях від 3 до 7 мережної моделі OSI, тоді як proxy посередники можуть контролювати з'єднання тільки на 5 – 7 рівнях.

Основні функції брандмауера.

Аналіз змісту пакетів. Механізми перевірки змісту фільтрованих інформаційних пакетів (Content Security) реалізовані у багатьох брандмауерах, розширюють функції інспекції даних до найвищого рівня забезпечення інформаційної безпеки. Ці механізми дозволяють захистити користувачів від різних ризиків, включаючи комп'ютерні віруси і шкідливі аплети Java і ActiveX.

Брандмауер представляє першу лінію оборони, забезпечуючи захист від вірусів шляхом запобігання їх проникненню в точці входу у внутрішню мережу організації. Більшість брандмауерів мають засоби, що дозволяють в реальному масштабі часу здійснювати декодування, декомпресію і розпаковування файлів (за протоколом FTP), що входять і виходять, Web-додатків (за протоколом HTTP), поштових повідомлень (за протоколом SMTP) та ін. Усі відправлені файли скануються і/або піддаються "карантину" відповідно до прийнятої політики безпеки. Деякі брандмауери можуть працювати спільно зі спеціалізованими антивірусними сканерами, передаючи їм дані для антивірусного контролю.

Підтримка поштового протоколу SMTP. SMTP – протокол був спочатку розроблений для забезпечення максимально гнучких можливостей взаємодії користувачів поштової системи. Тоді передбачалося, що доступ до Інтернет користувачі отримують з різних географічних регіонів. Потім протокол був розширений можливостями підтримки передачі різного роду інформації у

вигляді вкладень електронної пошти. В результаті виявилось, що досить складно забезпечити максимальну прозорість поштових з'єднань і при цьому захистити від зломщиків внутрішню мережу організації.

Механізми брандмауерів, засновані на детальному контролі SMTP-з'єднаннях, надають наступні можливості:

− приховання у вихідній пошті адреси відправника в полі From шляхом заміни його на деяку загальну адресу дозволяє повністю приховати внутрішню мережеву структуру і реальних внутрішніх користувачів електронної пошти;

− перенаправлення пошти, надісланої якому-небудь користувачеві, наприклад, користувачеві root;

− знищення пошти, надісланої деяким адресатом;

− видалення вкладень певного типу, наприклад, виконуваних файлів програм;

− видалення полів Received у вихідній пошті, що запобігає поширенню інформації про маршрути проходження електронної пошти усередині організації;

− заборона використання розширеного набору команд протоколу SMTP, які можна використати з ворожими цілями;

− видалення поштових повідомлень, що перевищують заданий розмір;

− сканування вкладень пошти на наявність вірусів. Ревізія http-пакетів.

2.3.5. Особливості використання технологій та програмних засобів криптозахисту та криптоаналізу інформації в інформаційно-телекомунікаційних системах

Технічний захист інформації можуть здійснювати будь-які організації та підприємства, яким такий захист потрібен. На відміну від цього, згідно з законодавчими та нормативними документами України та інших держав, криптографічний захист інформації (КЗІ) можуть здійснювати лише державні організації та підприємства або інші за їх дорученням. Але за умов всебічного поширення інформаційних технологій та вступу людства у стадію становлення інформаційного суспільства коло застосування КЗІ закономірно розширилось. КЗІ обслуговує сфери бізнесу, банківських послуг, електронної торгівлі, інформаційних технологій, хмарних обчислень та мільярди "звичайних" людей, які починають жити в "електронному" суспільстві.

Криптографічний захист інформації (КЗІ) – це вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховання/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Система КЗІ складається із власне криптографічних засобів, технічних засобів для захисту від витоку інформації до шифрування та після дешифрування, організаційних заходів щодо захисту від загроз людських факторів, а також правового, методичного, математичного, програмно-алгоритмічного, інформаційного забезпечень, які попереджують реалізацію загроз або істотно утруднюють реалізацію атак [9].

Цілі КЗІ випливають із поняття криптографії. Криптографія як теорія є методологічною основою сучасних систем забезпечення безпеки інформації в інформаційно-комунікаційних системах. Криптографія як технологія являє собою сукупність методів перетворення даних, орієнтованих на те, щоб захистити ці дані, зробити їх некорисними для незаконних користувачів. Такі перетворення забезпечують вирішення трьох проблем захисту даних: гарантію конфіденційності, цілісності та автентичності даних, які передаються чи зберігаються.

Завдання КЗІ. Для забезпечення безпеки даних необхідно підтримувати розв'язання трьох основних завдань:

− забезпечення конфіденційності даних, що передаються або зберігаються;

− підтвердження цілісності та автентичності даних;

− автентифікація абонентів при вході у систему та при з'єднанні.

Для реалізації цих завдань використовуються криптографічні технології шифрування автентифікації та цифрового підпису. Конфіденційність забезпечується за допомогою алгоритмів та методів шифрування, а також шляхом взаємної автентифікації абонентів на основі багаторазових чи одноразових паролів, цифрових сертифікатів, флеш-карт тощо. Цілісність та автентичність даних, що передаються, зазвичай досягаються за допомогою технології цифрового підпису. Автентичність дозволяє встановлювати з'єднання лише між легальними користувачами та попереджує доступ до телекомунікаційних послуг небажаних осіб.

КЗІ застосовується для захисту інформації, яка передається каналами зв'язку або зберігається в базах даних, робочих станціях, міститься у парольних та ключових даних систем автентифікації та розмежування доступу.

Чому проблема використання криптографічних методів в ІТС стала в даний момент особливо актуальною? З одного боку, розширилося використання комп'ютерних мереж, зокрема глобальної мережі Internet, по яких передаються великі обсяги інформації державного, військового, комерційного і приватного характеру, що не допускає можливість доступу до неї сторонніх осіб. З іншого боку, поява потужних комп'ютерів, технологій мережних і нейронних обчислень уможливила дискредитацію криптографічних систем, для яких ще недавно розкриття вважалося практично неможливим.

Проблемою захисту інформації шляхом її перетворення займається криптологія (*kryptos* – таємний, *logos* – наука). Криптологія поділяється на два напрями: криптографію і криптоаналіз. Цілі цих напрямів прямо протилежні.

Криптографія займається пошуком і дослідженням математичних методів перетворення інформації. Сфера ж інтересів криптоаналізу – дослідження можливості розшифрування інформації без знання ключів [10].

Сучасна криптографія включає чотири великих розділи:

1. Симетричні криптосистеми.
2. Криптосистеми з відкритим ключем.
3. Системи електронного підпису.
4. Керування ключами.

З основних напрямів використання криптографічних методів відзначимо

передачу інформаційними каналами зв’язку (наприклад, електронна пошта), встановлення дійсності переданих повідомлень, збереження інформації (документів, баз даних) на носіях у зашифрованому вигляді. Розглянемо деякі найбільш уживані терміни криптографії.

Криптосистеми поділяються на симетричні і з відкритим ключем. У симетричних системах і для шифрування, і для дешифрування використовується той самий ключ.

У системах з відкритим ключем використовуються два ключі – відкритий і закритий, котрі математично зв’язані один з одним. Інформація шифрується за допомогою відкритого ключа, що доступний усім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки отримувачу повідомлення.

Терміни “розподіл ключів” і “керування ключами” стосуються процесів системи обробки інформації, змістом яких є складання і розподіл ключів між користувачами.

Електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис [14].

Криптостійкістю називається характеристика шифру, що визначає його стійкість до дешифрування без знання ключа (тобто криптоаналізу). Є декілька показників криптостійкості, серед яких:

1. Кількість усіх можливих ключів.
2. Середній час, необхідний для криптоаналізу.

Перетворення тексту визначається відповідним алгоритмом і значенням параметра *k*. Ефективність шифрування з метою захисту інформації залежить від збереження таємниці ключа і криптостійкості ключа.

Абстрактно систему засекреченого зв’язку можна описати як безліч відображень безлічі відкритих повідомлень у безліч закритих. Вибір конкретного типу перетворення визначається ключем шифрування (або розшифрування).

Відображення повинні мати властивість взаємооднозначності, тобто при розшифруванні повинен виходити єдиний результат, що збігається з первісним відкритим повідомленням. Ключі шифрування й розшифрування можуть у загальному випадку бути різними, хоча для простоти міркувань припустимо, що вони ідентичні. Множина, з якої вибираються ключі, називається *ключовим простором*. Сукупність процесів шифрування, множини відкритих повідомлень, множини можливих закритих повідомлень і ключового простору називається *алгоритмом шифрування*. Сукупність процесів розшифрування, множини можливих закритих повідомлень, множини відкритих повідомлень і ключового простору називається *алгоритмом розшифрування*.

Розглянемо основні вимоги до криптосистем. Процес криптографічного закриття даних може здійснюватися, як програмно, так і апаратно. Апаратна реалізація відрізняється істотно більшою вартістю, однак вона має і переваги: висока продуктивність, простота, захищеність тощо. Програмна реалізація більш практична, допускає певну гнучкість у використанні.

Для сучасних криптографічних систем захисту інформації сформульовані такі загально прийняті вимоги:

1) зашифроване повідомлення має піддаватися читанню тільки за наявності ключа;

2) число операцій, необхідних для визначення використаного ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, повинно бути не меншим від загального числа можливих ключів;

3) число операцій, необхідних для розшифровування інформації шляхом перебору різних ключів, повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень);

4) знання алгоритму шифрування не повинно впливати на надійність захисту;

5) незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення;

6) структурні елементи алгоритму шифрування повинні бути незмінними;

7) додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути цілком і надійно сховані в шифрованому тексті;

8) довжина шифрованого тексту повинна бути рівною довжині вихідного тексту;

9) не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;

10) будь-який ключ з множини можливих повинен забезпечувати надійний захист інформації;

11) алгоритм повинен допускати, як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування.

В основі криптографічних алгоритмів лежать математичні перетворення, що дозволяють домогтися високої практичної стійкості більшості алгоритмів. Було доведено, що в криптографії існують тільки два основні типи перетворень – заміни й перестановки, усі інші є лише комбінацією цих двох типів. Таким чином, є криптографічні алгоритми, побудовані на основі заміни, перестановки й об'єднання цих двох перетворень.

У перестановочних шифрах символи відкритого тексту змінюють своє місце розташування. З іншого боку, у шифрах заміни один символ відкритого тексту заміщається символом зашифрованого тексту.

Класична криптографія, зокрема теорія зв'язку, у секретних системах, заснована К. Шеноном, виходила з того, що ключі, використовувані відповідно для шифрування й розшифрування, є секретними й однаковими, і передача їх повинна здійснюватися по надійному каналу обміну ключової інформації. Подібні алгоритми були названі симетричними, тому що шифрування й розшифрування відбувається на однакових ключах.

Однак розвиток теорії побудови алгоритмів шифрування з відкритими ключами, родоначальниками якої стали У. Діффі й М. Хеллман, поклала

початок повсюдному використанню асиметричних алгоритмів шифрування, у яких ключі шифрування й розшифрування різні залежно від застосування – один із ключів буде відкритим, тобто загальнодоступним, а інший необхідно зберігати в секреті. Різновидом таких криптосистем є системи електронних цифрових підписів, таємного електронного голосування, захисту від нав'язування неправильних повідомлень, електронного жеребкування й низка інших криптосистем.

Через деякий час симетричні алгоритми були розділені на два більші класи – блокові й потокові. У перших відкритий текст розбивається на блоки підходящої довжини, і кожний блок шифрується. У потокових алгоритмах кожний символ відкритого тексту зашифровується незалежно від інших і розшифровується в такий самий спосіб. Інакше кажучи, перетворення кожного символу відкритого тексту міняється від одного символу до іншого, у той час як для блокових алгоритмів у рамках шифрування блоку використовується одне й теж саме криптографічне перетворення.

Головна ідея, втілена в алгоритмах потокового шифрування, полягає у виробітку на основі секретного ключа послідовності символів із вхідного алфавіту, з яким працює алгоритм шифрування. Це можуть бути як, наприклад, символи англійської мови, так і цифри десяткової системи вирахування, при цьому вхідний текст перетвориться відповідно до обраного алфавіту. Слід урахувати, що така послідовність має довжину, яка дорівнює відкритому тексту. Її іноді називають гамою.

Шифрування й розшифрування може, наприклад, здійснюватися шляхом модульного додавання символу відкритого тексту із символом гами. Стійкість потокових алгоритмів шифрування залежить від того, наскільки вироблена гама буде мати властивість рівноймовірності появи чергового символу.

Потокові алгоритми мають високу швидкість шифрування, однак при їхньому програмному використанні виникають певні труднощі, що звужує область їх практичного застосування.

Слід зазначити, що в останні роки на базі вдосконалювання електронних технологій з'явилися нові теоретичні розробки в області квантової криптографії, заснованої на принципах невизначеності Гейзенберга.

Усе різноманіття існуючих криптографічних методів можна звести до таких класів перетворень.

Перестановки – метод криптографічного перетворення, що полягає в перестановці символів вихідного тексту за більш чи менш складним правилом. Використовується, як правило, у поєднанні з іншими методами.

Системи підстановок – найбільш простий вид перетворень, що полягає в заміні символів вихідного тексту на інші (того ж алфавіту) за більш чи менш складним правилом. Для забезпечення високої криптостійкості потрібне використання великих ключів.

Гамування є криптографічним перетворенням, яке широко використовується. Принцип шифрування гамуванням полягає в генерації гами шифру за допомогою датчика псевдовипадкових чисел і накладенні отриманої гами на відкриті дані.

Широко використовується *блокове шифрування*, яке являє собою послідовність (з можливим повторенням і чергуванням) основних методів перетворення, що застосовуються до блоку (частини) тексту, який шифрується. Блокові шифри на практиці зустрічаються частіше, ніж “чисті” перетворення того чи іншого класу, через їх більш високу криптостійкість. Російський і американський стандарти шифрування базуються саме на цьому класі шифрів.

Хоча б якими складними і надійними були криптографічні системи, їх слабке місце при практичній реалізації – проблема розподілу ключів. Для того щоб був можливий обмін конфіденційною інформацією між двома суб’єктами ІТС, ключ повинен бути згенерований одним із них, а потім якимось чином знову ж у конфіденційному порядку переданий іншому. Тобто у загальному випадку для передачі ключа знову ж потрібне використання якоїсь криптосистеми.

2.3.6. Особливості використання віртуальних захищених мереж (VPN) для забезпечення кібербезпеки інформаційно-телекомунікаційних систем

Сьогодні Інтернет є більш доступним, ніж коли-небудь раніше, і постачальники Інтернет-послуг (ISP) продовжують розвивати більш швидкі і надійні послуги при менших витратах, ніж виділені лінії. Щоб скористатися цим, більшість підприємств замінили виділені лінії новими технологіями, які використовують Інтернет-з'єднання, не жертвуючи продуктивністю і безпекою. Підприємства почали зі створення інтрамереж, які є захищеними внутрішніми мережами, призначеними для використання тільки співробітниками компанії. Інтернет дозволив віддаленим колегам працювати разом за допомогою таких технологій, як спільне використання робочого столу. Використовуючи віртуальні захищені мережі (VPN, Virtual Private Network) підприємства можуть розширити ресурси своєї локальної мережі, дозволяючи співробітникам працювати у віддалених офісах або будинках [15].

Концепція віртуальної захищеної мережі або просто VPN з'явилася як альтернатива захищеної комунікації через мережі загального користування, такі як Інтернет, і стала технологією надання послуг, яка орієнтована на безпечність та гарантує цілісність, конфіденційність і доступність інформації. Безпека передачі інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий канал обміну інформацією. (рис. 2.6). Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

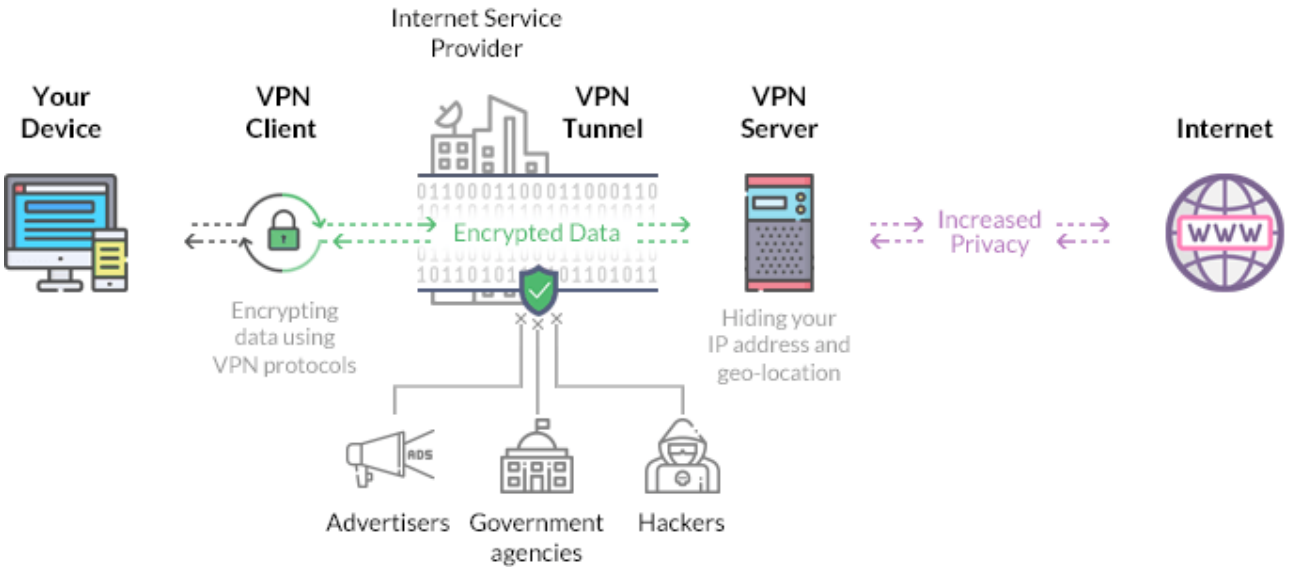

Рис. 2.6. Технологія VPN

Захист інформації в процесі її передачі по тунелю VPN заснований на:

− автентифікації взаємодіючих сторін;

− криптографічному закритті (шифруванні) даних, що передаються;

− перевірці автентичності та цілісності інформації, яка надходить.

VPN – це безпечний тунель між двома або більше комп'ютерами в Інтернеті, що дозволяє їм отримувати доступ один до одного як в локальній мережі. У минулому VPN здебільшого використовувалися компаніями для надійного зв'язку віддалених філій або підключення роумінг-співробітників до офісної мережі, але сьогодні вони також є важливою послугою для споживачів, захищаючи їх від атак при їх підключенні до загальнодоступних бездротових мереж. Відкриті бездротові мережі несуть серйозну загрозу для користувачів, оскільки зловмисники, які сидять в тих самих мережах, можуть використовувати різні методи для відстеження веб-трафіка і навіть захоплення облікових записів на сайтах, які не використовують протокол безпеки HTTPS. Крім того, деякі оператори мереж Wi-Fi навмисно вводять рекламу у веб-трафік, що може привести до небажаного відстеження.

У деяких регіонах світу уряди відстежують користувачів, які відвідують певні веб-сайти, щоб виявити їх політичну приналежність і визначити дисидентів – практиків, які загрожують свободі слова і прав людини.

Використовуючи VPN-з'єднання, весь трафік можна безпечно маршрутизувати через сервер, розташований в іншому місці у світі. Це захищає від локальних спроб відстеження і зламу, і навіть приховує реальну адресу Інтернет-протоколу з веб-сайтів і служб, до яких відбувається звернення.

Так, наприклад, використання користувачами технологій VPN для обходу блокування українськими провайдерами російських Інтернет-ресурсів може загрожувати персональній кібербезпеці громадян, а також кібербезпеці всієї країни. Про це заявили представники Інтернет-асоціації України (ІнАУ) на прес-конференції 31 травня 2017 року [16].

За різними оцінками, після введення в дію Указу Президента України “Про

застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", який набув чинності 17 травня 2017 року, 20 – 30% користувачів "Яндекса", "Вконтакте", "Одноклассников" і Mail.ru тощо встановлюють собі VPN-сервіси (насамперед, на мобільних пристроях), щоб мати доступ до заблокованих ресурсів. Цей Указ заборонив Інтернет-провайдерам надавати Інтернет-користувачам доступ до російських соціальних мереж "Вконтакте" та "Одноклассники", Інтернет-порталу "Яндекс" (пошукових і десятки супутніх сервісів), поштового сервісу Mail.ru, а також до сайтів розробників популярних антивірусів "Лаборатория Касперского" і "Доктор Веб". За словами експертів, під час входу зі своїх гаджетів у свою домашню мережу, чи в корпоративну мережу, чи мережу державної установи, до яких мають доступ, відбувається наступне: мобільні пристрої продовжують тримати зашифроване з'єднання з VPN-сервером десь за кордоном і відправляти туди дані про користувача та мережу. Пристрій має змогу збирати інформацію про локальну мережу та відправляти її куди завгодно, в тому числі з використанням камери чи мікрофона. І це є загрозою для кібербезпеки. Використання користувачами VPN несе загрозу насамперед для корпоративного та державного секторів. Після того, як оператори почали блокувати деякі Інтернет-ресурси, спецслужби різних країн почали надавати для нашої держави свої VPN-сервери, і таким чином мати ще більший доступ до корпоративних сегментів нашої держави.

"Російська Федерація та її спецслужби свідомо роблять браузери, VPN-сервери, і замість частини трафіка українських користувачів російських соцмереж отримують весь трафік і можливість потрапити у внутрішню українську корпоративну мережу", – заявив член правління ІнАУ Максим Тульєв. Небезпечними, на його думку, є безкоштовні VPN-сервіси, оскільки технологія VPN потребує значних коштів.

Проте не всі VPN-сервіси несуть загрозу, уточнили спікери. Було **рекомендовано** використовувати мережу TOR – вона не містить прихованих дірок, при цьому дає змогу обходити блокування і не принесе загрози підприємству. Крім TOR можна використовувати браузер Opera із вбудованим VPN, який не знаходиться під контролем Російської Федерації. У числі безпечних браузерів названі Firefox, Chrome, Edge, Safari.

Експерти **не рекомендують** використовувати новий браузер FreeU, "Яндекс.Браузер", а також будь-які нові сервіси, які щойно вийшли на ринок.

"VPN не несе ризику сам по собі, якщо ним правильно користуватися", - сказав представник міжнародної IT-організації ISACA Гліб Пахаренко. "Не демонізуйте технологію VPN. Вона існує давно, її багато хто використовує, у тому числі банки", – додав Анатолій П'ятников. А Гліб Пахаренко нагадав, що VPN дає доступ користувачам на непідконтрольних Україні територіях до заблокованих там українських ресурсів.

Існують різні технології VPN з різним ступенем шифрування. Наприклад, тунельний протокол "точка-точка" (PPTP) працює швидко, але не такий безпечний, ніж інші протоколи, такі як IPSec або OpenVPN, що використовують SSL / TLS (Secure Sockets Layer / Transport Layer Security). Крім того, при

використанні VPN на основі TLS також важливі тип алгоритму шифрування та довжина ключа.

З'єднання “точка-точка” – мається на увазі, що воно завжди встановлюється між двома комп'ютерами, які називаються “вузлами”. Кожен вузол відповідає за шифрування даних до того, як вони потраплять в тунель, і дешифрування цих даних відбудеться після того, як вони покинуть тунель. Після підключення до VPN-сервера всі дані починають передаватися між комп’ютером та сервером у зашифрованому вигляді. Вже з VPN-сервера всі запити передаються до зовнішніх ресурсів.

Хоча OpenVPN підтримує безліч комбінацій шифрів, протоколів обміну ключами й алгоритмів хешування, найбільш поширеною реалізацією, запропонованою постачальниками послуг VPN для з'єднань OpenVPN, є шифрування AES з обміном ключами RSA і сигнатурами SHA. Рекомендованими параметрами є шифрування AES-256 с ключем RSA довжиною не менше 2048 біт і криптографічний хеш-функція SHA-2 (SHA-256) замість SHA-1.

Слід зазначити, що шифрування може впливати на швидкість з'єднання. Вибір технології VPN та методів шифрування повинен проводитися для кожного конкретного випадку, в залежності від того, які дані будуть передаватися.

VPN поділяється на такі види [15]:

1. *Intranet VPN*. Такий варіант дозволяє об'єднати кілька філіалів організації. Передача даних здійснюється по відкритих каналах. Інтернет може використовуватися для звичайних компаній і для мобільних офісів. Але слід мати на увазі, що такий спосіб передбачає установку серверів в усіх офісах.

2. *Extranet VPN*. Доступ до інформації підприємства надається клієнтам й іншим зовнішнім користувачам. При цьому, їх можливості по використанню системи помітно обмежені. Не призначені для абонентів файли надійно захищаються засобами шифрування. Це відповідне рішення для фірм, яким необхідно забезпечити своїм клієнтам доступ до певних відомостей.

3. *Remote Access*. У цьому випадку створюється захищений канал між офісом і віддаленим користувачем, що підключаються до ресурсів підприємства з домашнього персонального комп’ютера через Інтернет. Подібні системи прості в побудові, але менш безпечні, ніж їх аналоги, вони використовуються підприємствами зі значною кількістю віддалених співробітників.

4. *Client / Server*. Цей варіант дозволяє обмінюватися даними між декількома вузлами всередині одного сегмента. Він користується найбільшою популярністю в організацій, яким необхідно в рамках однієї фізичної мережі створити кілька логічних, для захисту трафіка під час поділу використовується шифрування.

Тунельні протоколи VPN пропонують різні функції та рівні безпеки, і для кожного з них є переваги та недоліки. Існує п'ять основних тунельних протоколів VPN: Тунельний протокол захищених сокетів (SSTP); Тунельний протокол “точка-точка” (PPTP); Тунельний протокол другого рівня (L2TP);

OpenVPN і Internet Key Exchange версії 2 (IKEv2).

− SSTP використовує протокол HTTPS для передачі трафіка через брандмауери та веб-проксі, які можуть блокувати інші протоколи. SSTP надає механізм для перенесення трафіка протоколу “точка-точка” (PPP) по каналу SSL. Використання PPP дозволяє підтримувати надійні методи автентифікації, а SSL забезпечує безпеку на рівні транспорту з розширеним узгодженням ключів, перевіркою шифрування та цілісності.

− PPTP дозволяє зашифрувати багатопротокольний трафік, а потім обернути його в заголовок, який буде відправлений через мережу інтернет-протоколу (IP). PPTP можна використовувати для віддаленого доступу і VPN-з'єднань “точка-точка”. При використанні Інтернету PPTP-сервер є VPN-сервером з підтримкою PPTP з одним інтерфейсом в Інтернеті та другим інтерфейсом в корпоративній інтрамережі. PPTP використовує з'єднання протоколу управління передачею для управління тунелями та інкапсуляції загальної маршрутизації для перенесення кадрів PPP для даних у тунелі.

− L2TP дозволяє зашифрувати багатопротокольний трафік, а потім використовувати будь-який носій, що підтримує доставку даних PPP, наприклад, IP або асинхронний режим передачі. L2TP – це комбінація PPTP і Layer 2 Forwarding (L2F). L2TP представляє кращі функції PPTP і L2F. На відміну від PPTP, L2TP покладається на IP-безпеку (IPsec) в транспортному режимі для служб шифрування. Комбінація L2TP і IPsec відома як L2TP / IPsec. Обидва L2TP і IPsec повинні підтримуватися як клієнтом VPN, так і VPN-сервером. L2TP / IPsec - ідеальна передова секретність.

− OpenVPN – це програмний додаток з відкритим вихідним кодом, який реалізує методи VPN для створення безпечних з'єднань “точка-точка” або “сайт-сайт” у маршрутизованих або мостових конфігураціях і засобах віддаленого доступу. Він використовує власний протокол безпеки, який використовує SSL / TLS для обміну ключами. OpenVPN дозволяє однорангові вузли автентифікувати один одного за допомогою секретного ключа, сертифіката або імені користувача та паролю. Більшість провайдерів VPN, що використовують OpenVPN, використовують пряму секретність.

− IKEv2 – це протокол на основі протоколу IPSec, який використовується в Windows 7 і вище. IKEv2 – це стандарт наступного покоління для безпечного обміну ключами між одноранговими VPN-пристроями. IKEv2 особливо корисний в автоматичному відновленні VPN-з'єднання, коли користувачі тимчасово втрачають свої Інтернет-з'єднання.

Отже, за типом використовуваного середовища VPN можна поділити на:

− *захищені*. Найпоширеніший варіант віртуальних захищених мереж. За його допомогою можливо створити надійну і захищену підмережу на основі ненадійної мережі, зазвичай, Інтернету. Прикладом захищених протоколів VPN є: IPSec, SSL та PPTP. Прикладом використання протоколу SSL є програмне забезпечення OpenVPN.

− *довірчі*. Використовують у випадках, коли середовище, яким передають дані, можна вважати надійним і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки

стають неактуальними. Прикладами подібних VPN рішень є: Multi-protocol label switching (MPLS) і L2tp (Layer 2 Tunnelling Protocol). (Коректніше сказати, що ці протоколи перекладають завдання забезпечення безпеки на інших, наприклад, L2TP, як правило, використовують разом з IPSec).

VPN також може надавати спеціалізовані послуги для підключених до Інтернету пристроїв, таких як IP-телефонія або керування пристроями. VPN можна використовувати для безпечного підключення цих пристроїв до обчислювальної інфраструктурі, яка надає спеціалізовані послуги віртуальної захищеної мережі. VPN дозволяє безпечну передачу даних, що передаються або отримуються різними пристроями, які входять до області Інтернету речей (IoT).

Існує чотири основних типи VPN:

− *VPN-брандмауер* оснащений як брандмауером, так і VPN-можливостями. Цей тип використовує захист, що надається брандмауерами, для обмеження доступу до внутрішньої мережі та забезпечує зміну адрес, автентифікацію користувача, аварійні сигнали і протоколювання.

− *Апаратна VPN* забезпечує високу пропускну здатність мережі, а також покращує продуктивність і надійність, але є дорогою.

− *Програмна VPN* забезпечує гнучкість з точки зору управління трафіком. Це найкращий варіант, коли кінцеві вузли не контролюються однією стороною навіть при використанні різних брандмауерів і маршрутизаторів.

− *Рівень захищених сокетів (SSL) VPN* дозволяє користувачам підключатися до VPN-пристроїв за допомогою веб-браузера. SSL використовується для шифрування трафіка між веб-браузером і пристроєм VPN.

Необхідно також розуміти, що ризики безпеки, пов'язані з VPN, також існують. До них відносяться захоплення VPN, в якому неавторизований користувач захоплює VPN-з'єднання з віддаленого клієнта, атаки man-in-the-middle, в яких зловмисник здатний перехоплювати дані, слабку автентифікацію користувача, розділене тунелірування, в якому користувач отримує доступ до небезпечного підключенню до Інтернету, а також доступ до VPN-підключення до захищеної мережі, зараження шкідливими програмами на клієнтському комп'ютері, надання занадто значної кількості прав доступу до мережі та витоку DNS, в яких комп'ютер використовує DNS- з'єднання за замовчуванням, а не захищений DNS-сервер VPN.

Щоб усунути ці ризики, необхідно враховувати додаткові функції безпеки VPN під час вибору продуктів VPN. До них відносяться обов'язкові функції безпеки:

− підтримка надійної автентифікації;

− надійні алгоритми шифрування;

− використання антивірусного програмного забезпечення і засобів виявлення та запобігання вторгнень;

− надійний захист за замовчуванням для портів адміністрування та обслуговування;

− підтримка цифрового сертифіката;

− підтримка реєстрації та аудиту;

− можливість призначати адреси клієнтам у захищеній мережі, при цьому всі адреси залишаються закритими.

Крім того, для адміністраторів мережі та безпеки, а також для співробітників служби підтримки і для віддалених користувачів необхідно провести навчання, щоб вони слідували кращим передовим методам безпеки під час впровадження VPN і постійного використання.

Ще один спосіб поліпшити безпеку VPN – це цілковита пряма секретність (PFS, perfect forward secrecy). Якщо використовується PFS, зашифровані повідомлення та сеанси, записані в минулому, не можуть бути отримані та дешифровані при компрометуванні довгострокових секретних ключів або паролів. З PFS кожен сеанс VPN використовує різну комбінацію ключів шифрування, тому навіть якщо зловмисники вкрадуть один ключ, вони не зможуть розшифрувати будь-які інші сеанси VPN.

Питання самоконтролю

1. Характеристика основних завдань управління кібербезпекою.
2. Сутність та основні процедури управління кібербезпекою.
3. Вимоги міжнародних стандартів до процесу управління кібербезпекою.
4. Характеристика сучасних кібератак на інформаційно-телекомунікаційні системи та інформаційні ресурси в умовах ведення кібервійни.
5. Сутність та класифікація кібератак на інформаційно-телекомунікаційні системи та інформаційні ресурси.
6. Характеристика APT-кібератак як основної форми боротьби в кіберпросторі.
7. Технологічні аспекти захисту інформації в інформаційно-телекомунікаційних системах.
8. Технологічні рішення щодо ідентифікації, автентифікації та авторизації користувачів інформаційно-телекомунікаційних систем.
9. Особливості функціонування систем виявлення та попередження кіберзагроз та оцінки кіберризиків.
10. Антивірусний захист інформаційно-телекомунікаційної системи.
11. Використання брандмауерів (firewall) для контролю та фільтрації трафіка в інформаційно-телекомунікаційних системах.
12. Особливості використання технологій та програмних засобів криптозахисту та криптоаналізу інформації в інформаційно-телекомунікаційних системах.
13. Особливості використання віртуальних захищених мереж (VPN) для забезпечення кібербезпеки інформаційно-телекомунікаційних систем.
14. Особливості організації, підготовки та проведення навчань з кібербезпеки.

Інформаційні джерела

1. Про Стратегію кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016.
2. Про основні засади забезпечення кібербезпеки України: Закон України (зі змінами) від 05.10.2017 р. № 2163-VIII. Дата оновлення: 08.07.2018. URL: https://zakon.rada.gov.ua/laws/show/ 2163-19.
3. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.
4. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. (ISO/IEC 27001:2013; Cor 1:2014, IDT) [Чинний від 2017-01-01]. Вид. офіц. Київ: ДП "УкрНДНЦ". 2016. 22 с.
5. ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки, 2017. 65 с.
6. Впровадження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. Доповідь А. Конопльової 01.10.2019. URL: https://www.slideshare.net/AnastasiiaKonoplova?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideview.
7. Про основні засади забезпечення кібербезпеки України: Закон України (зі змінами) від 05.10.2017 р. № 2163-VIII. Дата оновлення: 08.07.2018. URL: https://zakon.rada.gov.ua/laws/show/ 2163-19.
8. Пількевич І.А. , Лобанчикова Н.М. , Молодецька К.В. Захист інформації в автоматизованих системах управління: навч. посіб. – Житомир: Вид-во ЖДУ ім.І.Франка. 2015. 226 с.
9. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України (зі змінами) від 5 липня 1994 року № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
10. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки: навч.посіб. Київ. 2018. 320 с.
11. Рекомендації CERT-UA щодо протидії APT (Advanced Persistent Threat). URL: https://cert.gov.ua/recommendations/18.
12. Перелік кібератак. URL: https://uk.wikipedia.org/wiki/перелік_кібератак.
13. Субач І. Ю. Системи виявлення кібернетичних атак: стан справ та перспективи розвитку // *Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення*: тези доп. VII наук.-техн.конф. (м. Київ, 23-24 жовт. 2014 р.). Київ. 2014. С. 60-64.
14. Про електронні довірчі послуги: Закон України (зі змінами) від 5.10.2017 року № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#n534.
15. Николахин А.Ю Использование технологии VPN для обеспечения информационной безопасности // Экономика и качество систем связи. 2018. № 3 (9). URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoybezopasnosti.

16. Технологія VPN може загрожувати кібербезпеці. URL: https://detector.media/infospace/article/126505/2017-05-31-tekhnologiya-vpn-mozhe-zagrozhuvati-kiberbezpetsi-inau/

Розділ 3 ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА КІБЕРОБОРОНИ

3.1. Основи організації наукових досліджень та підготовки фахівців Сектору безпеки і оборони з кібербезпеки

3.1.1. Аналіз досвіду провідних країн світу з підготовки фахівців кібербезпеки та кібероборони

Ефективність застосування військ (сил), оснащених сучасними високотехнологічними засобами ОВТ, найбільшою мірою залежить від якості підготовки особового складу та потребує відповідного удосконалення і розвитку системи військової освіти і науки. Експлуатація високотехнологічних зразків та комплексів ОВТ, які мають високу вартість та вирішують особливо важливі завдання особовим складом, який не має необхідного рівня і якості підготовки, не дозволяє ефективно їх застосовувати (повністю реалізовувати їх можливості). При цьому, дуже часто у зв'язку з непрофесійним застосуванням такі комплекси (засоби) виходять з ладу. Тобто завдання не виконуються і держава несе значні збитки.

Тому, серед загроз національній безпеці у воєнній сфері багато країн уже зараз вбачають не тільки у відставанні в розробленні та прийнятті на озброєння нових високотехнологічних засобів озброєння і військової техніки. Ще більшою мірою це стосується якості підготовки військових кадрів, які повинні на високому рівні виконувати завдання з управління військами (силами) і засобами та забезпечити їх раціональне застосування у війнах і збройних конфліктах сьогодення та майбутнього.

Останнім часом підвищена увага до проблем військової освіти і науки спостерігається майже в усіх провідних країнах світу. Це обумовлено загальною тенденцією зниження рівня професійної підготовки випускників військових закладів вищої освіти і, насамперед, у сфері отримання практичних навичок ефективної діяльності під час впровадження та застосування інноваційних оборонних технологій.

Найбільших успіхів у підготовці фахівців з кібербезпеки та кібероборони у світі досягли США, Ізраїль, Японія, РФ, КНР та країни-члени блоку НАТО. Невід'ємною складовою забезпечення кібербезпеки і кібероборони будь-якої держави є питання розбудови, удосконалення та нарощування систем наукових досліджень цих питань і кіберосвіти.

При розробці методології кіберосвіти фахівців Сектору безпеки і оборони України необхідно враховувати низку особливостей, притаманних сучасним інформаційним технологіям: швидка зміна поколінь інформаційно-телекомунікаційних технологій; постійне зростання можливостей впливу на складові кіберсистем та об'єкти критичної інформаційної інфраструктури; необхідність постійного оновлення знань з питань кібербезпеки; різні рівні

здатності і готовності до навчання тих, хто навчається; особливості курсу кібербезпеки; значна кількість специфічних складових кібербезпеки і кібероборони тощо.

Згідно з Законом України "Про національну безпеку України" [1] *Сектор безпеки і оборони* – система органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу України, діяльність яких перебуває під демократичним цивільним контролем і відповідно до Конституції та законів України за функціональним призначенням спрямована на захист національних інтересів України від загроз, а також громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки України.

Отже, потребує дослідження та вирішення таких завдань:

− здійснення аналізу існуючих систем підготовки фахівців з кібербезпеки і кібероборони у провідних країнах світу в контексті кібербезпеки і кібероборони України;

− здійснення аналізу існуючого стану системи і методології підготовки фахівців з питань кібербезпеки та кібероборони Сектору безпеки і оборони України;

− здійснення розробки системи, змісту і методології підготовки фахівців з питань кібербезпеки та кібероборони для Сектору безпеки і оборони України.

Важливим аспектом формування системи освіти фахівців з питань кібербезпеки і кібероборони є вивчення та дослідження досвіду провідних країн світу, у першу чергу США, де питанням підготовки фахівців кібербезпеки приділяється надзвичайна увага.

Ще у 1998 році у США був створений Національний центр захисту інфраструктури (NIPC), що поєднує представників органів влади, військового і приватного секторів для захисту національної інфраструктури (http://www.staysafeonline.info). Міжнародна асоціація фахівців з комп'ютерних досліджень (IACIS) забезпечує навчання в області комп'ютерних технологій (http://www.nips.gov). Успішно функціонує Національний союз кібербезпеки, створений спільно урядом і промисловцями США. Мета союзу – розробка підходів до проблеми безпеки в кіберпросторі, підвищення рівня освіти у сфері інформаційної безпеки, притягнення суспільної уваги до проблеми кібертероризму [2, 3]. Не менше уваги приділяється і формуванню системи освіти фахівців з кібербезпеки та кібероборони. Так, у складі Департаменту внутрішньої безпеки (Department of Homeland Security's (DHS)) США сформовано відділ освіти та підвищення освіченості з питань кібербезпеки і кібероборони [4]. Завданнями відділу є формування єдиної державної політики, системи та методології підготовки фахівців з кібербезпеки і кібероборони. Отже, цим відділом відпрацьовано та прийнято низку документів:

1. Національна програма підвищення освіченості з питань кібербезпеки. Мета програми сприяти індивідуальній кіберстійкості та освіченості населення з питань кібербезпеки, розумінню кіберзагроз та простих дій щодо їх нейтралізації.

2. Національна програма розвитку професіоналізму та розвитку персоналу. Мета програми сприяти підготовці фахівців з кібербезпеки, які володіють необхідними знаннями, навичками та здатні захистити інтереси нації від існуючих та виникаючих проблем в усіх складових кібербезпеки.

3. Національна програма освіти та тренінгу у галузі кібербезпеки (National Cybersecurity Education and Training Program (NCTEP)). Мета програми – розширити підготовку професіоналів кібербезпеки за рахунок створення динамічної освітньої системи, здатної підготувати нове покоління співробітників кібербезпеки, які будуть здатні до захисту від існуючих та майбутніх кіберзагроз.

У своєму виступі представник Департаменту внутрішньої безпеки (DHS) США Ноэль Кайл 8 червня 2017 року зазначив: "Щоб ліквідувати розрив між зростаючою потребою у фахівцях з кібербезпеки та системою підготовки кваліфікованого персоналу, вкрай важливо, щоб всі спільноти – галузеві організації, федеральні агентства й академічні заклади – з'єднались та прийняли комплексний підхід до координації зусиль у галузі освіти, навчання та працевлаштування фахівців кібербезпеки" [5].

У рамках програми NCTEP DHS пропонує кілька безкоштовних курсів для підтримки освіти з питань кібербезпеки. При цьому для вчителів молодших, середніх та старших класів передбачено надання навчальних матеріалів з кібербезпеки. Для державних службовців і ветеранів сформовані програми і здійснюється безкоштовне навчання та підвищення кваліфікації з кібербезпеки на базі закладів академічної освіти. DHS веде навчальний каталог розроблених навчальних курсів з вивчення питань кібербезпеки за всю країну. Також вирішуються питання розробки єдиної термінології, ведеться повний список задач кібернетичної безпеки, знань, навичок та компетентностей необхідних для вирішення цих задач [6]. Це надає змогу реалізувати комплексний підхід у побудові системи підготовки фахівців кібербезпеки з єдиним центром управління.

Найбільші комерційні компанії, що проводять навчання в області інформаційної безпеки: Check Point Software Technologies, Cisco Systems, IBM Tivoli Systems Global Security Laboratory, Internet Security Systems, Microsoft, Network Associates, Prosoft Training. Com, Sun Microsystems, Symantec. Серед навчальних центрів, що спеціалізуються на підготовці фахівців з кіберзахисту найбільш відомими є: CERT, GIAC, CSI, Cisco Systems.

Питання інформаційної і кібербезпеки вивчаються тими, хто навчається, в усіх військових навчальних закладах МО США та інших країнах-членах НАТО, передусім *у видових закладах вищої освіти*: Військова академія Армії США у Вест-Пойнті (US Militari Academi, West Point, NY, 16.03.1802) – коледж електронних та комп'ютерних систем (Department of Electrical Engineering and Computer Science); центр інформаційних технологій і операцій (Information Technology and Operations Center), у складі якого "Лабораторія досліджень і аналізу інформаційної війни" (The Information Warfare Analysis and Research Laboratory (IWAR)); Академія Військово-Повітряних Сил в Колорадо-Спрінгс

(United States Air Force Academy, Колорадо); Академія Військово-Морських Сил в Анаполісі (Меріленд).

Ці питання вивчаються і *в інших військових закладах вищої освіти*, таких як: Технологічний університет ВПС (Air Force Institute of Technology, Wright-Patterson AFB, Ohio) – факультети Інформаційної безпеки та Військово-космічних сил; Університет інформаційних технологій (Universiti of information Technologi, Fort Gordon, GA); Університет національної оборони (National Defense University) – факультет інформаційних та кібернетичних наук (College of Information and Cyberspace); коледж інформаційного менеджменту (Information Resources Management College-School of Information Warfare and Strategy at NDU) Fort McNair, Washington, D.C.; командно-штабний коледж – факультет № 4 (Інформаційно-психологічних операцій) (The Joint Forces Staff College, Norfolk, VA).

У видових навчальних і дослідницьких центрах інформаційної війни: Air Force Information Warfare Center (AFIWC), Neelis Air Force Base, 1.07.1953; Fleet Information Warfare Center (FIWC), Norfolk, 4.11.2005; Space Information Warfare Center (SIWC), Schriever Air Force Base, Colorado, 8.12.1993 та інших.

У військових закладах вищої освіти з підготовки фахівців кібербезпеки гуманітарного профілю: Військовий інститут іноземних мов ЗС США (Defense Language Institute, Monterey); Центр і школа спеціальних методів війни імені Дж. Ф. Кеннеді (Форт-Брег); школа підготовки спеціалістів засобів масової інформації МО США.

Для удосконалення методів навчання в Міністерстві оборони США створений спеціальний підрозділ – “Управління програм з інформаційної безпеки” (Information Assurance Program Office). Як видно, мережа підготовки фахівців досить розвинута. Але навіть за таких масштабів, на думку експертів, у США відчувається нестача фахівців в області кібербезпеки [7].

На відміну від США, зважаючи на значно меншу чисельність збройних сил, в інших країнах-членах блоку НАТО (Великобританія, Федеративна Республіка Німеччина, Республіка Польща тощо) ефективність вирішення зазначених проблем досягається шляхом формування та забезпечення функціонування інтегрованих навчально-наукових, дослідно-випробувальних комплексів (високотехнологічних оборонних кластерів), які здійснюють на єдиній базі освітню і наукову діяльність за високотехнологічними напрямами.

Найбільш вдало інтеграція військової освіти і науки за високотехнологічними напрямами реалізована у Військовому університеті технологій (Республіка Польща), де на одній базі зосереджені всі високотехнологічні спеціальності та спеціалізації підготовки військових фахівців (факультети: національної безпеки, електроніки та телекомунікацій, енергетики, технічної фізики, геодезії і картографії, інформатики, інженерії безпеки, інженерії матеріалів, криптології і кібербезпеки, авіації і космонавтики, механіки і машинобудування, механотроніки, управління тощо) та підрозділи наукових досліджень з цих питань [8]. Те ж саме реалізовано в Університеті Бундесверу у Мюнхені (ФРН) (спеціальності: електротехніка та інформаційні технології, комп'ютерні науки, аерокосмічна інженерія,

менеджмент інформаційних систем, математична інженерія, політологія та соціальні науки, розвиток людських ресурсів, медіа-менеджмент, дослідження міжнародної безпеки, економіко-організаційні науки, інженерна психологія, комп'ютерні технології та комунікаційні технології, машинобудування, комп'ютерна техніка, державне управління, оборонна інженерія) [9, 10]. За рахунок інтеграції високотехнологічних напрямів підготовки фахівців і наукових досліджень в єдиному навчальному закладі та на єдиній базі в провідних країнах світу забезпечують позбавлення їх дубляжу і розпорошення зусиль при вирішенні однотипних завдань, раціональне використання та економію ресурсів і кадрового потенціалу, полігонної, матеріально-технічної бази, ефективне виконання замовлень на підготовку (перепідготовку) фахівців і здійснення наукових досліджень для усіх міністерств і відомств Сектору безпеки і оборони держави в рамках єдиних стандартів. В подібних єдиних для держави високотехнологічних військових навчально-науково-випробувальних центрах зосереджена підготовка фахівців для Секторів безпеки і оборони у більшості країн-членів НАТО та інших провідних країнах світу.

Так, за дорученням НАТО і Консорціуму програми “Партнерства заради миру” (the Partnership for Peace Consortium (PfPC)), військових академій та дослідницьких інститутів, багатонаціональною командою вчених та практиків був розроблений документ “Кібербезпека: типовий навчальний план” [11]. Цей документ за мету має представити країнам НАТО та країнам-партнерам цілі поглибленого навчання та підтримки навчальних програм курсів теоретичної підготовки, в широкому сенсі пов’язаних з кібербезпекою. “Кібербезпека: типовий навчальний план” складається з чотирьох розділів: 1) Кіберпростір і основи кібербезпеки; 2) Вектори ризику; 3) Міжнародні організації в сфері кібербезпеки, політики і стандартів; 4) Управління кібербезпекою в національному контексті. Чотири розділи та супутні матеріали були ретельно підібрані з метою охоплення гранично широкого спектру питань та предметів кібербезпеки.

3.1.2. Погляди щодо побудови національної системи підготовки фахівців з питань кібербезпеки та кібероборони

Фахівців з високотехнологічних напрямів (радіоелектроніки, ІТ, військової кібернетики та систем управління, технічних видів розвідки, робототехнічних систем та комплексів боротьби з ними, інформаційної та кібербезпеки, захисту інформації, радіоелектронної боротьби, космічних і геоінформаційних систем, зв'язку тощо) в Україні готують у міжвидових інститутах (Житомирському військовому інституті імені С.П. Корольова, Військовому інституті телекомунікацій та інформатизації імені Героїв Крут, Військовому інституті Київського національного університету імені Тараса Шевченка, які разом, об’єднано можна розглядати, як певний аналог Університету Бундесверу в Мюнхені (ФРН) або Військового університету технологій (Військової технічної академії імені Ярослава Домбровського (Республіка Польща) інших подібних інтегрованих технологічних військових закладів вищої освіти країн-членів НАТО).

Аналіз питань підготовки фахівців кібербезпеки Сектору безпеки і оборони України в закладах вищої освіти, що підпорядковані Міністерству оборони України, Генеральному штабу Збройних Сил України, Міністерству внутрішніх справ України, Службі безпеки України, Державній службі спеціального зв'язку та захисту інформації тощо показує аналогічну (так само, як і в цивільних закладах вищої освіти) проблему відсутності єдиної методології і сформованої системи підготовки фахівців з питань кібербезпеки та загальної кіберосвіти. Відсутність єдиних керівних документів, методичного забезпечення навчання, розбіжність у поглядах на мету, завдання та зміст підготовки з питань кібербезпеки у ВВНЗ знижує ефективність та якість підготовки фахівців для сектору безпеки та оборони України в цілому. Особливо яскраво це проявилося з початком повномасштабної "гібридної війни" проти України, в якій значна частка протиборства сторін відбувається в інформаційному та кіберпросторах.

Підготовку фахівців Сектору безпеки і оборони України з питань кібербезпеки і кібероборони доцільно проводити з урахуванням профілей їх підготовки та рівнів освіти. При цьому створюються умови щоб фахівці, які не мають технічної освіти, отримали більш повне уявлення про технологічні аспекти кібербезпеки і достатньою мірою розумілися щодо особливостей реалізації політики кібербезпеки, як у сфері оборони держави, так і на національному та міжнародному рівнях, а фахівці з високотехнологічних напрямів отримали повні і всебічні сучасні знання з питань кібербезпеки і кібероборони, їх організації та управління ними у сфері оборони з врахуванням кращих практик країн-членів НАТО.

Змістом навчання мають бути навчальні дисципліни або блоки навчальних дисциплін, які охоплюють питання: кібернетика, кіберпростір та його особливості, загрози і ризики у кіберсфері, основи інформаційної, кібербезпеки і кібероборони, технологічні, соціотехнічні, інформаційні та інші аспекти кібербезпеки і кібероборони, особливості організації та стандарти у сфері кібербезпеки і кібероборони у світі та в Україні, управління кібербезпекою у сфері безпеки та оборони.

Розуміння тими, хто навчається, питань виникнення і формування кіберпростору, його структурних компонентів, архітектури та особливостей, дозволить зрозуміти і засвоїти – у чому полягає феномен і парадигма кібербезпеки, закласти основи знань для всього подальшого вивчення питань кібербезпеки. При цьому, особлива увага приділяється основам методології аналізу загроз і ризиків в області інформаційної та кібербезпеки, вивченню типових підходів до оцінки їх забезпечення, в тому числі тих, що засновані на управлінні ризиками. Окремим блоком вивчаються питання функціонування й архітектури глобального Інтернету, мережних інфраструктур держав, а також управління мережами, стандарти мережних та інформаційних технологій, проектування та експлуатації мереж. Методичні основи та практика проведення аналізу загроз, ризиків і уразливостей є базовими для формування навичок розробки стратегії та архітектури кібербезпеки, запобігання, обмеження і нейтралізації відомих і невідомих уразливостей та загроз, управління кібер-

ризиками з метою їх зниження. Огляд уразливостей, характерних для кіберпростору, форм, способів і засобів використання таких уразливостей, вивчення основного спектра різноманітних сценаріїв і технологій кіберрозвідки, кіберзахисту або активного впливу (несанкціонованого проникнення, отримання інформації, зміни алгоритмів діяльності тощо) сформує у тих, хто навчається, вміння оцінювати ризики деструктивних впливів, у тому числі, й пов'язаних з використанням мобільних девайсів (гаджетів).

Важливою складовою підготовки фахівців з питань кібербезпеки і кібероборони є вивчення ними світового і вітчизняного досвіду створення і розвитку систем кібербезпеки та їх складових, вирішення питань забезпечення кібербезпеки на різних етапах її становлення, розподілу сфер відповідальності, задач, функцій, організації взаємодії з питань кібербезпеки і кібероборони між складовими національної безпеки та оборони, міжнародних і національних стандартів у галузі кібербезпеки, особливостей формування національної політики з кібербезпеки, найкращих світових практик у вирішенні зазначених питань та тенденцій їх розвитку, загальної системи та структури міжнародних і національних організацій у сфері кібербезпеки, їх завдання, організаційна структура, повноваження, функції, розподіл повноважень між ними, організація та характер взаємодії з національними організаціями з кібербезпеки, міжнародних та національних правових аспектів забезпечення кібербезпеки та відповідальності за здійснення деструктивних впливів у кіберпросторі та їх наслідки.

Підготовка фахівців за високотехнологічними напрямами, фахівців кібербезпеки та всіх інших військових фахівців з вищенаведених базових питань кібербезпеки відрізняється лише шириною та глибиною їх подання.

Компетентності з питань кібербезпеки, необхідні для виконання завдань за посадами випускниками вищих військових навчальних закладів – фахівцями з кібербезпеки і кібероборони, будуть закладатися при вивченні питань управління кібербезпекою у сфері оборони в рамках варіативних дисциплін. На основі попередньо засвоєних, тими хто навчається, базових питань з кібербезпеки, здійснюється їх підготовка до виконання завдань за посадою командира підрозділу військової частини з кібербезпеки або офіцера з кібербезпеки органу військового управління. Для цього вони ознайомлюються з основним кіберзагрозами у воєнній сфері, відомчими нормативними актами з питань кібербезпеки і кібероборони, змістом, завданнями та складовими частинами кібероборони, силами та засобами кібероборони, формами та способами бойового застосування підрозділів кібервійськ і вимогами до їх спроможностей, досвідом їх підготовки та застосування, у тому числі за прикладами провідних країн світу, методами роботи посадових осіб та методиками планування застосування підрозділів кіберзахисту у мирний час, в особливий період та за воєнного стану, усвідомлюють розподіл повноважень з питань кібербезпеки і кібероборони між суб’єктами забезпечення кібербезпеки і кібероборони, засвоюють особливості підготовки і проведення навчань з

кібероборони, аудиту та оцінки кібербезпеки на рівні окремої військової частини та органу військового управління.

Особливу увагу необхідно приділяти практичній складовій підготовки фахівців кіберзахисту тактичного рівня на розробленому, наближеному до реального, тактичному або оперативному фоні із використанням кіберполігонів та засобів дистанційного проведення кібернавчань. Актуальною є розробка комплексних тактичних задач (комплексних методичних тактичних задач) для практичної підготовки фахівців кіберзахисту. Змістом задач буде вивчення методів роботи посадових осіб (командира підрозділу) військової частини кіберзахисту, організація та бойове застосування підрозділів кіберзахисту. В основу задач доцільно покласти алгоритм планування за стандартами НАТО TLP та MDMP (military decision-making process), а групові вправи поєднувати з практичними заняттями для відпрацювання практичних питань, у тому числі з використанням кіберполігонів.

Подальше нарощування циклу розглянутих питань надасть можливість сформувати зміст навчання для підготовки фахівця з кібербезпеки тактичного рівня з необхідними компетенціями.

На підставі визначених у Стратегічному оборонному бюлетені України [12] пріоритетних напрямів розвитку Збройних Сил України з урахуванням досвіду бойових дій на сході України та кращих світових практик у зв’язку з відсутністю раціональної, чітко структурованої системи підготовки військових кадрів за високотехнологічними напрямами від тактичного до стратегічного рівня стає можливим реалізувати варіант подібний до кращих практик країн-членів НАТО.

Відповідно до світового досвіду основні зусилля на тактичному рівні підготовки фахівців за високотехнологічними напрямами необхідно зосередити на інтеграції наукового, науково-педагогічного та матеріально-технічного потенціалів на єдиній базі, шляхом формування об’єднаного вищого військового начального закладу для комплексного проведення наукових досліджень та підготовки фахівців за високотехнологічними галузями, спеціальностями, спеціалізаціями. А саме: інформаційної та кібербезпеки (кібероборони), технічних видів розвідки, радіоелектронної боротьби, захисту інформації, криптології, космічних систем, автоматизованої обробки розвідувальної інформації, інформаційно-аналітичної роботи, інформаційно-психологічної протидії, автоматизованих систем управління, систем оперативного управління силами та засобами, інформаційно-комунікаційних систем, геоінформаційних систем, експлуатації та бойового застосування робототехнічних (безпілотних, безекіпажних) систем (комплексів) і комплексів боротьби з ними, спеціальної метрології, енергетики, квантово-оптичних систем, впровадження квантових і нанотехнологій та штучного інтелекту у військовій сфері, зброї, побудованої на нетрадиційних і новітніх принципах тощо [13].

Це дозволить: запобігти дублюванню функцій різними структурами; забезпечити раціональне використання фінансів, кадрових та інших ресурсів; підвищити якість підготовки фахівців з високотехнологічних напрямів для всіх

видів Збройних Сил, інших міністерств і відомств Сектору безпеки і оборони держави; суттєво підвищити ефективність здійснення досліджень, розробки, створення, випробування і застосування інноваційних високотехнологічних систем (зразків) ОВТ.

З цією метою та відповідно до досвіду провідних країн світу, такий єдиний, інтегрований дослідницький військовий технологічний заклад вищої освіти у своєму складі повинен мати: освітню складову за високотехнологічними напрямами; потужну систему воєнно-наукових досліджень з науково-організаційною структурою; навчально-наукову, дослідницьку та випробувальну бази (науково-дослідно-випробувальний комплекс високих оборонних технологій) зі стаціонарними та мобільними зразками озброєння і військової техніки, командними пунктами та лабораторіями; експериментально-бойові підрозділи високотехнологічної спрямованості, які відпрацьовують основи та тактику бойового застосування інноваційних високотехнологічних засобів з дослідженням їх бойової ефективності та спроможностей, визначенням перспективних зразків і напрямів їх подальшого розвитку. Раціональна структура системи підготовки військових фахівців та наукових досліджень за високотехнологічними напрямами повинна також бути взаємоповязаною з промисловістю, державними та приватними науково-дослідними закладами (рис. 3.1).

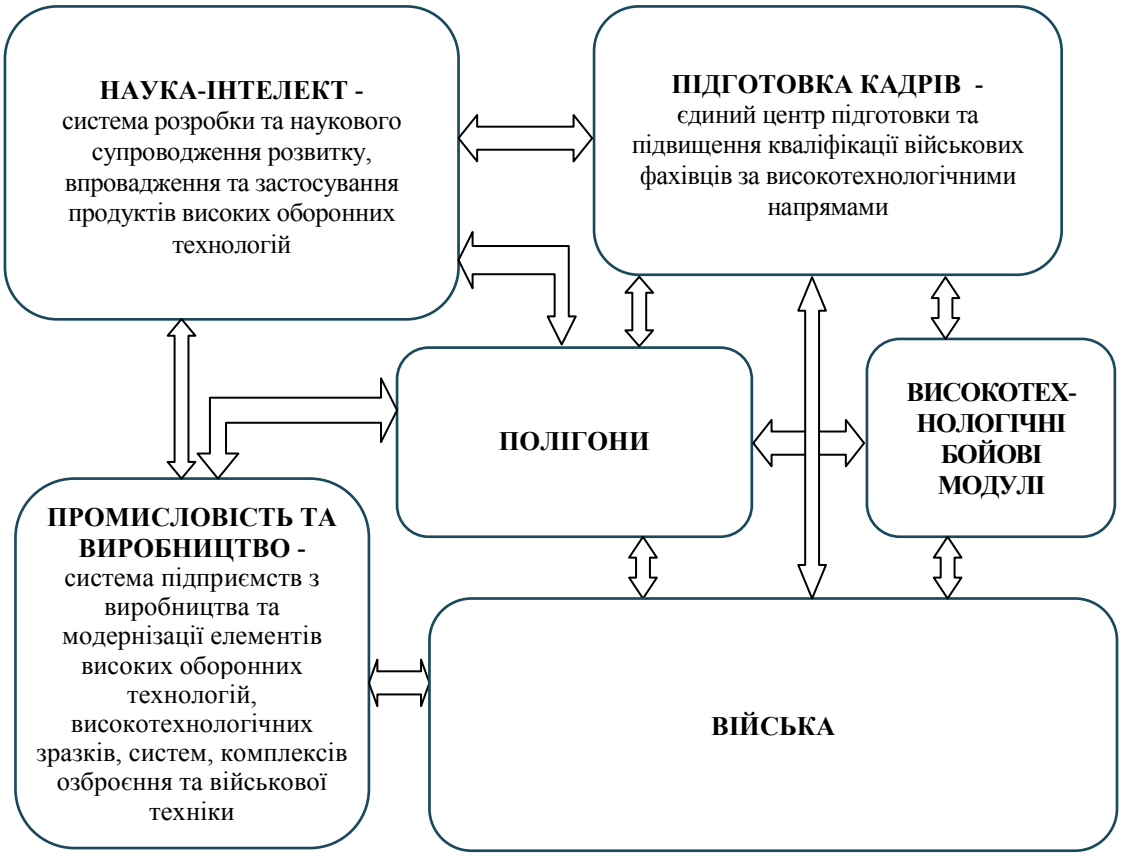

Рис. 3.1. Система підготовки військових фахівців та наукових досліджень за високотехнологічними напрямами

Безумовно, що зазначений дослідницький освітньо-науково-випробувальний заклад у сфері високих оборонних технологій в першу чергу має концентрувати свою діяльність на дослідженні: концепцій, стратегій, проблем і особливостей війн сучасності (4GW, "гібридних війн", проксі-війн тощо) та тих, які прогнозуються, технологій їх ведення, своєчасного виявлення гібридних впливів в усіх сферах і протидії ним, а також подолання їх наслідків; високотехнологічних аспектів превентивної оборони, як виду стратегічних дій у сучасних умовах [14, 15]; проблем виявлення деструктивних інформаційних, психологічних та когнітивних впливів на військовослужбовців і цивільне населення та протидії ним; методів підвищення психофізичної стійкості та психологічної готовності військовослужбовців до виконання бойових завдань в умовах сучасної "гібридної війни" та профілактики формування у них бойового стресу і посттравматичних стресових розладів; проблем забезпечення інформаційної (інформаційно-психологічної), когнітивної та кібер- безпеки держави з урахуванням особливостей гібридних (проксі) війн; проблем формування та розвитку стратегічних комунікацій; проблем розвитку та застосування технічних систем розвідки; проблем розробки і застосування засобів радіоелектронного подавлення та ведення радіоелектронної боротьби; проблем створення та бойового застосування систем оперативного управління силами і засобами та автоматизованих систем управління зброєю, систем типу "С2-С5 Х…Х" (С2, С3, С4ISR тощо); проблем формування, підготовки, високотехнологічного оснащення, забезпечення та застосування сил спеціальних операцій; проблем розвитку та застосування когнітивних технологій в інтересах оборони; проблем розвитку та застосування нано-, піко- та квантових технологій в інтересах оборони; проблем розвитку та застосування штучного інтелекту в інтересах оборони; проблем застосування космічних систем в інтересах оборони; проблем створення захищених робототехнічних систем (комплексів) (безпілотних авіаційних комплексів, робототехнічних комплексів наземного і морського базування) та їх бойового застосування; проблем боротьби з робототехнічними комплексами противника (безпілотними літальними апаратами (дронами), робототехнічними комплексами наземного і морського базування тощо) [16-18]; проблем організації та проведення наукових досліджень та випробувань у сфері високих оборонних технологій і підготовки висококваліфікованих військових фахівців для цієї сфери.

Аналіз стандартів підготовки фахівців тактичного рівня Сектору безпеки і оборони України всіх галузей знань, спеціальностей та спеціалізацій (крім високотехнологічних спеціальностей та спеціалізацій) показує наявність лише компетенції щодо застосування інформаційних технологій за профілем діяльності та повну відсутність компетенцій випускника з питань кібербезпеки і кібероборони. Таким чином, виникає потреба доповнити нормативну частину навчання базовим курсом (дисципліною, блоком у дисципліні) основ кібербезпеки з урахуванням подальшого посадового призначення випускників. Змістом їх навчання мають стати питання кібернетики, кіберпростору та його особливостей, загроз і ризиків у кіберсфері, основ інформаційної, кібербезпеки і кібероборони, технологічних, соціотехнічних, інформаційних та інших

аспектів кібербезпеки і кібероборони, основних заходів кіберзахисту під час виконання обов'язків за посадою.

При здійсненні підготовки оперативного та стратегічного рівнів слід враховувати наступне. Відповідно до світових тенденцій розвитку технологій, ОВТ та воєнного мистецтва, всі офіцери, які отримують освіту оперативного та стратегічного рівнів незалежно від галузей, спеціальностей, спеціалізацій підготовки, повинні набути компетенції та володіти знаннями щодо: стану та тенденцій розвитку високих та інформаційних технологій і їх застосування у сфері оборони; інформаційно-аналітичної діяльності у сфері оборони (яка відіграє визначальну роль в арміях країн-членів НАТО) та імітаційного моделювання; організації застосування автоматизованих систем управління військами (силами) (АСУВ (с)) та систем типу C4ISR; організації та застосування технічних систем моніторингу (розвідки) операційного (бойового) простору в інтересах військ (сил); застосування сучасних геоінформаційних технологій та систем в інтересах військ (сил); скритого управління військами та комплексної протидії технічним розвідкам; основ інформаційної безпеки держави у воєнній сфері та захисту інформації; основ кібербезпека у воєнній сфері та кібероборони; стратегічних комунікацій в сфері оборони.

Фахівці з кібербезпеки та кібероборони, які отримали освіту цих рівнів повинні отримати знання та бути здатними практично здійснювати:

– формування та реалізацію державної політики з питань інформаційної, кібербезпеки та кібероборони;

– формування та реалізацію політики Міністерства оборони України та Збройних Сил України щодо дій у кіберпросторі;

– виконання заходів зі створення та розвитку інформаційних систем та ресурсів у Збройних Силах України;

– координацію дій суб'єктів інформаційної, кібербезпеки та кібероборони Міністерства оборони та Збройних Сил України;

– розробку стандартів підготовки фахівців з інформаційної, кібербезпеки та кібероборони;

– організацію взаємодії та проведення заходів (в т.ч. щодо підготовки держави до кібероборони) зі структурними підрозділами інших центральних органів виконавчої влади та міжнародними партнерами з питань кібербезпеки і кібероборони;

– організацію та підтримувати взаємодію з системою відомчих команд реагування на комп'ютерні інциденти (CERT/CSIRT);

– планування та узгоджене управління діяльністю суб'єктів у кіберпросторі за єдиним замислом і планом, контроль та координацію їх дій;

– моніторинг та аналіз кіберінцидентів, деструктивних інформаційних та когнітивних дій у кіберпросторі та ефективності дій системи кібербезпеки і кібероборони, виявлення уразливостей в інформаційних та кіберсистемах своїх і противника;

– планування, організацію та координацію розвідувальних (Cyber Warfare Intelligence), оборонних (Defensive Cyber Warfare) і наступальних (Offensive Cyber Warfare) операцій в кіберпросторі (Cyberspace Operation) та кібероперацій (Cyber Operation);

– організацію та координацію кібер-, електронних, мережних, інформаційних, когнітивних і психологічних дій у кіберпросторі (включаючи соціальні мережі).

Для підвищення якості підготовки фахівців оперативного рівня, у тому числі фахівців з кібербезпеки, є доцільність інтегрування підготовки у межах окремої спеціальності з подальшим поділом на спеціалізації.

Аналіз професійних стандартів та освітньо-професійних програм всіх спеціальностей та спеціалізацій офіцера оперативного рівня показав наявність компетенції з володіння інформаційними технологіями під час вирішення професійних завдань. При цьому, у компетенціях повністю відсутнє згадування питань кібербезпеки і кібероборони. В сучасних умовах таке нехтування питаннями кібербезпеки і кібероборони не є прийнятним та потребує виправлення. Це викликає необхідність введення базового курсу основ кібербезпеки у військовій сфері для всіх спеціальностей та поглибленого курсу для фахівців ІТ та кібербезпеки.

Для базового курсу основ кібербезпеки у військовій сфері змістом навчання варто передбачити питання національного та відомчого законодавства у сфері кібербезпеки і кібероборони держави, склад сил та засобів кібербезпеки і кібероборони, їх завдання, можливості, форми та способи застосування, основи планування, підготовки та проведення кібероперації Збройних Сил України, організація системи кібербезпеки у військових частинах та органах військового управління.

Для фахівців ІТ та кібербезпеки доцільно запропонувати поглиблений курс кібербезпеки у сфері безпеки й оборони за спеціалізаціями з урахуванням подальшого посадового призначення, а змістом їх навчання мати: вивчення міжнародних та відомчих стандартів у сфері кібербезпеки та кібероборони; зміст, завдання, форми організації кібероборони держави; критична кібер- та інформаційна інфраструктура держави; структура та принципи управління глобальною мережею Інтернет, телекомунікаційними мережами, соціальними мережами; склад сил і засобів кібербезпеки та кібероборони держави, їх завдання, можливості; основи підготовки та ведення кібероборони держави та кібероперацій Збройних Сил України; форми та способи застосування військових частин та підрозділів кібербезпеки під час здійснення кібероборони держави, кібероперації та інших операцій Збройних Сил України та угруповань військ; методи роботи посадових осіб з кібербезпеки органів військового управління, командирів військових частин та установ кібербезпеки під час виконання завдань у мирний час, в особливий період та за воєнного стану.

Проведений аналіз стандартів підготовки фахівців стратегічного рівня підготовки також показав відсутність компетенції випускника з питань кібербезпеки і кібероборони держави, у зв’язку з чим перелік компетенцій випускника повинен бути доповним компетенцією з питань кібербезпеки і кібероборони держави.

Для реалізації зазначеної компетенції слухачі повинні засвоїти зміст дисципліни “Кібербезпека та кібероборона держави”, змістом якої має бути:

− вивчення основ забезпечення кібербезпеки та кібероборони держави;

− склад сил та засобів кібербезпеки та кібероборони Сектору безпеки і оборони України, їх завдання, можливості, форми та способи застосування;

− основи підготовки і ведення кібероборони держави та спеціальних операцій у кіберпросторі;

− методи роботи посадових осіб під час підготовки і ведення кібероборони держави та спеціальних операцій у кіберпросторі;

− аудит та оцінка стану кібербезпеки на державному рівні.

Важливим інструментом підготовки фахівців з кібербезпеки оперативного та стратегічного рівнів є впровадження системи комплексних тактичних та оперативних задач з відпрацювання питань підготовки та бойового застосування військових частин та органів військового управління кіберзахистом та кібероборoною. Ці задачі повинні бути розроблені на загальному оперативному та стратегічному фоні та інтегровані у загальний зміст навчання. Наступним кроком практичної підготовки є впровадження у вищих військових навчальних закладах та органах військового управління системи комплексних командно-штабних та тактико-спеціальних навчань з питань кібербезпеки і кібероборони. Завдяки навчанням складові Сектору безпеки і оборони України будуть мати змогу випробувати в дії своє бачення і розуміння, процедури, системи та методологію кібербезпеки і кібероборони держави. Вони допоможуть підготуватися до сучасних викликів з кібербезпеки, адаптуватись до нових умов ведення “гібридної війни”, а також забезпечити готовність сектору безпеки і оборони України до здійснення кібероборони. Навчання становлять вагомий елемент стримування, адже вони не лише сприяють розвитку потенціалу України з питань кіберзахисту і кібероборони, але й допомагають продемонструвати на що реально здатні об’єднані сили Сектору безпеки і оборони України [19].

Підготовка фахівців ґрунтується на знаннях, отриманих під час здобуття середньої освіти та нарощується під час навчання у військових закладах вищої освіти до рівня, необхідного до виконання завдань за призначенням. Її впровадження дозволить досягти єдності поглядів на застосування складових Сектору безпеки та оборони України та сумісності між ними. Розглянута система підготовки фахівців Сектору безпеки і оборони України дозволяє сформувати та підтримувати актуальність компетентності випускників з питань кібербезпеки і кібероборони для виконання завдань за призначенням протягом усього терміну служби в умовах перенесення бойових дій в інформаційний та кіберпростір.

3.1.3. Сутність, зміст та цілі кібернавчань

Проблеми підготовки фахівців у сфері кібербезпеки актуальні для багатьох країн світу. Першочерговий інтерес викликає досвід у цій галузі США, Російської Федерації (РФ), КНР та країн НАТО.

Напрями, зміст та обсяги підготовки фахівців кібербезпеки у цих країнах визначаються:

− рівнем та напрямами розвитку національних Збройних Сил;

− ступенем їх уразливості у кіберпросторі;

− ступенем розуміння органами державного управління загроз кібербезпеці;

− заходами нормативно-правового та організаційного забезпечення системи кібербезпеки;

− визначеними завданнями кадрового забезпечення розгорнутих і перспективних систем кібербезпеки, а також можливостями систем військової і цивільної освіти кожної із визначених країн.

Найбільш потужна система підготовки військових фахівців кібербезпеки створена у США для кадрового забезпечення Кіберкомандування, деяких інших компонентів ЗС США, у тому числі підрозділів сил спеціальних операцій та операцій бойового забезпечення, а також Агентства національної безпеки (АНБ). Крім США підготовку військових фахівців у сфері кібербезпеки здійснюють країни-члени НАТО. Так, офіцерський склад ЗС країн НАТО має можливість проходити перепідготовку і підвищувати кваліфікацію на різних спеціалізованих курсах у рамках Альянсу, зокрема, на курсах психологічних операцій і в роботі з цивільним населенням для командного складу НАТО при навчальному центрі британської військової розвідки в м. Чиксендзі (Великобританія), курсах НАТО в м. Обераммергау (Німеччина), в Об'єднаному центрі передових технологій з кібероборони НАТО (англ. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) у м. Таллінн (Естонія) тощо.

На окрему увагу заслуговує такий вид підготовки сил кібербезпеки, як проведення навчань та тренувань різного рівня. Показовою у цьому напряму є діяльність, спрямована на злагодження підрозділів кібероперацій збройних сил США та НАТО.

Так, у США заходи оперативної та бойової підготовки ЗС із залученням сил кібербезпеки спрямовані окрім іншого на практичне відпрацювання питань їх переведення з мирного у воєнний стан та організацію дій згідно з планами воєнного часу із врахуванням особливостей їх підпорядкування (сили кібербезпеки входять до складу Кіберкомандувань видів ЗС США і Морської піхоти, які оперативно підпорядковані Кіберкомандуванню). На таких навчаннях, як правило, моделюються різні стани воєнно-стратегічної обстановки і у подальшому командно-штабним методом відпрацьовуються варіанти залучення сил кібероборони на різних фазах воєнних конфліктів. В основу таких заходів покладено вирішення наступних задач:

− перевірка можливості реалізації різних способів боротьби у кіберпросторі в умовах автоматизації управління Збройними Силами та активної протидії зі сторони противника;

− моделювання кібероперацій для вивчення способів впливу на інформації, об’єкти мережної інфраструктури й органи управління противника, оцінки здійснюваних ефектів і наслідків, як для противника, так і для США та їх союзників;

− оцінка бойових можливостей сил кібероборони і перспектив їх інтеграції з можливостями сил і засобів збройної боротьби на суходолі, у морі, повітрі та навколоземному космічному просторі для досягнення синергетичного ефекту при проведенні усього спектра військових операцій.

Аналіз практичних заходів показує, що на даний час головна увага приділяється підвищенню ефективності захисту глобальної інформаційної інфраструктури (GII, Global information infrastructure) при різноманітних сценаріях кібернападів з боку агресорів. Крім того, зусилля спрямовані на інтеграцію кібероперацій у плани проведення інформаційних та повітряно-космічних операцій, а також на оцінку можливостей проведення самостійних заходів для досягнення стратегічних цілей.

Серед усієї множини заходів бойової підготовки, що здійснюються за участі видових сил кібероборони слід відзначити навчання ВПС серії "Кіберлайтнінг", які проводяться для перевірки стану системи забезпечення інформаційної безпеки військових об'єктів. Перші такі навчання пройшли у жовтні 2010 року на АвБ Баклі (штат Колорадо) і були присвячені оцінці реальності оперативних планів захисту комп'ютерних мереж 460-го космічного крила 14-ї повітряної армії Космічного Командування ВПС США від несанкціонованого доступу. В результаті було продемонстровано можливість виведення з ладу критично важливих об'єктів за допомогою кіберзасобів. Основні зусилля були спрямовані на забезпечення безперебійного функціонування сил і засобів даного формування за прямим призначенням в умовах активізації противником дій у кіберпросторі. Замислом навчань передбачалося створення екстремальної обстановки, викликаної виведенням з ладу за допомогою кіберзасобів системи бойового управління крила, призначеної, головним чином, для попередження про ракетно-ядерний удар, забезпечення космічного зв'язку, управління орбітальним угрупованням космічної розвідки і космічних операцій.

Для дезорганізації роботи АвБ Баклі, де розгорнуто станції управління різними космічними системами, проведено комплекс спеціальних підготовчих заходів. Умовний противник, роль якого відігравала 262-га ескадрилья 688-го крила інформаційних операцій у комп'ютерних мережах 24 повітряної армії, застосував метод соціальної інженерії, орієнтований на експлуатацію найбільш уразливого елемента системи безпеки – людини. Протягом двох місяців до початку активної фази навчань було організовано вивчення порядку функціонування системи бойового управління і зв'язку АвБ, а також особисті характеристики обраних для атаки користувачів комп'ютерної мережі.

У період проведення підготовки застосовувалися хакерські прийоми для отримання персональних даних користувачів з метою введення їх в оману. Зокрема, приховано добувалися відомості про об'єкти атаки із соціальних мереж Facebook і Twitter; здійснювався збір парольно-адресної інформації шляхом перехоплення повідомлень з бездротових мереж, які у подальшому застосовувалися для обману користувачів і переконання їх у необхідності переходу на сайти, що містили деструктивне програмне забезпечення. Задіювалася також технологія "фітингу", яка передбачає відправку військовослужбовцям нібито від їхніх друзів поштових повідомлень з "троянськими" програмами із закладеними у них кодами на несанкціоноване вилучення інформації і подальше виведення з ладу комп'ютерів.

Зібрані на підготовчому етапі умовним противником дані дозволили у ході активної фази навчань здійснити несанкціонований доступ до інформаційних баз 460-го космічного крила, які містять таємний перелік цілей, бойових задач і ознак.

Окрема увага приділялася вилученню із віртуальних "сміттєвих корзин" комп'ютерів своєчасно не знищеної конфіденційної інформації. На телефони військовослужбовців 460-го крила надходили дзвінки і повідомлення нібито від бойових товаришів з метою отримання закритої інформації про хід навчать і заходи захисту комп'ютерних мереж від несанкціонованого доступу.

Крім того, протидіюча сторона доклала зусиль для виведення з ладу системи бойового управління і зв'язку АвБ у період надходження навчально-бойових команд від вогневих та взаємодіючих інформаційно-розвідувальних засобів ПРО, а також при відпрацюванні особовим складом АвБ Баклі задач антитерористичної готовності. Для цього, зокрема, умисно здійснювалася спроба входу у комп'ютерні мережі без цифрового підпису для того, щоб аварійно спрацювала автоматика і заблокувала роботу системи бойового управління у відповідності з регламентом стандартних процедур забезпечення інформаційної безпеки. Розблокування мереж вимагало до 24 годин, що виявилося критичним фактором у період надходження навчально-бойових команд і перевірки антитерористичної готовності.

У такій оперативній обстановці особовий склад, задіяний у навчаннях "Кіберлайтнінг", виконував задачі із виконання заходів підвищеної інформаційної безпеки шляхом введення різних ступенів готовності до захисту інформаційної інфраструктури, обмеженню інформаційного обміну, встановленню спеціальних процедур (на період зростання кіберзагроз) надання доступу у службові мережі. Поряд з цим, відпрацьовувалися варіанти розгортання резервних мереж бойового управління для забезпечення неперервного функціонування 460-го космічного крила за прямим призначенням, а також вживалися заходи екстреного реагування і ліквідації наслідків кібератаки.

Підсумки навчань дозволили Командуванню ВПС США оцінити реальний стан справ у сфері інформаційної безпеки на критично важливих об'єктах і уточнити програми підвищення кваліфікації військовослужбовців у даній області у рамках професійно-посадової підготовки. Одним із основних висновків стало визнання необхідності включення подібного роду заходів у плани бойової підготовки усіх видових з'єднань і частин, які оперативно підпорядковані Кіберкомандуванню.

Яскравим прикладом проведення комплексних навчань є навчання НАТО з кібербезпеки "Cyber Coalition", які проводяться кожен рік, починаючи з 2008 року. Навчання "Cyber Coalition – 2019" проводились в Об'єднаному центрі передових технологій з кібероборони НАТО (NATO CCD COE) з 2-6 грудня 2019 року [20]. До навчання було залучено 900 учасників, які виконували завдання згідно зі сценарієм й віддалено і представляли 28 країн-членів НАТО та 8 країн-партнерів Альянсу: Японію, Україну, Грузію, Швейцарію, Фінляндію, Ірландію, Швецію та Європейський Союз в особі Військового

штабу Європейського Союзу (European Union Military Staff (EUMS) та Комп'ютерної групи реагування на надзвичайні ситуації (Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU). Україна вперше брала участь у таких навчаннях [21].

На навчаннях відпрацьовуються питання: взаємної міжнародної та міжвідомчої сумісності між силами і засобами кіберзахисту різних країн, захист інформаційно-телекомунікаційних систем, протидія впливу на об'єкти критичної інформаційної інфраструктури країн-членів НАТО, захист різних видів високотехнологічного озброєння та військової техніки. З кожним роком мета навчань та перелік питань, що відпрацьовуються під час навчань, набувають нового більш широкого змісту.

В ході навчання "Cyber Coalition-2019" особлива увага була надана удосконаленню координації і співпраці між НАТО і членами Альянсу, посиленню здатності захищати кіберпростір Альянсу і проведенню операцій в кіберпросторі. А також були перевірені процедури НАТО та окремих країн щодо обміну інформацією, ознайомлення з обстановкою в кіберпросторі і прийняття рішень.

Участь представників Збройних Сил України у навчанні як держави-учасниці є важливим аспектом, спрямованим на досягнення взаємосумісності в процесах реагування на порушення кібербезпеки та прийняття рішень щодо забезпечення кібероборони з державами НАТО, що передбачено ціллю партнерства G7300 "Кібероборона" [21].

Інший приклад це навчання "Locked Shields" (Зімкнуті Щити), які також проводяться в Об'єднаному центрі передових технологій з кібероборони НАТО. У кібернавчаннях Locked Shields 2019 брали участь понад 1000 міжнародних експертів з кібербезпеки. Навчання проходять "в лабораторному середовищі" і вважаються одними з найбільших навчань з кібербезпеки у світі. Використовується ігровий підхід, що дозволяє учасникам виступати в ролі вигаданих груп реагування. Їх мета – оцінити ситуацію, зберегти доступність послуг і захистити мережі, які стали жертвами кібератак [22].

Загальна структура проведення навчань з кібербезпеки відрізняється від класичного підходу до проведення звичайних військових навчань, який, як правило, передбачає участь лише двох протидіючих сторін ("синьої" та "червоної" команд), наявністю додаткового елементу – кібернетичної інфраструктури, що використовується кожною зі сторін для досягнення переваги над умовним противником (рис. 3.2).

До складу кібернетичної інфраструктури ("біла" команда) входять ресурси та користувачі (рис. 3.2), що не належать жодній із протидіючих сторін, але можуть впливати на їх дії у кіберпросторі. Як правило, це звичайні користувачі, які використовують електронну пошту, завантажують файли, відвідують веб-сайти тощо. Відповідно обладнання та програмні засоби, які обслуговують потреби таких користувачів, також відноситься до складу "білої" команди. До участі у навчаннях можуть залучатися також треті сторони ("сіра" команда), яка здійснює оцінку дій учасників навчань та змінює бойову обстановку.

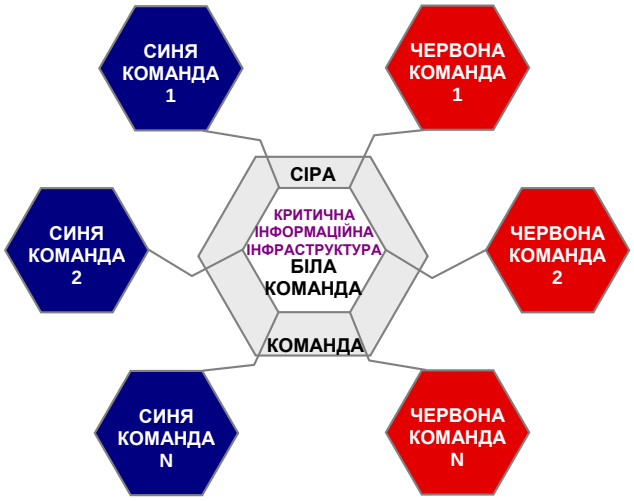

Рис. 3.2. Організаційна структура проведення навчань з кібербезпеки

Важливим елементом підготовки та злагодження сил кібербезпеки є проведення навчань, тренувань та змагань різного рівня (від міжнародних до міжвузівських).

Меншими за обсягом залучених сил та засобів, але не менш вагомими є навчання під приводом Агенції національної безпеки (АНБ) США CDX (Cyber Defense Exercise), які проходять з метою підвищити навички молодого покоління "кібервоїнів" курсантів військових академій США та Канади. Перевіряється здатність будувати, забезпечувати безпеку та захищати мережі від кібератак тощо. Так, CDX-2017 проходили серед військових та силових структур США – Військову академію США, Академію Повітряних Сил США, Академію берегової охорони США, Королівський військовий коледж Канади та інші структури, які виступали на стороні захисників – команди Blue Team. Їм протистояли Red Team, команди "хакерів", що здійснювали свої атаки 24 години на добу. За "червоних" грали фахівці АНБ. Перемогу отримала команда Військово-Морської Академії США. Подібні навчання є найбільш доцільним та раціональним способом отримання практичного досвіду застосування сил та засобів кібербезпеки і кібероборони.

Також існує ціла низка навчань з кібербезпеки, які тривалий час проводиться у рамках НАТО: Red Flag, Cyber Shield, Quantum Dawn, Cyber Storm, Cyber Guard, Cyber Europe.

Достатньо розгалужені системи підготовки військових фахівців з кібербезпеки створені також у Росії та Китаї. В інших країнах мають місце окремі елементи такої підготовки.

Поширення кіберзагроз на усіх рівнях суспільної діяльності змушує навчати широкі верстви населення основам захисту від таких загроз. Зокрема, показовим є введення до шкільної програми багатьох країн відповідних навчальних предметів.

Отже, важливим елементом підготовки повинна бути постійно діюча система курсової підготовки. Вона виконує функції підтримуючої та тренувальної системи між рівнями підготовки. Її повноцінне функціонування

потребує постійного зібрання, аналізу, систематизації та впровадження в зміст курсів з питань кібербезпеки всіх основних досягнень й інновацій в цій сфері, створення баз даних та сайта, з якого можливо отримати доступ до спеціалізованих курсів, постійного моніторингу контенту з питань кібербезпеки, виявлення нових загроз і ризиків та реакції на них у вигляді спеціально розроблених курсів. Важливе місце під час реалізації курсової підготовки займає дистанційне навчання.

3.1.4. Кіберполігон: призначення, склад та структура

Проблематика розробки та впровадження лабораторних середовищ для відпрацювання дій в кіберпросторі здебільшого розвивається у створенні таких типів кіберполиігонів: університетського (типу кіберполігону KYPO Масарикового університету м. Брно, Чехія); частки цивільного (на прикладі рішень компанії Forward Defense, м. Абу-Дабі, ОАЕ); національного військового (кіберполігон National Cyber Range, м. Орландо, шт. Флоріда, США); міжнаціонального (кіберполігон НАТО, м. Таллінн, Естонія). Програмно-апаратні засоби вказаних кіберполігонів не мають своєю метою та функціонально і технічно не забезпечують проведення комплексних досліджень інформаційного впливу на технічну й ергатичну складову систем управління різного рівня та призначення. При цьому, втрачається можливість дослідження синергетичного ефекту взаємного посилення інформаційно-психологічних і кібервпливів, які реалізуються та розвиваються в кіберпросторі. Традиційні підходи обмежуються здебільшого дослідницькими функціями вивчення загроз суто кібернапряму без урахування реального досвіду сучасних гібридних впливів, що знижує адекватність отримуваних результатів.

Розробка та створення кіберполігона для дослідження і багатостороннього відпрацювання заходів протидії гібридним впливам в кіберпросторі реалізується загальнонауковими методами теорії системного аналізу.

Практика доводить, що сучасні методи та способи реалізації гібридних впливів супроводжуються значним потоком динамічно змінюваних кризових ситуацій. Їм властива апріорна невизначеність за метою, суб'єкта та об'єкта впливу, змісту, суті і способу реалізації. Технологічно побудова відомих систем протидії таким кризовим ситуаціям, форми і способи їх застосування орієнтовані на формування статичної надмірної структури системи. Розподіл завдань між усіма складовими системи здійснюється рівномірно з вибірковістю елементів лише за їх призначенням. Збільшення кількості та щільності потоку кризових ситуацій (КС), кіберінцидентів та їх типів відпрацьовується збільшенням елементів структури. Це породжує інформаційну надмірність даних та ускладнення їх передачі й обробки. На таких самих принципах побудовані програмні засоби реалізації процесів оперативного виявлення, захисту та активної протидії інформаційним загрозам у кіберпросторі. Такі підходи не є дієвими в реальних умовах обстановки, під час застосування противником переважаючих або рівних за складом та рівнем розвитку засобів інформаційного впливу і здійснення масованих інформаційних та кібератак, які

супроводжуються іншими несиловими і силовими методами досягнення мети конфлікту. Саме це є характерним для гібридних воєн сьогодення.

Дієві результати реалізації завдань аналізу та синтезу складних систем, автоматизованого збору, обробки й аналізу інформації в умовах апріорної невизначеності та щільності потоку деструктивних впливів і значної динаміки КС забезпечує застосування синергетичних методів. Зокрема, методів ситуаційного управління, фрактального аналізу, самоорганізації, біфуркаційних моделей тощо. Впровадження принципів ситуативного управління надає можливості раціонального розподілу і перерозподілу власних ресурсів і концентрації зусиль на критичних для забезпечення безпеки напрямах дій супротивника. Методи фрактального аналізу, самоорганізації і біфуркаційні моделі дозволяють своєчасно виявити загрози та кризові ситуації, передбачити напрям їх розвитку і реальну спрямованість. На практиці це забезпечує підвищення ефективності заходів протидії інформаційним впливам завдяки випередженню противника у своєчасності, повноті та достовірності інформації, за часом реагування та у діях.

Таким чином, має місце актуальна проблема розробки методологічного забезпечення автоматизованого моніторингу, аналітичної обробки інформації, прогнозування, планування та здійснення заходів пасивної й активної протидій інформаційним загрозам в кіберпросторі в умовах апріорної невизначеності і щільності потоку деструктивних впливів і значної динаміки кризових ситуацій шляхом впровадження методів ситуаційного управління, фрактального аналізу, самоорганізації і біфуркаційних моделей. Її вирішення та підвищення ефективності комплексу заходів забезпечення інформаційної та кібербезпеки в кіберпросторі з відпрацюванням заходів протидії гібридним впливам в цілому вимагає наявності відповідних кіберполігонов.

Створення діючого кіберполігона для відпрацювання інноваційних засобів забезпечення інформаційної та кібербезпеки в кіберпросторі в умовах гібридних конфліктів різної інтенсивності і змісту, з відпрацюванням заходів протидії гібридним впливам забезпечується рішенням комплексу завдань:

1. Удосконалення науково-прикладних та технологічних принципів побудови і реалізації програмно-апаратних засобів моніторингу кіберпростору, захисту та впливу, їх практична апробація.

2. Розробка фундаментальних та прикладних принципів побудови математичного забезпечення програмно-апаратних засобів реалізації процесів моніторингу, аналітичної обробки інформації, прогнозування, планування та здійснення заходів пасивної й активної протидії інформаційним і кіберзагрозам у кіберпросторі.

3. Розробка та практична апробація у середовищі кіберполігона програмних засобів реалізації процесів моніторингу, аналітичної обробки інформації, прогнозування, планування і здійснення заходів пасивної й активної протидії інформаційним і кіберзагрозам у кіберпросторі.

4. Розвиток новітніх форм, способів та методів протидії викликам і загрозам тероризму, захисту критичних інфраструктур, суб’єктів та об’єктів органів управління Сектору безпеки і оборони держави, суспільства й особи за

допомогою реалізації комплексу заходів інформаційної безпеки в кіберпросторі в умовах гібридних конфліктів різної інтенсивності.

Розвиток науково-дослідної та учбово-лабораторної баз у сфері інформаційної та кібербезпеки, проведенні з її використанням багатосторонніх національних та міжнародних навчань, удосконалення системи підготовки, перепідготовки та підвищення кваліфікації військових фахівців у галузі інформаційної та кібербезпеки з впровадженням комплексних підходів і стандартів НАТО:

1. Розробка методичних основ для класифікації, стандартизації та сертифікації кіберполігонів і створення системи класифікації і стандартів кіберполігонів.

2. Формування основ для створення потужних регіональних кіберцентрів та залучення цих структур до цілодобового оперативного чергування у системі національної і загальноєвропейської інформаційної і кібербезпеки з використанням сил і засобів кіберполігона, відпрацьованих на ньому теоретичних та прикладних принципів побудови програмно-технічних засобів, форм і способів протидії гібридним впливам у кіберпросторі.

Це базується на здійсненні комплексу наукових досліджень фундаментального і прикладного характеру, реалізації інженерних завдань і організаційно-технічних заходів, суть і зміст яких передбачає наступне.

Завдання. Удосконалення науково-прикладних та технологічних принципів побудови і реалізації програмно-апаратних засобів моніторингу в кіберпросторі, захисту та впливу шляхом створення спеціалізованого комплексного кіберполігона.

Кіберполігон – це сукупність програмно-апаратних засобів, об'єднаних єдиною розподіленою локальною мережею з виходом в Інтернет, що призначена для відпрацювання прикладних питань розробки, проектування та проведення випробувань програмно-технічних систем (комплексів) забезпечення інформаційної (інформаційно-психологічної) та кібербезпеки в ході реалізації функцій моніторингу, захисту, пасивного та активного впливів, проведення багатосторонніх навчань, забезпечення узагальнення досвіду, розвитку форм, способів та методів прогнозування, запобігання, виявлення і протидії кризовим ситуаціям у кіберпросторі, здійснення заходів практичної підготовки, перепідготовки та підвищення кваліфікації військових (цивільних) фахівців (за національними та стандартами НАТО), а також для лабораторно-експериментальної підтримки проведення фундаментальних та прикладних наукових досліджень у галузі інформаційної і кібербезпеки держави.

Спеціалізований комплексний кіберполігон створюється за ідеологією відкритих, розподілених, складних, ергатичних інформаційно-управляючих систем, інваріантних за своєю структурою та рівнем завдань. У його структурі та архітектурі передбачено впровадження технологій захищених комп'ютерних мереж зі стаціонарним та мобільним комплектами обладнання зі взаємозамінними, стандартизованими в межах цільових завдань модулями. В якості функціональної основи передбачено використання циклів управління: Observation/спостереження (збір інформації від внутрішніх та зовнішніх джерел); Orientation/орієнтування (формування декількох можливих планів дій

з оцінкою кожного з них за векторами критеріїв); Decision/рішення (вибір найкращого плану дій для практичної реалізації); Action/дії (практична реалізація вибраного плану дій). Це забезпечить впровадження моделі незалежного ситуативного управління з відпрацюванням у масштабі часу, близькому до реального, потоку кризових ситуацій.

Розробка та виготовлення діючих кіберполігонів здійснюється з базових дискретних компонентах (рис. 3.3, 3.4).

До складу базової окремої компоненти кіберполігона входять два ідентичні за призначенням, складом, функціональними можливостями комплекту спеціалізованих програмно-апаратних комплексів:

− комплект сил кібероборони;

− комплект сил тестування на кіберзахищеність.

Комплект сил кібероборони призначений для забезпечення кібербезпеки сервісів та служб дата-центру кіберполігона, а також захисту його операторів від технологій інформаційного впливу через кіберпростір.

Комплект сил тестування на кіберзахищеність призначений для тестування сервісів та служб дата-центру кіберполігона, а також дослідження стійкості його операторів до технологій інформаційного впливу через кіберпростір.

До складу кіберполігона доданий об’єкт тестування, який являє собою потужний дата-центр, сервіси та служби якого, з одного боку, захищаються силами та засобами сил кібероборони, з іншого, – тестуються на кіберзахищеність силами та засобами другого комплекту.

Окремі компоненти, загальні для двох комплектів, які входять до кіберполігона, це:

− кластер планування, організації й управління роботи кіберполігона;

− кластер міжнародного співробітництва;

− підсистема забезпечення функціонування сервісів та служб дата-центру;

− моделювання заходів та засобів кіберзахисту дротових і безпровідних мереж дата-центру;

− моделювання заходів і засобів кіберзахисту системи управління, мережної (фізичної і логічної) топології, програмно-апаратного забезпечення сервісів та служб дата-центру;

− моделювання технологій інформаційного захисту операторів дата-центру через кіберпростір;

− моделювання технологій криптографічного захисту;

− моделювання заходів, засобів і технологій захисту від інформаційних і кібервпливів критичних елементів;

− моделювання та імітації дій в кіберпросторі, проведення навчань (тренувань) з кібербезпеки та кібероборони;

− моделювання кібератак на криптосистеми дата-центру;

− моделювання соціотехнічних кібератак через кіберпростір на операторів дата-центра, суб’єкти та об’єкти органів управління Сектору безпеки і оборони держави, суспільство й особистості в умовах гібридних конфліктів різної інтенсивності;

− тестування сервісів та служб дата-центру на кіберзахищеність.

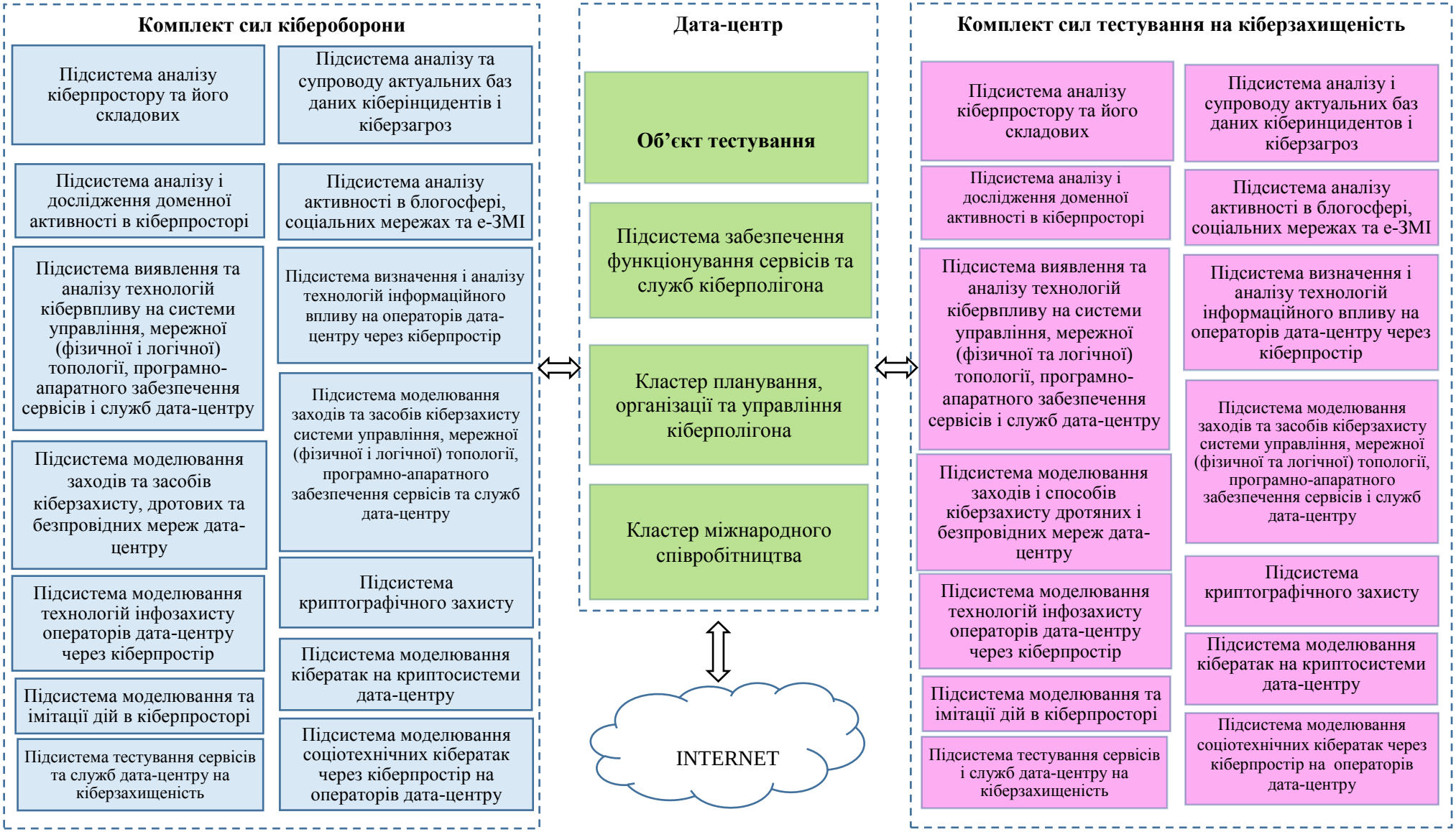

Рис. 3.3. Структурна схема кіберполігона

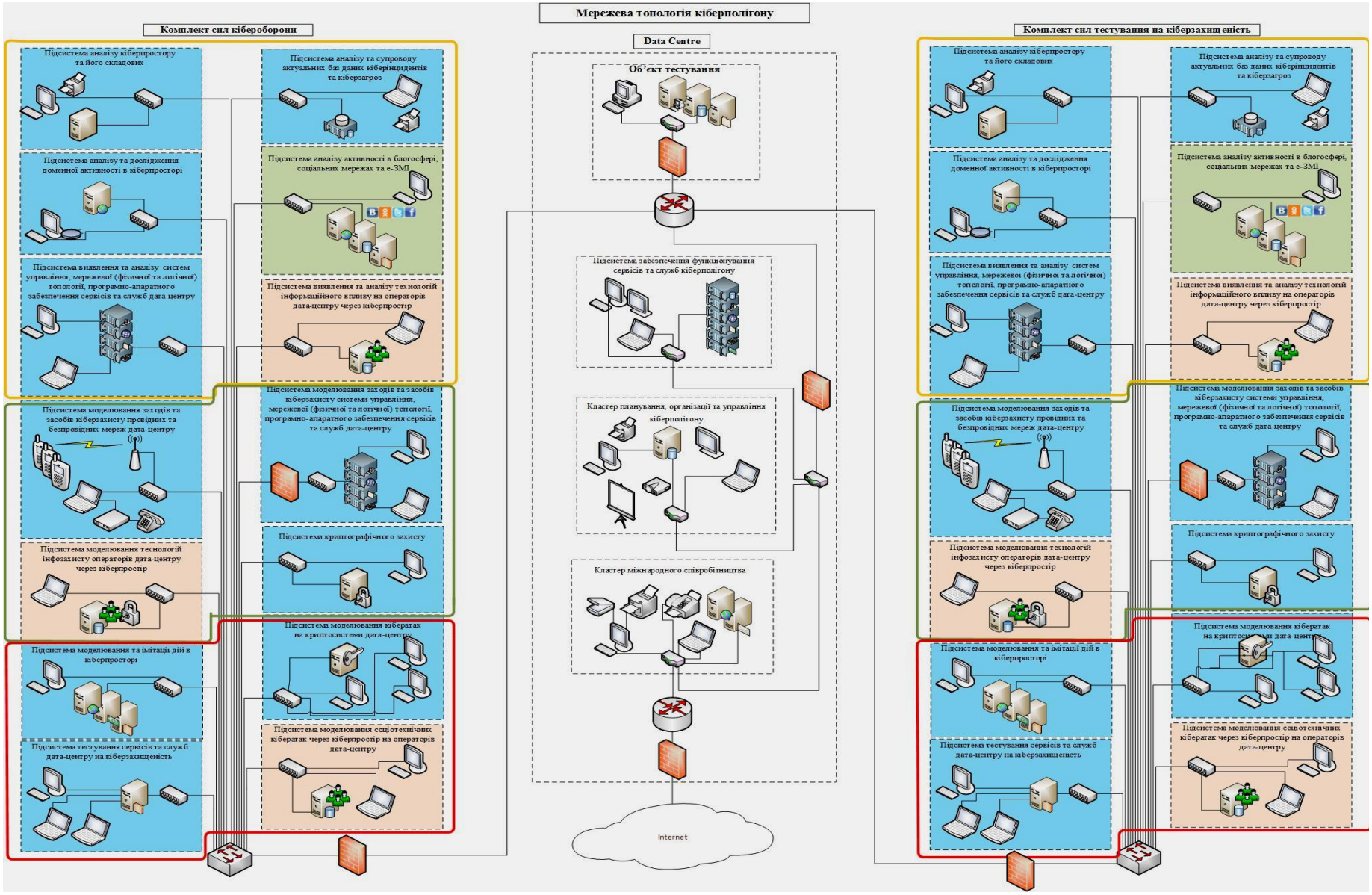

Рис.3.4. Мережна топологія кіберполігона

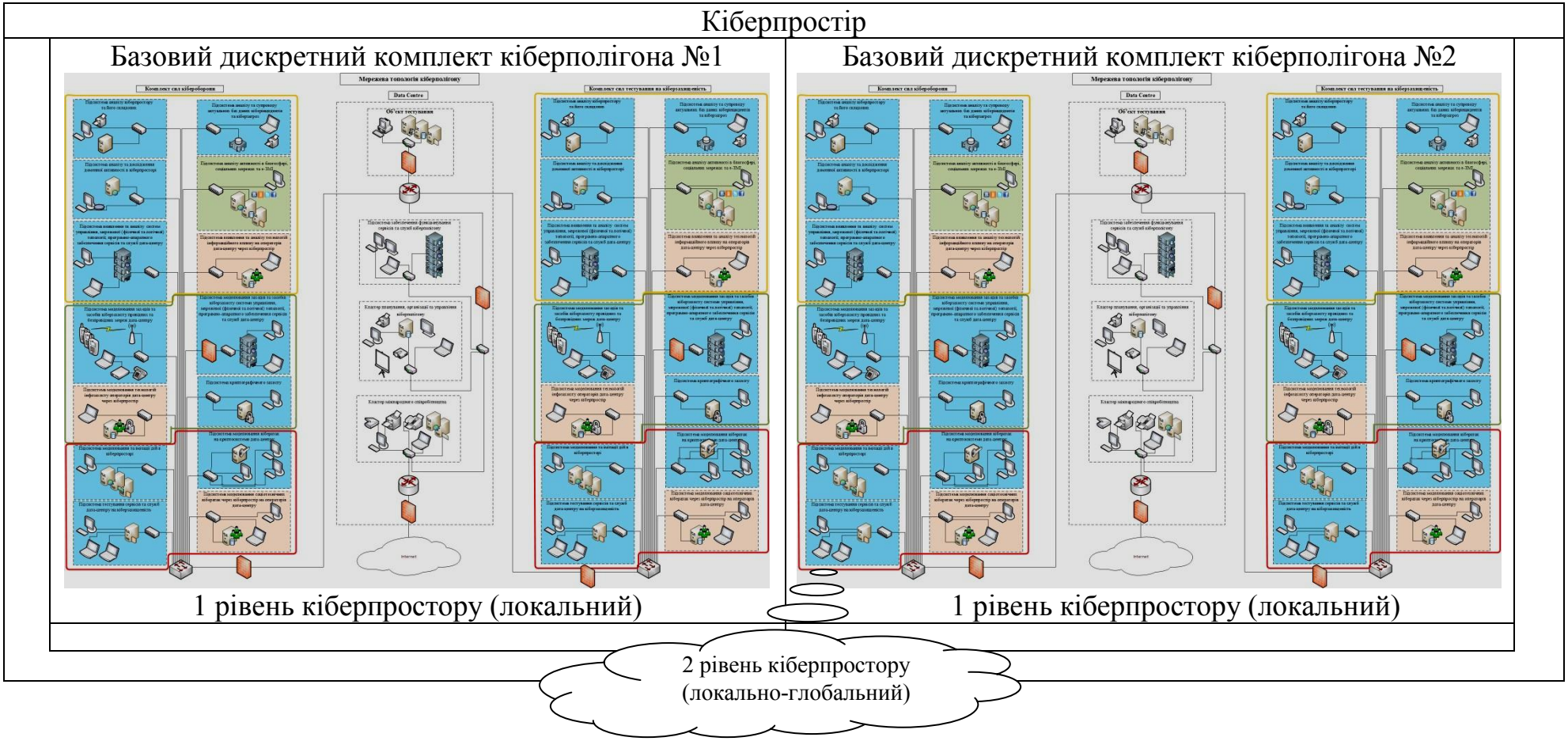

Рис.3.5. Структурна схема повнофункціонального кіберполігона

Схема мережної топології кіберполігона показана на рис. 3.4. В її основу покладені комплекти, об'єкти, компоненти, кластери і підсистеми кіберполігона, визначені структурною схемою рис. 3.3.

Повнофункціональна схема кіберполігона включає два базові дискретні компоненти. Розробка кожного компонента може здійснюватися окремо, ізольовано або за загальними підходами з обміном результатів проектування. Об'єднання двох дискретних компонент структур рис. 3.3 з архітектурою рис. 3.4 здійснюється шляхом їх інформаційного об'єднання в єдине кіберсередовище, яке створене функціонально об'єднаними: внутрішнім (локальним), комбінованим (локально-глобальним) і зовнішнім (глобальним) кіберпростором (рис. 3.5). З технологічної точки зору таке функціонально-інформаційне об'єднання здійснюється на протокольних рівнях відповідного типу.

Запропонована структура повнофункціонального комплексного кіберполігона поступово, на трьох локально-глобальних рівнях кіберпростора, з нарощуванням можливостей забезпечує відпрацювання форм, способів, методів, алгоритмів, методик та технологій виявлення кібератак, заходів пасивної й активної протидії ним, ліквідації наслідків застосування кіберзброї та відновлення нормальних режимів функціонування мереж управління військами та зброєю, а також реалізацію комплексу заходів моніторингу і виявлення загроз, їх аналізу, прогнозування, планування здійснення активних та пасивних дій з протидії інформаційно-психологічним впливам у кіберпросторі та аналіз ефективності проведених заходів.

Програмно-апаратні ресурси підсистеми тестування на кіберзахищеність повинні забезпечувати можливість проведення кібервпливів різного типу, використовуючи відповідні мережні протоколи, уразливості системного та прикладного програмного забезпечення, недосконалості антивірусного програмного забезпечення. Наприклад: сканування портів, відмова в обслуговуванні, прослуховування та перехоплення потоку інформації в каналах мережі, псевдосанкціоноване проникнення в підсистему захисту, знищення, спотворення, крадіжка інформації, блокування доступу до неї в підсистемі кібероборони за допомогою засобів спеціального програмного впливу тощо. Технічні пристрої і спеціалізоване програмне забезпечення повинні гарантувати надійний захист системних ресурсів та інформації, яка циркулює і зберігається на комп'ютерах в локальній мережі підсистеми кібероборони.

У рамках проекту фахівці з інформаційної безпеки (кожен окремо або у складі певних команд) зможуть відпрацьовувати спеціальні прийоми кібернападу та захисту від нього, не завдаючи реальної шкоди існуючій електронній інфраструктурі держави.

Структура повнофункціонального комплексного кіберполігона забезпечує одночасно автономне, багатостороннє та багаторівневе виконання цільових завдань відповідно до реальних умов.

Розробка і створення кіберполігонів вимагає рішення таких часткових завдань:

− удосконалення науково-прикладних і технологічних принципів побудови та реалізації програмно-апаратних засобів моніторингу кіберпростору, захисту і

впливів для створення кіберполігона;

− розробка структури та детальної архітектури кіберполігона відповідно до відомих науково-прикладних і технологічних принципів його побудови;

− створення дискретних компонент кіберполігона з двох базових його комплектів за схемою та архітектурою (рис. 3.3 та 3.4), забезпечення функціонування (налаштування, тестування) першого (локального) рівня кіберпростору відповідно до категорій декомпозиційного розподілу (рис. 3.5);

− створення повнофункціонального комплексного кіберполігона шляхом інформаційного об'єднання створених дискретних компонентів в єдине інформаційне середовище, які функціонують і породжують внутрішню комбіновану (локально-глобальну) і зовнішню складову кіберпростору;

− розробка програми і методики випробувань комплексного кіберполігона з повнофункціональною структурою та архітектурою;

− проведення випробувань створеного кіберполігона, оцінювання результатів випробувань, коригування його структури і функціонала, затвердження результатів випробувань.

Для ефективного виконання комплексу заходів забезпечення інформаційної і кібербезпеки в кіберпросторі з відпрацюванням заходів протидії гібридним впливам передбачається здійснити розробку методологічного забезпечення реалізації процесів моніторингу, аналітичної обробки інформації, прогнозування, планування і здійснення заходів пасивної та активної протидії інформаційним і кіберзагрозам у кіберпросторі. Умови апріорної невизначеності, щільність потоку деструктивних впливів та значної динаміки кризових ситуацій враховується впровадженням методів ситуаційного управління, фрактального аналізу, самоорганізації та біфуркаційних моделей. Передбачається введення принципів ситуативного управління програмно-апаратним середовищем кіберполігона, на якому виконується комплекс заходів та процесів забезпечення інформаційної безпеки в кіберпросторі. Ці процеси розглядаються як динамічні і циклічні, такі, що реалізовуються під конкретну кризову ситуацію на обраному переліку необхідних і достатніх елементів з доступних та наявних складових кіберполігона. Для цього створюється і послідовно паралельно виконує завдання об'єднаних функціонально та інформаційно пов'язаних віртуальних підсистем – інформаційно-управляючих кластерів (ІУК). Такі ІУК ситуативно синтезуються для виявлення, локалізації і ліквідації конкретної кризової ситуації. Відмічене реалізується у формі ситуативного структурно-параметричного синтезу складної розподіленої інформаційно-управляючої системи. Фактично реалізується процес ситуативного управління структурою і параметрами кіберполігона. Така процедура забезпечує просторово-часове, структурне і функціональне рознесення завдань відпрацювання щільного потоку деструктивних впливів при значній динаміці кризових ситуацій. При цьому, знижується розмірність приватних завдань обробки інформації і навантаження на канали передачі даних. В якості практичного результату маємо: ефективне реагування на щільний потік динамічно-змінюваних деструктивних впливів при значній динаміці кризових ситуацій з властивостями апріорної невизначеності суб'єктів

та об’єктів впливу, змісту, суті та способу реалізації; виконання цільових завдань у масштабі часу, близькому до реального, і з високими показниками достовірності і повноти вихідної інформації.

Ефективне виконання завдань забезпечення інформаційної безпеки залежить від постійного проведення фундаментальних та прикладних наукових досліджень, в ході яких отримують концепцію ситуаційного управління структурою та параметрами програмно-апаратного середовища кіберполігона для ефективної реалізації комплексу заходів і процесів забезпечення інформаційної безпеки в кіберпросторі в умовах значної щільності потоку динамічно-змінюваних деструктивних впливів при високій динаміці кризових ситуацій з властивостями апріорної невизначеності.

На кожному інформаційно-управляючому кластері здійснюється комплекс процесів, які реалізуються на основі:

− методики кластерного пошуку і систематизації інформації про інформаційні загрози в кіберпросторі;

− методики виявлення та ідентифікації кризових ситуацій в умовах щільного їх потоку і динаміки змін з впровадженням принципів самоорганізації;

− методики автоматизованого оперативного і поглибленого інтегрального аналізу інформації моніторингу;

− методик прогнозування розвитку кризових ситуацій і загроз в інформаційній сфері з використанням біфуркаційних моделей;

− методологічних підходів до планування заходів протидії інформаційним загрозам в кіберпросторі та оцінювання їх ефективності;

− методологічних підходів фрактальної побудови програмно-апаратних комплексів автоматизованого пасивного і активного інформаційного (інформаційно-психологічного) та кіберзахисту.

Розробку фундаментальних та прикладних принципів побудови математичного забезпечення програмно-апаратних засобів реалізації процесів моніторингу, аналітичної обробки інформації, планування і здійснення заходів пасивної і активної протидії інформаційним загрозам в кіберпросторі.

В ході виконання цього завдання передбачається отримати наукові основи для розробки програмних засобів реалізації процесів моніторингу, аналітичної обробки інформації, планування і здійснення заходів пасивної і активної протидії інформаційним загрозам у кіберпросторі.

Розробка і практична апробація у середовищі кіберполігона програмних засобів реалізації процесів моніторингу, аналітичної обробки інформації, прогнозування, планування і здійснення заходів пасивної і активної протидії інформаційним загрозам у кіберпросторі.

Суть виконання цього завдання полягає в розробці програмно-апаратних комплексів, набору програмних додатків, розрахункових програм, моделей тощо, заснованих на розроблених фундаментальних і прикладних принципах побудови математичного забезпечення програмно-апаратних засобів реалізації процесів моніторингу, аналітичної обробки інформації, планування і здійснення заходів пасивної і активної протидії інформаційним загрозам в кіберпросторі

для ефективної протидії гібридним впливам, які забезпечують виконання завдань:

− ситуативного управління структурою і параметрами програмно-апаратного середовища кіберполігона;

− кластерного пошуку і систематизації інформації про інформаційні загрози в кіберпросторі;

− виявлення та ідентифікація кризових ситуацій в умовах щільного потоку деструктивних впливів і значної динаміки зміни кризових ситуацій з впровадженням принципів самоорганізації;

− автоматизованого оперативного і поглибленого інтегрального аналізу інформації моніторингу;

− прогнозування розвитку кризових ситуацій і загроз в інформаційній сфері з використанням біфуркаційних моделей;

− планування заходів протидії інформаційним загрозам в кіберпросторі і оцінювання їх ефективності;

− кібервпливу та захисту від несанкціонованого доступу до інформаційно-телекомунікаційних систем;

− формування лабораторного середовища для проведення спецдосліджень у галузі технічних і програмних засобів кіберзахисту;

− визначення оптимального способу нейтралізації загроз в кіберпросторі з урахуванням наявних апаратно-програмних засобів технічного захисту інформації;

− моделювання процесів нападу і захисту інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури;

− оцінювання рівня захищеності електронних ресурсів і апаратно-програмних засобів інформаційно-телекомунікаційних систем;

− аналізу ефективності кібервпливу на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури протидіючої сторони.

Створення програмного забезпечення з вказаними функціями передбачається з використанням технологій побудови інтелектуальних експертних систем, систем підтримки прийняття рішень, геоінформаційних систем на сучасних мовах, технологіях та у середовищах програмування високого рівня.

Розроблені програмно-апаратні засоби є невід’ємною складовою кіберполігона.

Результати цього завдання:

1) комплект програмно-апаратних комплексів, набір програмних додатків, моделей тощо, які реалізують вищеперелічені функції з програмною документацією до них;

2) програми і методики випробувань розроблених комплектів програмно-апаратних комплексів, набір програмних додатків, моделей тощо, для застосування на різних рівнях кіберпростору (відповідно до категорій рис. 3.5);

3) результати випробувань розроблених комплектів програмно-апаратних комплексів, набору програмних додатків, моделей тощо, на першому і другому рівнях кіберпростору (відповідно до категорій рис. 3.5).

Розвиток новітніх форм, способів і методів протидії викликам і загрозам тероризму, захист критичних інфраструктур, суспільства, керівництва держави та його сектору безпеки, особистості за допомогою реалізації комплексу заходів інформаційної безпеки в кіберпросторі, спрямованих на протидію гібридним впливам.

Суть цього завдання полягає в реалізації конкретних практичних завдань на програмно-апаратних засобах кіберполігона. При цьому використовується метод напівнатурного моделювання із застосуванням принципів і прийомів теорії ігор, реалізацією антагоністичного конфлікту між умовно протиборчими сторонами, які діють на своїх базових дискретних компонентах кіберполігона. Персонал для роботи на автоматизованих робочих місцях кіберполігона може бути сформований з науково-педагогічних працівників, вчених, ад'юнктів, курсантів та фахівців з військ. Залежно від цілей досліджень розробляються сценарії дій. Документування результатів діяльності кіберполігона, їх апостеріорний аналіз забезпечує вироблення новітніх форм, способів та методів протидії викликам і загрозам тероризму, захисту критичних інфраструктур, суспільства, керівництва, особи. Викладене проілюстроване схемою на рис. 3.6.

Результатами виконання цього завдання повинні стати:

1) методики і сценарії проведення багатосторонніх навчань на кіберполігоні з питань забезпечення інформаційної безпеки в кіберпросторі;

2) діючий комплект програмно-апаратного комплексу кіберполігона для комплексного відпрацювання питань інформаційної (інформаційно-психологічної) та кібербезпеки з можливостями його стандартизації і сертифікації;

3) методи і методики підготовки персоналу для систем забезпечення інформаційної і кібербезпеки, отримані персоналом знання і навички;

4) результати випробувань розроблених комплектів програмно-апаратних комплексів, набору програмних додатків, моделей тощо, на третьому рівні кіберпростору в умовах, наближених до реального застосування;

5) новітні форми, способи та методи протидії викликам і загрозам тероризму, захисту критичних інфраструктур, суспільства, керівництва держави та його сектору безпеки, особистостей за допомогою реалізації комплексу заходів інформаційної безпеки в кіберпросторі, спрямованих на протидію гібридним впливам;

6) відпрацьовані теоретичні і прикладні принципи, програмно-технічна складова і висококваліфіковані фахівці стануть основою для створення потужного кіберцентру та залучення цієї структури до цілодобового оперативного чергування у системі національної і загальноєвропейської інформаційної і кібербезпеки.

Розвиток науково-дослідної і учбово-лабораторної баз у сфері інформаційної і кібербезпеки, проведення багатосторонніх національних і міжнародних навчань, удосконалення системи підготовки, перепідготовки і підвищення кваліфікації військових фахівців у галузі інформаційної і кібербезпеки. Введення комунікативних технологій оперативного обміну досвідом у сфері забезпечення інформаційної і кібербезпеки для протидії гібридним впливам.

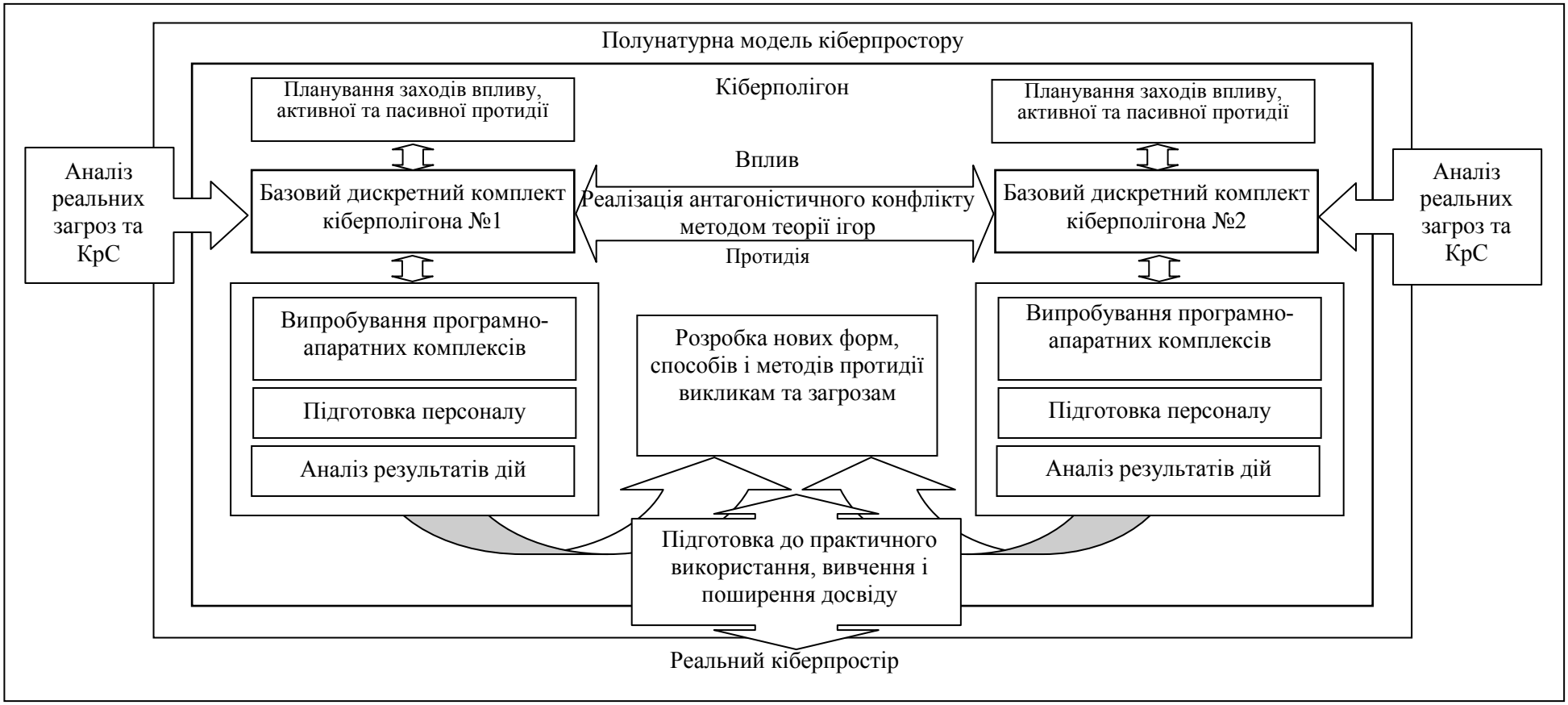

Рис. 3.6. Схема дослідження новітніх форм, способів та методів протидії інформаційним загрозам в кіберпросторі та через кіберпростір

Виконання вказаного завдання полягає в здійсненні комплексу організаційних заходів шляхом використання і впровадження результатів і досвіду виконання попереднього (четвертого) завдання проекту, зокрема:

− проведення на постійній основі багатосторонніх національних та міжнародних навчань з питань інформаційної і кібербезпеки з удосконаленням і виробленням нових способів протидії новим та прогнозованим загрозам, впровадження стандартів Альянсу і досягнення взаємосумісності Збройних Сил України з країнами-членами НАТО у сфері інформаційної і кібербезпеки;

− впровадження нових напрямів перспективних фундаментальних і прикладних наукових досліджень з використанням емерджентних властивостей діючого кіберполігона, в якому поєднанні методи напівнатурного моделювання, принципи і прийоми теорії ігор, антагоністичного конфлікту, спрямовані на інтегроване дослідження проблем забезпечення інформаційної (інформаційно-психологічної) та кібербезпеки в кіберпросторі для протидії гібридним впливам;

− сприяння ефективному рішенню наукових завдань і виконання дослідницьких функцій з розробки кваліфікаційних робіт претендентами освітнього рівня вищої освіти (бакалавр, магістр, доктор філософії) у сфері кібербезпеки учасниками проекту;

− вироблення рекомендацій відносно удосконалення змісту та методик підготовки, перепідготовки і підвищення кваліфікації військових та цивільних фахівців у галузі інформаційної і кібербезпеки в країнах-членах та країнах-партнерах Альянсу за національними стандартами і стандартами НАТО.

Виконання вказаних завдань забезпечує підвищення ефективності комплексу заходів з забезпечення інформаційної і кібербезпеки в кіберпросторі з відпрацюванням заходів протидії гібридним впливам. Це досягається шляхом розробки та виготовлення діючого комплекту комплексного кіберполігону і відпрацювання на ньому багатосторонніх практичних заходів з вироблення новітніх форм і способів протидії викликам і загрозам тероризму, захисту критичних інфраструктур, суспільства, керівництва держави, особистості.

Комплексні кіберполігони принципово відрізняється від існуючих аналогів поєднанням досліджень інформаційного впливу на технічну та ергатичну складову систем управління різного рівня і призначення (держави, критичними об’єктами, військами і зброєю та інші) з урахуванням синергетичного ефекту взаємного посилення відмічених категорій впливів, гібридних дій, що реалізовуються та розвиваються в кіберпросторі в ході ведення.

Відмінність програмно-апаратної складової таких кіберполігонів полягає у впровадженні принципів ситуативного управління, фрактального аналізу, самоорганізації, біфуркаційних моделей, що забезпечує ефективне виконання завдань забезпечення інформаційної (інформаційно-психологічної) та кібербезпеки в умовах апріорної невизначеності, щільності потоку деструктивних впливів і значної динаміки кризових ситуацій в інформаційній сфері, характерній для сучасних гібридних конфліктів.

Застосування комплексних кіберполігонів як лабораторного середовища для дослідження форм і методів протидії гібридним впливам, підготовки

персоналу, розвитку науково-прикладних напрямів удосконалення апаратно-програмної бази для реалізації протидії інформаційним і кіберзагрозам без втручання в існуючу інформаційну структуру держави, які враховують синергію інформаційно-психологічного та кібервпливів, що підтверджується реальним практичним досвідом, але без втручання в реальні системи, є відмінністю функціонального призначення кіберполігона.

3.1.5. Особливості організації наукових досліджень та впровадження високотехнологічних розробок

Особливості формування термінології. Гармонізація нормативних документів України у сфері кібербезпеки і кібероборони, відповідно до міжнародних стандартів і стандартів ЄС та НАТО і досягнення необхідного рівня інтероперабельності та успішності дій в цій сфері, потребує однакового розуміння всіма фахівцями відповідного базового термінологічного апарату. Але, в ході проведення чисельних консультацій, практичних навчань, науково-практичних конференцій, семінарів та тренінгів, що займають значне місце серед різноманітних заходів програм взаємодії між Україною і НАТО та США у сфері кібербезпеки, були виявлені протиріччя в цьому, що знижує ефективність заходів та можливість в майбутньому ефективно виконувати спільні, передбачені законодавством та досягнутими в його рамках домовленостями, завдання. Аналіз існуючих Законів України та інших нормативно-правових актів України, ЄС, провідних країн світу, зокрема США, стандартів НАТО, свідчить про дефініційну, термінологічну та нормативно-правову невизначеність або/та розбіжність об'єктно-предметної області багатьох понять, що складають базовий термінологічний набір терміносистеми сфери кібербезпеки та кібероборони. Здійснення нормативно-правового, науково-технічного, організаційного і кадрового забезпечення створення в Україні ефективної національної системи кібербезпеки та кібероборони із врахуванням світового досвіду потребує вирішення зазначеної проблеми. Для цього фахівці галузі повинні володіти відповідними методиками й алгоритмами. Розглянемо зазначені аспекти.

Логічна операція формування значення для терміна "дефініція" (лат. *definitio* – визначення) є важливим засобом скорочення складних описів та окремих міркувань у наукових теоріях та галузях знань, чим виконує важливу функцію у науково-освітній та практичній діяльності.

У термінології, як розділі лексикології, аксіомою є, що визначення будь-якого терміна (дефінієндума) та зміст і значення визначаючого поняття (дефінієнса) мають бути тотожними, вичерпувати один одного і мати один і той самий зміст (денотат). До науково-технічних термінів висуваються додаткові вимоги: системність, вмотивованість, однозначність, точність, відсутність синонімів.

За певних історичних, воєнно-наукових, зовнішньополітичних та інших причин у термінологічній системі галузі кібербезпеки та кібероборони України склалися протиріччя, що вимагають відповідного наукового розв'язання. Воно

полягає в недотриманні в термінографії сфери кібербезпеки принципів однозначності, точності та відсутності синонімів. А саме, у терміносистемі сфери кібербезпеки одночасно існує й паралельно застосовується низка дефініцій, в яких одному дефінієндуму ставиться у відповідність декілька дефінієнсів, або навпаки, один дефінієнс розкриває значення різних дефінієндумів. Це ускладнюється елементами надлишковості або недостатності денотата та відбувається на фоні жорсткої нормативно-правової легітимізації термінів, що запропоновані та втілені в обіг на рівні емоційних та емпіричних логічних операцій окремих авторів, без необхідного наукового супроводження. Термінологічна сфера кібероборони в Україні ще не сформована, тим не менш, процесу її формування притаманні ті ж самі помилки. Ускладнення цього протиріччя в площині практичного застосування термінологічного апарату сфери кібербезпеки та кібероборони відбувається за рахунок невідповідності термінологічних систем сфер кібербезпеки міжнародного співтовариства, зокрема ЄС та НАТО й України.

Вирішення протиріччя полягає у формуванні за правилами науково-технічної лексикографії множини семантичних аналітичних та синтетичних визначень термінологічної системи сфери кібербезпеки та кібероборони. Організацію та виконання даної роботи можливо здійснити за таким алгоритмом:

1. Вибір термінів та їх дефініцій з множини ключового набору термінів термінологічних систем сфер кібербезпеки та кібероборони.

2. Збір максимальної кількості вживаних конкретних дефініцій кожного терміна терміносистеми, включно з іноземних офіційних джерел міжнародних організації та країн-партнерів.

3. Аналіз кожної дефініції:

− на системність – тобто належність терміна до певної термінологічної системи; за результатом – виключення зайвих термінів;

− на відсутність синонімів; за результатом – виключення зайвих термінів, що в межах однієї терміносистеми, забезпечує запобігання взаємному непорозумінню фахівців;

− на однозначність, тобто на тотожність тільки одного наукового або технічного терміна Dfd та відповідного йому поняття Dfn; за результатом – виключення зайвих термінів;

− на точність – при чому слід з’ясувати чому виникло занадто широке значення змісту (надлишковість) або занадто вузьке визначення;

− на вмотивованість, тобто спроможність передати змістовне навантаження без додаткового застосування термінологічного словника.

4. Декомпозиція обраних для подальшої роботи термінів.

5. Композиція однозначних нових дефініцій термінів. При чому, дефініція кожного нового словосполучення (складного терміну) має містити дефініційні ознаки кожного слова складного терміна, які мають формувати дефініцію складного терміна. При цьому, складний термін має формувати нові властивості притаманні тільки йому.

6. Аналіз нової дефініції терміна на вмотивованість, точність, однозначність, відсутність синонімів, системність.

7. Порівняльний аналіз на точність та вмотивованість синтезованої дефініції терміна з аналогом міжнародної терміносистеми в даній сфері.

8. Формування пропозицій щодо включення термінів до фахових термінологічних словників.

9. Формування пропозицій щодо гармонізації нормативних документів України у сфері кібербезпеки та кібероборони відповідно до міжнародних стандартів і стандартів ЄС та НАТО [41].

Окремої уваги потребує вирішення питання організації та здійснення наукових досліджень за високотехнологічними напрямами.

Основними факторами, які впливають на розвиток і впровадження високотехнологічних розробок в інтересах національної безпеки й оборони в Україні, є:

− відсутність раціональної, незалежної, дієвої та ефективної системи пошуку, аналізу та всебічної експертної оцінки можливості реалізації та ефекту від впровадження перспективних, передових, проривних ідей і високотехнологічних проектів та їх впливу на забезпечення обороноздатності;

− відсутність або/та неузгодженість, незакінченість, безсистемність низки законодавчих та нормативно-правових актів, доктрин, концепцій, програм щодо гармонізації розвитку фундаментальної і прикладної науки та передових розробок в інтересах безпеки і оборони;

− відсутність єдиного державного органу (у тому числі з функціями управління і контролю), відповідального за формування та реалізацію політики пошуку, здійснення відбору, фінансування та реалізації розробок у сфері високих та проривних інноваційних технологій для забезпечення обороноздатності держави;

− певне зниження спроможності наукових шкіл, технологічності виробничих підприємств, відставання вітчизняної науки та промисловості в практичних і технологічних аспектах розробки і впровадження високотехнологічних проектів;

− розпорошеність зусиль, повноважень, ресурсів (економічних, технічних, часових) та наукового і науково-педагогічного потенціалу за територіальним розміщенням і цільовим призначенням;

− системне недофінансування фундаментальної науки, проектів у сфері високих та проривних інноваційних технологій, глибока комерціалізація оборонно-промислового комплексу, недостатній розвиток державно-приватного партнерства.

Таке становище у сфері розвитку високих та проривних інноваційних оборонних технологій в Україні за сучасних умов вимагає створення дієвої системи пошуку, здійснення відбору та реалізації тих розробок, які за умови їх реалізації здатні забезпечити стратегічні переваги у сфері безпеки і оборони держави на основі принципово інноваційних рішень.

Таку систему доцільно створити дворівневою.

І рівень: Національне (державне) агентство передових розробок для Сектору безпеки і оборони (прим.: назва умовна) (аналог DARPA (DARPA – Defense Advanced Research Projects Agency – агентство передових оборонних дослідницьких проектів США)), яке повинно мати статус спеціально уповноваженого державного органу, відповідального за визначення політики розвитку, супроводження розробки високотехнологічних систем озброєння і військової техніки для забезпечення обороноздатності держави. Воно має бути підпорядкованим Уряду (профільному віце-прем'єру або Міністру оборони) та підзвітним Раді національної безпеки і оборони. Основний напрям його діяльності – займатися проектами в критичних високотехнологічних сферах та галузях, які за умови їх реалізації надають державі стратегічні переваги.

З цією метою агентство повинно здійснювати:

− пошук, аналіз і оцінку ідей, проектів;

− всебічну оцінку спроможностей держави (технологічних, економічних, фінансових, політичних, безпекових) для їх реалізації;

− всебічну оцінку ризиків та загроз проекту (фінансових, політичних, безпекових, технологічних);

− оцінку (прогноз) ефекту (впливу) від впровадження результатів проекту (політичного, економічного, воєнного, інформаційного);

− здійснення функцій державної експертизи розробок з питань таємниць;

− підготовку висновків та рекомендацій щодо подальшої розробки проекту;

− формування вимог і завдань центрам компетенції (ІІ рівень), координація їх діяльності і контроль реалізації проектів;

− формування спроможностей і сприяння державно-приватному та міжнародному партнерству (у разі їх можливості та доцільності);

− відбір та ліцензування експертів.

Має складатися з керівництва Агентства, керівників проектів (за напрямами), державних експертів (за кластерами і напрямами), підрозділів, що забезпечують діяльність.

ІІ рівень: система Центрів компетенції за профільними напрямами. Може складатися з відповідних підрозділів установ Національної академії наук України, закладів вищої освіти, за необхідності з дослідним виробництвом або лабораторіями, які забезпечують можливість практичної оцінки і перевірки розробок і пропозицій. Кожен Центр відповідає тільки за свої напрями, які іншими Центрами не дублюються.

Основні завдання Центрів компетенції:

− моніторинг знань, у т.ч. спецінформації у визначеній предметній галузі;

− формування, утримання й оновлення науково-технічної бази інформаційного ресурсу за кластерами та напрямами, у т.ч. страхового фонду документації;

− збір, систематизація, поширення й примноження знань та ефективних практик за напрямами, забезпечення ефективного доступу до експертного інформаційного ресурсу;

− підтримка формування та розвитку наукових шкіл;

− розробка відповідних стандартів і впровадження отриманого досвіду;

– поглиблення рівня підготовки та розвиток науковців і висококваліфікованих інженерів-дослідників;

– оптимізація та концентрація на єдиній базі наукового, конструкторського, технологічного та виробничого потенціалу, фінансових, та інтелектуальних ресурсів;

– супроводження та координація науково-виробничої діяльності;

– виготовлення і дослідження діючих макетів, дослідних зразків інноваційних засобів ОВТ.

При цьому, повинна бути сформованою дієва система контролю і відповідальності. Всі безпосередньо пов'язані з прийняттям рішень. Керівники і виконавці юридичних осіб, у складі яких створені Центри компетенції, мають нести особисту відповідальність за результати роботи згідно із законом (дисциплінарну, адміністративну, кримінальну, матеріальну). Державні експерти – за висновки, керівники проекту – за рішення і т. ін.

Практика воєнних конфліктів останніх десятиліть не без підстав свідчить, що у сучасній війні перемагає той, хто швидше сприймає нові технології та втілює їх у життя, бере на озброєння та практично впроваджує нові воєнні доктрини і концепції, які відповідають духу часу, і, врешті-решт, у кого командири не тільки самі використовують нові технології та ідеї, а й добре знають, які із них, коли і як може використовувати противник.

Інноваційні високі технології сьогодні перетворюються в системоутворюючий фактор сучасного протиборства (включно - збройної боротьби). Завдяки їх використанню суттєво зростає кількість можливих сценаріїв розв'язування і ведення воєнних конфліктів, забезпечується детальне планування і прогнозування їх наслідків, в усіх галузях (політичній, економічній, воєнній тощо). Вони дозволяють досягнути якісно нового етапу розвитку воєнного мистецтва – переходу від управління військами в ході збройного конфлікту до управління конфліктом у цілому.

Взагалі, інтеграція високотехнологічних ресурсів угруповання військ у районі конфлікту в єдиний інформаційний простір забезпечує можливість адаптивного реагування на ситуації шляхом коригування рішень фактично у реальному часі та є базовою основою практичної реалізації мережецентричної концепції ведення бойових дій. Своєчасно отримані від різних джерел та якісно проаналізовані дані розвідки забезпечують маневрування військ (частин, підрозділів), їх всебічне забезпечення та оперативне адаптивне управління їх діями відповідно обстановці.

Високий ступінь інтегрованості та синергії дій сил та засобів, який досягається за рахунок створення єдиного інформаційного простору угруповання військ у районі конфлікту значно підвищує ефективність їх застосування.

Відповідно до мети, завдань, форм та способів забезпечення застосування високотехнологічних засобів у воєнній сфері, у світі на теперішній час сформувалися типові структури органів управління. Особливістю при їх формуванні у провідних країнах світу стало поєднання в одній структурі напрямів діяльності, пов'язаних між собою.

Сучасні високі технології змінюють процеси організації бойових дій (операцій) та методи управління ними, і тому вимагають відповідної підготовки та перепідготовки фахівців. Відповідно до цього відбувається удосконалення систем військової освіти в провідних країнах світу. Практично кожна з таких країн має військові технологічні заклади вищої освіти, в яких зосереджена підготовка фахівців тактичного й оперативного рівнів та проводяться наукові дослідження з питань застосування високотехнологічних розробок та зразків ОВТ в інтересах національної безпеки і оборони.

3.2. Загальні характеристики планування та проведення операцій у кіберпросторі та через кіберпростір

3.2.1. Сутність та можливості дій у кіберпросторі

За досвідом провідних країн світу до найбільш ефективних та результативних впливів у сучасних високотехнологічних (гібридних, проксі тощо) війнах відносяться впливи спрямовані на порушення систем управління державою та її Сектором безпеки і оборони та дискредитацію (маніпуляцію репутацією) і викривлення сприйняття військово-політичного керівництва та визначних осіб і діячів держави особовим складом збройних сил, населенням та світовою спільнотою, шляхом комплексного і системного ведення за єдиним замислом і планом різноманітних, але, в першу чергу, інформаційних, інформаційно-психологічних, когнітивних та кібер дій [25].

В даному випадку скоординоване використання спроможностей, що пов’язані з діями у кіберпросторі та через кіберпростір спрямованими та узгодженими з іншими лініями діяльності в рамках операції з метою впливу на порушення функціонування, підриву та отримання контролю над процесами управління у противників або потенційних противників, захищаючи при цьому свої процеси управління визначаються, як *кібероперація*.

Під *інформаційними діями (операціями)* будемо розуміти скоординоване використання (під час військових операцій) спроможностей, що пов’язані з використанням інформації, та узгоджене з іншими лініями діяльності в рамках операції та спрямовані на порушення функціонування, підрив та отримання контролю (узурпацію) над процесом прийняття рішення противниками або потенційними противниками, захищаючи при цьому свій процес прийняття рішення. Цілі інформаційних операцій повинні бути конкретними, вимірюваними, досяжними, бути в інтересах досягнення кінцевого стану (бути релевантними) та мати визначені часові рамки.

Складовою інформаційної операції, як правило, є психологічна операція. *Психологічні операції* – це операції із поширення визначеної інформації та виконання дій щодо цільових аудиторій для впливу на їх емоції, мотиви, об’єктивне мислення та поведінку урядів, організацій, груп та окремих осіб.

Психологічні операції являють собою заходи щодо поширення спеціально підготовленої інформації з метою здійснення впливу на поведінку і дії

населення інших країн. Метою психологічних операцій є створення сприятливих для держави і Збройних Сил умов поведінки противника. Для досягнення успіху психологічні операції доцільно об'єднувати з заходами щодо забезпечення скритності дій, військової дезінформації, фізичним знищенням елементів інфраструктури та радіоелектронної боротьбою.

Аналіз деструктивних дій, які ведуться з використанням спеціальних технологій в інформаційному та кіберпросторах України, дозволив виявити комплексні узгоджені за метою, замислом, місцем і часом інформаційні, інформаційно-психологічні та кібервпливи на всі верстви населення, соціальні і демографічні групи, керівництво держави, Міністерство оборони України та командування Збройних Сил України.

Для їх реалізації використовуються засоби телерадіомовлення, Інтернет ресурси (інформаційні сайти, соціальні мережі, спеціалізовані форуми тощо) та підробні (фейкові) новини і дезінформація, які розповсюджуються в кіберпросторі та через кіберпростір.

Серед усіх деструктивних інформаційно-психологічних, інформаційно-кібернетичних дій, що проводяться, найбільш ефективними є ті, що спрямовані проти керівного складу держави та командування Збройних Сил.

Дослідження показали, що, як правило, такі дії є комплексними і включають елементи “непрямих впливів”, маніпуляцію репутацією, сугестивний вплив. В рамках такої загальносистемної дії визначаються керівники, ті особи, вплив на яких забезпечує досягнення мети найкращим чином, обираються способи та форми впливу і проводяться за єдиним замислом і планом узгоджені, комплексні інформаційні, інформаційно-психологічні, кіберінформаційні впливи.

Вирішальним є те, що достатньо запустити відповідну інформацію, а далі, зважаючи на особливості соціуму, він сам буде продукувати плітки, будувати домисли та поширювати інформацію далі.

Таким чином, у кіберпросторі формується контент, активізація якого у визначений момент може блокувати дії будь-якого керівника і тим самим заблокувати дії структури, яку він очолює, або зробити її функціонування не ефективним, або примусити її працювати так як потрібно стороні, що проводить деструктивні впливи. Крім того, в умовах особливого періоду (воєнного стану) такі дії створюють передумови до паніки, непокори, дезорієнтації, дезертирства тощо.

Розглянемо як здійснюються деякі подібні спеціальні операції, з метою порушення функціонування систем державного та військового управління, та можливі шляхи протидії їм.

Одними з найбільш ефективних стратегій впливу на систему державного та військового управління є стратегії так званих “несилових дій”, “непрямих впливів”, “м’якої сили” та “м’яких впливів” тощо, які отримали широке розповсюдження і як стратегії нападу, і як стратегії захисту [26].

Їх дієвість обумовлена тим, що у штучно створених системах (державах, суспільстві, установах) слабкі, а здебільшого, зовсім непомітні впливи на певні уразливі “критичні” точки цих систем з часом призводять до порушення їх

функціонування, яке у кінцевому результаті може привести до кризи або, що є більш цінним, забезпечити можливість зовнішнього управління ними не на користь національним інтересам держави, на інституції якої такі впливи здійснюються.

Про розвиток та впровадження нових форм реалізації зазначених стратегій, їх ефективність та наслідки свідчать факти кризових явищ у політиці та економіці багатьох країн світу, які мали місце протягом попередніх десятиліть [27].

А також, що в провідних країнах світу такий підхід не тільки офіційно прийнятий, але й, як правило, нормативно визначений. А саме, у якості основних напрямів здійснення впливів розглядаються: організаційні засади країни, її ресурсні та матеріально-технічні можливості.

Слід зазначити, що положення, які складають теоретичну базу стратегій "несилових дій" та поширилися у провідних країнах світу у другій половині XX століття, а на цей час стали вже загальносвітовою практикою, були відомі ще у стародавньому світі. Ще у V столітті до н.е. відомий китайський філософ і теоретик Сунь-Цзи у трактаті "Про військове мистецтво" писав: "Мистецтво війни полягає у тому, щоб знищити противника зсередини. Той, хто майстерно веде війну, впокорює чуже військо не б'ючись, захоплює чужі фортеці без облоги, руйнує чужі держави без тривалих кампаній. Сто разів битися та перемогти не краще з кращих. Краще з кращих це підкорити чужу армію без битви" [28].

Тобто, ще у давнину досвідчені державні та воєнні діячі прагнули досягти перемоги над державою-супротивником, використовуючи дезорганізацію системи управління нею та її армією ще за мирного часу, а під час війни – до вирішальної битви.

У сучасних умовах цей принцип став загальноприйнятим і отримав поширення на всі сфери діяльності людства. На це вказують багато авторів, наприклад, відомий британський фахівець Дж. Шерр зазначає: "Акценти почали зміщуватись – і мають зміщуватись – з виявлення відкритих загроз до виявлення точок тиску уразливих місць, які можуть бути використані для того, щоб підірвати державу зсередини, зруйнувати відносини між владними структурами, і зіпсувати відносини між державою і суспільством" [29].

Саме на основі пошуку уразливих об'єктів в інформаційній інфраструктурі фактично побудовані сьогодні доктрини "м'якої сили", а бурхливий розвиток інформаційних технологій є матеріальною основою трансформування доктрин "м'якої сили" в концепції ведення сучасних війн і війн майбутнього, де питанням інформаційних дій приділяється головна увага в трьох площинах: морально-психологічній, радіоелектронній, кібер.

Отже, значна кількість країн приділяє багато уваги цьому напряму, серед яких особливо виділяються США, КНР та РФ [30, 31].

Таким чином, несилові методи зовнішньої політики у провідних країнах світу стали основною парадигмою національної безпеки, яка передбачає досягнення цілей насамперед маніпулюванням свідомістю особистості, суспільства, окремої країни та її інформаційними та соціальними ресурсами.

При цьому, надання гарантій безпеки особі, соціальним групам, суспільству та державі в цілому в цих умовах можливе лише на основі системної превентивної діяльності органів державного та військового управління щодо прогнозування можливих загроз, їх своєчасного виявлення та нейтралізації.

Технологія впливу на визначені держави за допомогою застосування стратегій "непрямих дій" і "м'якої сили" будується на основі наступних базових ідей і підходів:

– використання відкритих та прихованих форм і методів впливу з метою руйнування основ державності противника за умови відсутності відкритої конфронтації або прямого силового зіткнення;

– досягнення панування над країною-об'єктом впливу здійснюється за рахунок позбавлення її економічної та ресурсної самодостатності, що позбавляють її можливості до сталого розвитку.

Це досягається шляхом створення в рамках системи державного та військового управління країни-жертви особливого організаційного механізму "зовнішнього управління", що дозволяє встановити опосередкований і прихований контроль над процесами життєдіяльності.

Загалом можливо виділити два варіанти розвитку стратегії "непрямих дій": агресивний та несиловий.

Специфічною особливістю несилового варіанта є сприяння бажаної зміни геополітичної могутності держави на свою користь за рахунок "природної" деградації країни-жертви. Це дозволяє атакуючій державі дочекатися ослаблення свого супротивника до необхідного рівня і появи умов, за яких проведення силових акцій щодо захоплення території може не знадобитися. В даному випадку роль Збройних Сил буде зведена до закріплення силовим шляхом створеної ситуації в конкретному регіоні.

Впровадження агресивного варіанта стратегії "непрямих дій" можна проілюструвати на прикладі подій, що відбувалися на пострадянському просторі та Близькому Сході. Багатьма дослідниками вважається, що події, які сталися, є наслідком застосування теорії "керованого хаосу", авторами якої є Дж. Шарп [32] і Ст. Манн [33], на основі якої була розроблена технологія реалізації стратегії "м'якої сили", що базується на таких принципах:

– об'єднання всіх політичних сил, які виступають проти існуючого законного уряду;

– підрив упевненості керівництва країни у своїх можливостях щодо стабілізації обстановки і в лояльності силових структур;

– дестабілізація обстановки в країні шляхом ініціювання протестних настроїв, що культивуються в різних верствах суспільства з метою підриву легітимності існуючого політичного режиму;

– ініціювання зміни влади шляхом заперечування результатів виборів та організації актів громадянської непокори.

Практично в усіх країнах, втягнутих в масові заворушення за цими стратегіями, "стихійний" збір натовпу і подальше управління ним були організовані за допомогою розсилання повідомлень про намічені мітинги і

протестні акції через соціальні мережі та електронну пошту, а також на мобільні телефони.

Формовані політтехнологами громадські структури у соціальних мережах створюють протестну масу людей на наступних рівнях:

− на інформаційному рівні опозиційні сили акцентують увагу людей на існуючих проблемах з виробленням загостреною реакції на недоліки в суспільному житті і популістськими пропозиціями щодо їх вирішення;

− на ментальному рівні у людей формується стійке переконання, що при даному режимі “так далі жити не можна” і “жити стало нестерпно”;

− на соціальному рівні активізується діяльність етнічних, соціальних, релігійних та регіональних груп з метою їх мобілізації на застосування радикальних методів вирішення існуючих у суспільстві проблем.

Тому такі події є виступами людей замаскованими під стихійні з метою зміни неугодних відповідним силам політичних режимів.

Застосування стратегії “м’якої сили” звичайно реалізуються в наступній послідовності:

− на першому етапі здійснюється дестабілізація соціально-політичної та економічної систем країни-жертви шляхом створення масштабної системної кризи і занурення її в стан “керованого хаосу”, що робить політичний режим даної країни уразливим для зовнішнього впливу;

− на другому етапі, в умовах, “керованого хаосу” формується структура соціально-політичного впливу в особі опозиційного центру, завданням якого є взяття влади в країні при зміні політичного режиму;

− на третьому етапі починається процес формування нових інститутів державного управління та силових структур під егідою міжнародних організацій.

Таким чином, стратегія “м’якої сили” є важливим і дієвим потенційним політичним інструментом, на який потрібно зважати у сучасних умовах.

Реалізація стратегії “м'якої сили” неможлива за умови адекватної відповіді самої системи державного та військового управління. Така протидія функціонує якщо ключові фігури (керівники) знаходяться на своїх місцях та ефективно працюють. Тому одним із основних елементів стратегії “м'якої сили” є блокування роботи відповідних керівників шляхом комплексних впливів на них. Одним із способів реалізації таких впливів є маніпуляція репутацією.

Ефективність державного управління, в такій складній та динамічній системі, якою є система державного та військового управління, залежить від багатьох факторів [34], насамперед таких:

− вірного обґрунтованого визначення національних цінностей, національних інтересів, національних цілей;

− своєчасного виявлення загроз життєво важливим інтересам особи, суспільства та держави;

− обмежень, насамперед, нормативно-правового характеру на можливості щодо здійснення державного та військового управління;

− реальних владних повноважень кожної з гілок влади, відповідних керівників на місцях щодо забезпечення національної безпеки та оборони;

− забезпеченість узгодженості позицій основних учасників, які здійснюють формування та реалізацію державної політики у сфері національної безпеки та оборони;

− наявність стратегічного мислення у керівництва держави та політичної волі щодо його практичного втілення;

− відповідність складу, структури, завдань та функцій системи забезпечення національної безпеки, її окремих компонентів та їх взаємозв'язків наявним та потенційним загрозам;

− інформаційне-аналітичне, науково-методичне, організаційно-технічне, ресурсне та нормативно-правове забезпечення діяльності системи забезпечення національної безпеки та оборони;

− наявності підготовлених фахівців державного та військового управління, а також ефективної системи їх підготовки;

− раціонального підбору та розстановки кадрів;

− мотивації державних службовців на ефективне виконання своїх обов'язків.

Зазначені фактори досить тісно взаємозв'язані між собою. Взагалі, інтегрально, ефективність функціонування системи державного та військового управління ґрунтується на професіоналізмі, раціональному ієрархічному розподілі службових повноважень та мотивації, а також залежить від репутації суб'єктів управління.

Тому, при визначенні шляхів реалізації стратегій, що розглядаються, особливу увагу приділяють можливості впливу на систему комплектації кадрів, враховуючи її особливості, які дозволяють виявити та використовувати найбільш уразливі її елементи.

Відомо, що управління, як вид суспільної діяльності, передбачає систему скоординованих впливів суб'єкта на об'єкт з метою досягнення певної організаційної мети. Тому «несилові дії», спрямовані на зниження ефективності управління, забезпечують досягнення цієї мети шляхом певних впливів саме на зазначених суб'єктів. Вибір конкретних способів, методів та прийомів реалізації зазначених стратегій витікає зі специфіки їх діяльності.

Найбільш часто застосованим методом реалізації стратегій впливу є спеціальні операції, які спрямовані на те аби прибрати кваліфіковані кадри з ключових керівних посад. Основним завданням у такому випадку є заміщення професіоналів, або створення таких умов, щоб вони залишали місця служби, або не змогли якісно виконувати свої посадові обов'язки.

Блокування роботи може здійснюватися різними методами й на різних рівнях: на рівні створення відповідних нормативних актів, розпоряджень, наказів, тощо, здійснення морально-психологічного тиску, демотивації та дискредитації особи тощо.

Порушення функціонування всієї системи державного та військового управління успішно можна досягти шляхом керування прийняттям законів у сфері безпеки та оборони та їх змістом.

Одним із варіантів паралічу країни зазначеним шляхом в умовах сучасної війни є вплив на прийняття таких законів, кожний з яких є правильним і

необхідним, але у сукупності вони блокують прийняття будь-яких ефективних рішень. Таким чином, створюється система, в якій один закон вступає в протиріччя з іншим. Це суттєво доповнює арсенал маніпуляції репутацією тому, що кожен керівник так або інакше потрапляє в ситуацію коли прийняте за одним законом рішення є правильним, а за іншим – злочинне.

Розрізняють декілька рівнів маніпулятивного впливу на осіб, що займають керівні посади.

1. *Умовити*. Першим кроком, що реалізується щодо впливу на керівника, є маніпуляція його життєвим досвідом, позиціями, вподобаннями та віруваннями. Людина може бути лояльною до впливу, що здійснюється на неї та буде готовою відповідно до своїх переконань змінити сторону, на яку працює. Прикладом такого впливу є факт переходу на службу до Російської Федерації керівників державних установ та службовців Збройних Сил України у березні 2014 року при анексії Кримського півострову [35]. Частина особового складу свідомо мала наміри зробити такий крок під впливом багаторічної інформаційної кампанії проти українського народу. Частина людей не захотіла змінювати місце проживання і прийняла умови агресора.

2. *Підкупити*. Якщо керівника (командира, начальника) не можливо умовити, то наступним способом примусити його виконувати дії, необхідні для іншої сторони, є підкуп. Непоодиноким явищем є те, що з початком бойових дій частина командирів залишає свої підрозділи (наприклад, так поступила більшість іракських військових керівників під час проведення в Іраку в 2003 році збройними силами міжнародної коаліції військової операції «Шок і трепет» («Свобода Іраку»)), що призводить до втрати управління та подальшої поразки військ у військовій компанії.

3. *Маніпуляція репутацією*. Розповсюдженим способом "знищення" керівника є маніпуляції його репутацією. Такий сценарій полягає у формуванні і розповсюдженні неправдивої інформації, яка дискредитує керівника, або формує таке уявлення, що дана посадова особа є небезпечною для організації, якою керує, або є некомпетентною, має якісь особисті вади тощо.

Найпростіше така інформація розповсюджується в кіберпросторі та через кіберпростір засобами глобальної мережі Інтернет. Неконтрольоване поширення через соціальні мережі, форуми, блоги переважно неправдивої інформації та такої, що важко перевірити відбувається з метою формування негативного образу керівника.

Прикладом такого явища є поява з початком російської агресії в Україні та анексією Кримського півострова Інтернет ресурсів, форумів, груп у соціальних мережах, заміток у блогах, в яких подається спеціально підготовлена інформація про президента, уряд, парламент, керівників українських силових відомств із зазначенням нібито зради та скоєних злочинів проти української держави та народу України. Інформація активно тиражується і розповсюджується з метою створити відповідний резонансний вплив на думку громадськості.

Типовий (спрощений) алгоритм, який використовувався деструктивними силами для дискредитації та компрометації керівників (командирів, начальників):

1) визначення осіб керівного та командного складу компрометація, яких сприяє досягненню визначеної мети;

2) визначення складу і змісту інформації, яку необхідно зібрати по визначених особах та їх оточенню;

3) збір, обробка та аналіз інформації;

4) формування контенту для здійснення дезінформації, паплюження образу й авторитету, маніпуляції репутацією воєнно-політичного керівництва держави та керівного складу військових формувань держави, нагнітання недовіри до органів управління, керівного та командного складу, підрив їхнього авторитету, їх дискредитація та деморалізація;

5) формування та просування деструктивних меседжів та наративів через стратегічні комунікації, популярні ЗМІ, сайти, блоги, інформаційні та соціальні мережі (на форумах, у соціальних групах, Інтернет-спільнотах), теле- й радіоканали;

6) пошук та широке залучення тих хто буде просувати та підтримувати деструктивні меседжі і наративи у національному та міжнародному кібер інформаційному просторі (представники ЗМІ, незадоволені, «ображені», «корисні ідіоти», агенти впливу на міжнародному рівні та серед місцевого населення тощо);

7) здійснення заходів по маскуванню дій;

8) здійснення моніторингу ефективності дій, реагування на них, корегування та координації, визначення необхідності продовження, посилення або завершення.

4. *Фізичне знищення*. Є крайньою мірою, що застосовується в окремих випадках, якщо відповідний керівник (начальник) займає ключовий пост, є професіоналом своєї справи та суттєво заважає планам противника, а інші способи усунути його від виконання своїх обов'язків виявилися безрезультатними.

В контексті вище зазначеного, одним із важливих і ефективних засобів впливу на визначених осіб (групи осіб) є навіювання або сугестія [36] – як процес впливу на психіку людини, пов'язаний зі зниженням свідомості й критичності при сприйнятті навіяного змісту, спровокованим підказкою, навідними питаннями, який не вимагає ні розгорнутого особистого аналізу, ні оцінки спонукання до певних дій. Суть навіювання полягає у впливі на відчуття людини, а через них – на її волю і розум.

Як основний спосіб маніпулювання свідомістю, навіювання стає складовою частиною спеціальних операцій спрямованих на порушення системи державного та військового управління.

За рахунок використання навіювання можливо досягнення наступних цілей:

− за мирного часу: підготовка суспільно-політичної ситуації та формування іміджу і репутації певних посадових осіб;

− у воєнний час: забезпечення маніпуляції репутацією керівників Сектору зпеки і оборони із застосуванням усіх активних деструктивних форм, методів і способів навіювання;

− у післявоєнний час: забезпечення створення позитивного іміджу нової системи влади.

Аналіз показав застосування таких методів навіювання: дезінформація, пропаганда, диверсифікація громадської думки, психологічний тиск, поширення чуток, переконання, штучне формування, так званих, помилкових спогадів тощо.

У відомих роботах описано кілька сугестивних підходів у здійсненні психологічного впливу з метою маніпулювання свідомістю, думками, уявленнями та діями людей [37]:

1. Психоаналітично орієнтований підхід, який використовує "підсвідомість" з метою маніпулювання свідомістю.

2. Гіпнотичний підхід, за якого використовується трансовий стан.

3. Підхід за допомогою еріксонівського гіпнозу передбачає застосування мовних стратегій для нейтралізації здатності до опору навіюванню.

4. Підхід нейролінгвістичного програмування здійснюється за рахунок спеціально підібраного нейросемантичного гіпертексту, що містить найбільш важливі слова та фрази для особи чи групи осіб, котрі зазнають сугестії.

Особливо ефективні сугестивні технології в Інтернеті. Цьому сприяє низка факторів:

− висока довіра до неофіційних ресурсів мережі;

− аудиторія залучається до інформації з метою розв'язати будь-які проблеми;

− формування мережних співтовариств на основі емпатії (співчуття).

Таким чином, маніпуляція репутацією є ще одним та у низці випадків найбільш дієвим видом деструктивних дій, спрямованих на порушення функціонування системи державного та військового управління.

З практики несилового протистояння між країнами в інформаційному та кіберпросторі можна зробити висновок, що усі згадані технології та способи організації деструктивних дій, спрямованих на порушення функціонування систем державного та військового управління, застосовуються комплексно в рамках єдиної інформаційно-психологічної операції (рис. 3.7) [38], що відмічається на прикладі гібридної агресії проти України.

Останнім часом телебачення, друковані й особливо електронні ЗМІ, вдаються до небезпечних для суспільства методів інформаційно-психологічного впливу, розповсюдження неперевіреної інформації, а іноді і дезінформації.

Проведений, аналіз випусків новин деяких каналів, показав, що в них найбільшим чином використовуються наступні маніпуляції інформацією:

− напівправда або вибіркова правда;

− посилання на анонімний авторитет або джерело;

− багаторазове повторення не дуже суттєвої інформації;

− зміщення акцентів;

− роздмухування деталей;
− використання ярликів (“каратели”, “хунта” тощо).

Рис. 3.7. Загальносистемні деструктивні дії спрямовані на порушення функціонування систем державного та військового управління

При цьому, доля негативної (деструктивної) інформації незначна і подається приховано і виважено. Сцени відвертого насильства, вбивства заретушовані, показуються і коментуються коректно.

Широко застосовується емоційна форма подачі інформації диктором з надмірною жестикуляцією та сарказмом, навмисною артикуляцією мови.

Цікавими також є факти частоти згадування певних подій в медіасфері. Зазначено, що таким гучним подіям, які відбулися в районах Іловайська та Дебальцеве, передували значні сплески активності в інформаційній сфері. Активно поширювалася інформація негативного змісту стосовно ключових керівників Збройних Сил України та державних діячів. Наприклад, проведені контент-аналіз та моделювання у системі “Инфострим” [39] щодо подій

навколо Дебальцеве у лютому 2015 року показують амплітудні коливання кількості поширених таких повідомлень (рис. 3.8). Аналіз залежності свідчить про те, що інформаційна операція з нагнітання обстановки та створення паніки в українському суспільстві почалися задовго до початку військової операції та досягла свого піку безпосередньо з ходом бойових дій.

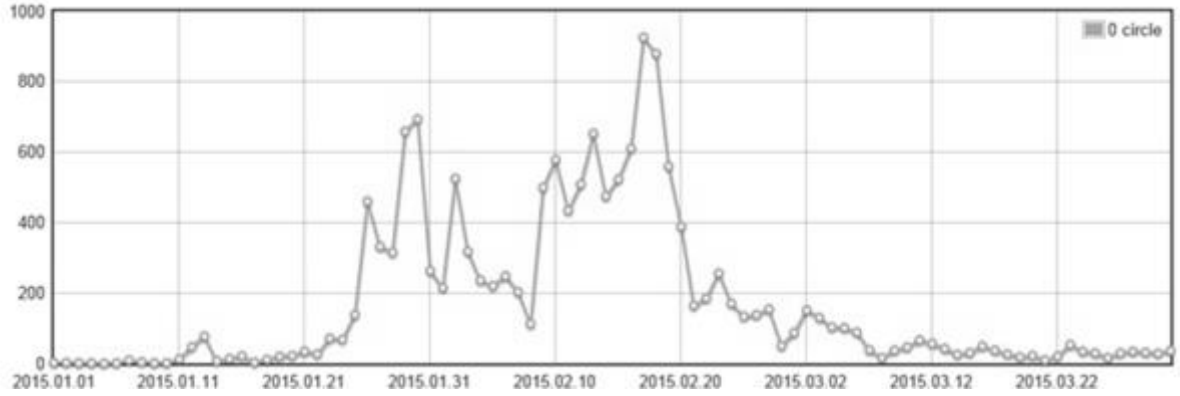

Рис. 3.8. Частота появи у електронних ЗМІ повідомлень деструктивного змісту напередодні та під час проведення операції у Дебальцеве [40]

Аналіз ЗМІ показав, що спостерігається тенденція широкого застосування негативної суспільно-політичної інформації, яка призводить до наступних наслідків:

1. Розширення потоків негативної інформації, наслідком чого є посилення девіантної поведінки не тільки окремих індивідів, але і цілих соціальних спільнот.

2. Посилення потенційних можливостей соціальної інформації ефективно впливати на всі без винятку соціальні групи населення в негативних або вузькоегоїстичних цілях.

3. Здатність соціальної інформації впливати не тільки на свідомість людей, а і на підпорогову сферу, викликати процеси зомбування особистості.

4. Поява реальної можливості активно втручатися в процеси управління з використанням інформаційних і кіберзасобів.

5. Створення інформаційної і кіберзброї та можливість ведення інформаційної, психологічної, когнітивної, кібервійн, як основного засобу продовження державної політики, а також політики недержавних регіональних та геополітичних акторів.

Для приховання факту застосування інформаційно-психологічного впливу застосовують широкий спектр маніпулятивних прийомів.

Ось тільки деякі з них: анонімний авторитет, буденна розповідь, напівправда або вибіркова правда, повторення, інформаційне перевантаження, використання ярликів, коментарі, приєднання до аудиторії, підміна фактів, підміна або переписування історії, штучне формування помилкових спогадів, зсув акцентів, маніпулятивне поєднання фактів, фальшивий прототип, роздмухування деталей, використання технології 25 кадру та подібних тому тощо.

При цьому дії представників національного медійного ресурсу, які навмисно чи ні підтримують започатковані деструктивними геополітичними (регіональними, місцевими) акторами інформаційні акції для створення, так званих, “сенсацій” значно погіршують і без того складну ситуацію. В гібридній війні, яка відбувається на території України, деструктивними акторами активно використовувались недостовірні та неавторитетні джерела, негативні повідомлення в ЗМІ значно перевищували позитивні, постійний пресинг, сарказм та глузування над діями вищого керівництва силовими структурами та командирами створювали негативну реакцію та песимізм у підрозділах сил антитерористичної операції, Сектору безпеки і оборони держави.

Наслідками зазначеного в 2014-2018 роках стала дискредитація низки дій Збройних Сил України та їх керівників, підрив авторитету багатьох командирів, розпалювання невдоволення діями вищого військово-політичного керівництва держави. В 2014-2015 роках здійснювалося активне впровадження сумнівів у необхідності ведення бойових дій, підрив морально-психологічної стійкості військових, спонукання їх до дезертирства. У разі відсутності реагування та ефективної протидії зазначеним інформаційно-кібернетичним діям, можна прогнозувати невідворотні наслідки підриву спроможностей Сектору безпеки і оборони держави та Збройних Сил України.

3.2.2. Сутність та зміст кібероперацій

Нині кібероперації виступають альтернативою застосування засобів вогневого ураження. У більшості випадків ефективність кібероперацій на порядок вище ефективності операцій із застосуванням засобів вогневого ураження. Високий показник ефективності кібероперації пояснюється тим, що сучасні засоби кібервійни досягли такого рівня бойових можливостей, який гарантує їм внесення радикальних змін у сутність воєнного протиборства.

Кібероперація – це скоординовані й узгоджені за метою, завданнями, масштабом, місцем і часом паралельні або послідовні кібердії розвідувального, оборонного та/або наступального характеру, які проводяться за єдиним замислом і планом і мають на меті завоювання переваги над противником у кіберпросторі для вирішення стратегічних, оперативних, а у низці випадків і тактичних завдань в установлений період часу в кіберпросторі та/або через кіберпростір за рахунок порушення процесів управління силами і засобами в оборонній, соціальній, технічній (соціотехнічній) сферах та нанесення збитків суб’єктам та об’єктам з критичною інформаційною інфраструктурою протиборчої сторони і захисту власних кіберсистем від аналогічних дій у відповідь.

Кібероперації полягають у:

− прихованому проникненні у системи управління стратегічною зброєю з подальшим несанкціонованим її спрацюванням, що призводить до виникнення техногенних аварій та катастроф й знищення відповідної інфраструктури;

− блокування систем управління військами, передача у війська помилкових наказів і директив у найважливіші моменти бойових дій;

– дезорганізація орбітального угруповання протиборчої сторони (за його наявності);

– блокуванні запуску стратегічних ракет, зміні польотного завдання ракет шляхом їх перенацілювання на власні об'єкти з критичною кібернетичною інфраструктурою або об'єкти іншої держави.

Найбільш ймовірний сценарій проведення кібероперації показано на рис. 3.9 [44].

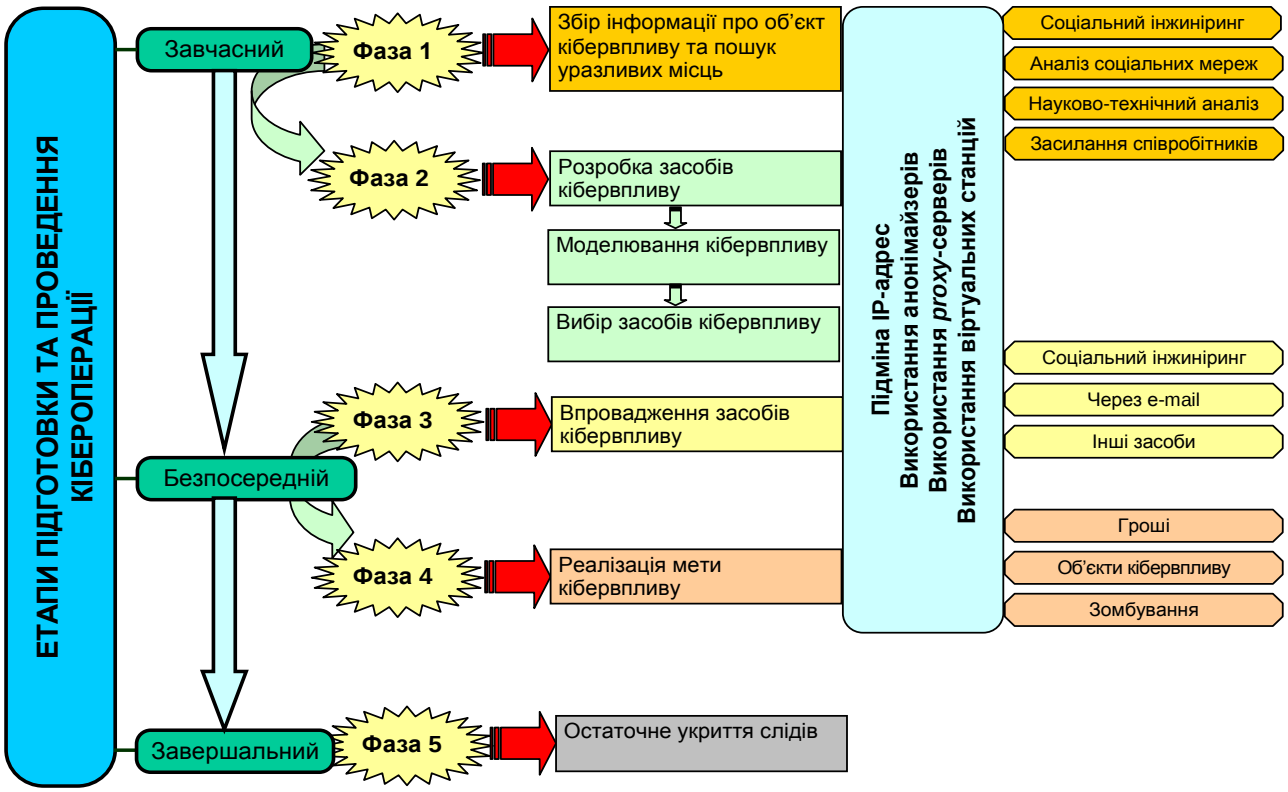

Рис. 3.9. Типовий сценарій проведення кібероперації

Типова кібероперація включає три основні етапи:

– завчасний;
– безпосередній;
– завершальний.

На першому етапі реалізується перші дві фази кібероперації. Під час першої фази зусилля фахівців спрямовуються на збір інформації про об'єкт кібервпливу та пошук його уразливих місць у системах безпеки, апаратному та програмному забезпеченні тощо. З цією метою використовуються усі наявні способи та ресурси, на кшталт методи соціального інжинірингу, аналіз соціальних мереж, науково-технічний аналіз, засилання співробітників на визначений об'єкт із закритою системою управління (адміністрацію президента, урядовий апарат, банки, нафтові корпорації, підприємства атомної енергетики та ін.) тощо.

Під час другої фази здійснюється розробка засобів кібервпливу. Розробляються різні "експолойти", уразливості "нульового дня", програми

віддаленого керування тощо. Проводиться моделювання кібервпливу на моделях об'єктів кібервпливу з метою доопрацювання засобів кібервпливу та вибору з них найбільш дієвих для даних умов.

На другому, безпосередньому етапі кібероперації, реалізуються також дві основні фази – третя та четверта. Під час третьої фази, як правило, вирішується концептуальне питання щодо впровадження засобів кібервпливу у закриті системи управління протиборчої сторони. Для цього використовують методи соціального інжинірингу, спам-розсилку та інші засоби проникнення. Під час четвертої фази здійснюється безпосередньо дезорганізація і вивід з ладу систем управління та інформаційно-телекомунікаційних систем об'єктів впливу.

На третьому, завершальному етапі, який є заключним етапом проведення кібероперації, під час п'ятої фази вживаються усі можливі заходи щодо укриття слідів кібероперації. При цьому слід зауважити, що на кожному з етапів та під час кожної із фаз заходи щодо укриття слідів є неодмінним атрибутом їх проведення [44].

Операція в кіберпросторі складається з чотирьох основних оперативних компонентів:

− кіберпротиборство;
− кібероперація в мережах;
− операція з кіберпідтримки;
− операція з кіберобізнаності.

Кібероперація включає два основні оперативні компоненти:

− операція в комп'ютерних мережах, до якої входять кібероперації з кіберрозвідки, кіберзахисту та кібервпливу;
− операція з кіберпідтримки глобальної комп'ютерної мережі.

Співвідношення між оперативними компонентами операцій в кіберпросторі та кібероперацій показано на рис. 3.10.

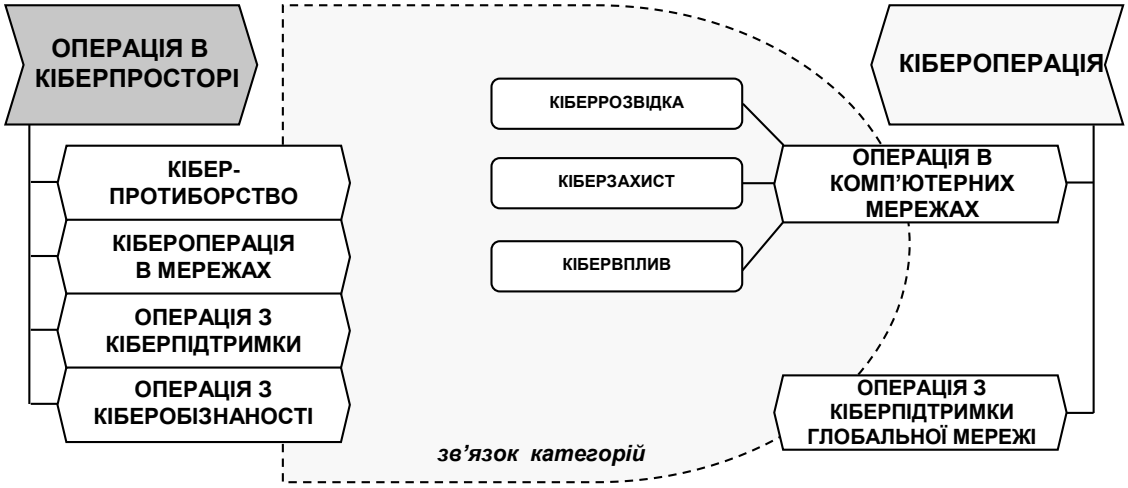

Рис. 3.10. Система кібероперацій за поглядами американських військових

Розглянемо більш детально оперативні компоненти операції в кіберпросторі, спираючись на "Концептуальний план розвитку можливостей

сухопутних військ з ведення кібероперацій в кіберпросторі на період з 2016 по 2028 роки" США. Структуру визначених оперативних компонент показано на рис. 3.11.

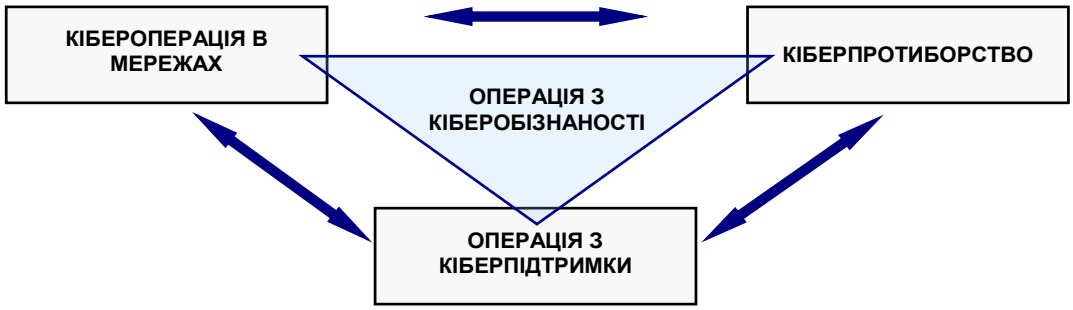

Рис. 3.11. Структура оперативних компонент операції в кіберпросторі

Операція з *кіберобізнаності* здійснюється з метою автоматизованого оцінювання й аналізу ситуації в кіберпросторі про протиборчу сторону й стан своїх військ. На основі добутих даних відкривається можливість прийняття обґрунтованих рішень на усіх рівнях – стратегічному, оперативному, тактичному. На рисунку показано, що операція з кіберобізнаності має зв'язок з іншими трьома оперативними компонентами операцій в кіберпросторі.

Згідно з класичним визначенням терміна "ситуаційна обізнаність" – усвідомлення сприйняття елементів обстановки в єдиному просторово-часовому континуумі та проекція їх на найближче майбутнє.

У широкому сенсі ситуаційна обізнаність – це можливість отримання у реальному масштабі часу досить повного і точного набору необхідної для прийняття рішення інформації про ситуацію, що відбувається з урахуванням різних умов (погодних, кліматичних, місцевості, даних про противника та свої війська тощо).

Доопрацювання теоретичної моделі "Ситуація ситуаційної обізнаності" доктора М. Ендслі дозволяє подати операцію з кіберобізнаності ієрархічною моделлю, вигляд якої показано на рис. 3.12.

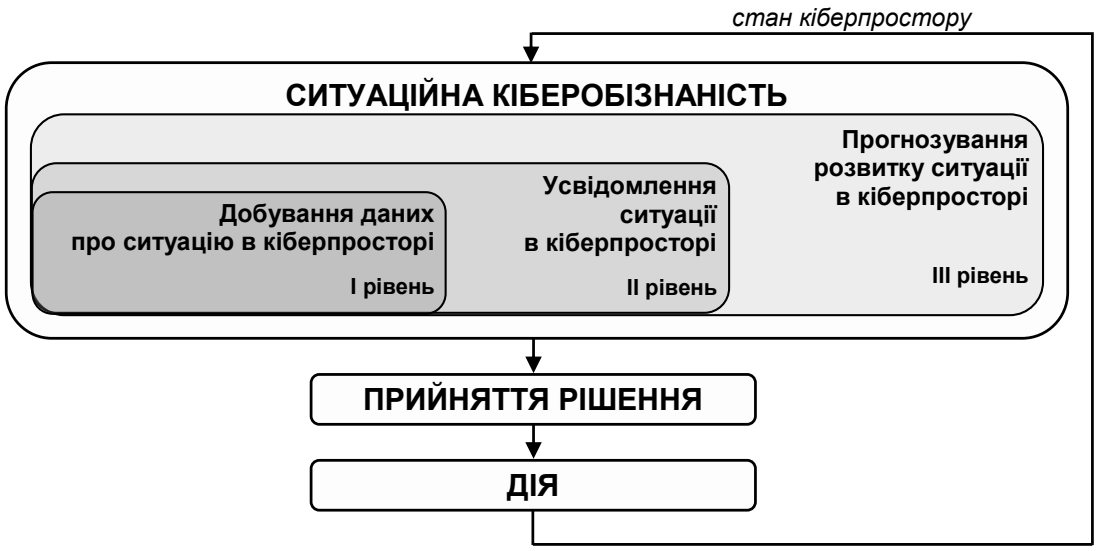

Рис. 3.12. Ієрархічна модель операції з кіберобізнаності

Згідно з моделлю (рис. 3.12) стан кіберобізнаності є результатом аналізу та оцінювання ситуації, що включає: на першому ієрархічному рівні – добування даних про ситуацію в кіберпросторі; на другому – усвідомлення ситуації, що відбувається в кіберпросторі; на третьому – прогнозування розвитку ситуації в кіберпросторі.

На кожному з рівнів операція з кіберобізнаності включає у себе наступні елементи.

На першому рівні добуваються дані про ситуацію в кіберпросторі.

Визначається:

− склад сил та засобів протиборчих сторін;

− перелік суб'єктів кібервпливу;

− перелік об'єктів з критичною інформаційною інфраструктурою.

На другому рівні з метою усвідомлення ситуації в кіберпросторі:

− оцінюються наміри та кіберможливості протиборчих сторін;

− оцінюється ступінь уразливості протиборчих сторін та їх критичної інформаційної інфраструктури.

На третьому рівні:

− здійснюється прогнозування розвитку ситуації та наслідків від здійснення кібердій;

− визначаються кіберможливості необхідні для ефективного планування та здійснення кібердій.

Кібероперація в мережах є складовою оперативною компонентою операцій в кіберпросторі (рис. 3.12). Вона проводиться з метою встановлення управління над мережами та об'єктами з критичною інформаційною інфраструктурою, а також з метою їх захисту від кібервпливів протиборчої сторони в кіберпросторі та інших просторах (морському, наземному, повітряному, космічному).

Основними елементами кібероперації в мережах є:

− кіберуправління підрозділом;

− кіберуправління контентом;

– захист від кіберзагроз, у тому числі забезпечення безпеки інформації управління, комп'ютерних мереж і захисту критичної інформаційної інфраструктури.

Кіберуправління підрозділом – це технологія, процеси та політика, виконання якої необхідне для забезпечення ефективного управління комп'ютерами та мережами.

Кіберуправління контентом – це технологія, процеси та політика, виконання якої необхідне для забезпечення гарантованої доставки у визначеному форматі точної та достовірної інформації.

Захист від кіберзагроз – дії, що поєднують функції забезпечення безпеки інформації та захисту комп'ютерних мереж і об'єктів з критичною інформаційною інфраструктурою з метою виявлення, запобігання та протидії протиборчій стороні при маніпулюванні нею інформацією.

Кіберпротиборство – це складова оперативна компонента кібероперацій (рис. 3.11), що має розширені повноваження на проведення кібероперацій у кіберпросторі та поза ним (на суходолі, морі, в повітрі та космосі) і має на меті захист власних глобальних мереж шляхом виявлення та протидії кібервпливам протиборчої сторони. Основними зразками кіберозброєння при веденні кіберпротиборства виступають спеціалізовані комп'ютери з відповідним програмно-алгоритмічним забезпеченням, телекомунікаційні мережі та інфраструктура.

Для ведення кіберпротиборства разом з кіберопераціями в мережах та операціями з кіберпідтримки використовуються кіберрозвідка, кібервплив та динамічна кібероборона. Кіберрозвідка передбачає добування розвідувальних даних про протиборчу сторону з використанням комп'ютерних мереж при підтримці засобів РЕР та РЕБ. Кібервплив у вигляді кібератак при підтримці, за необхідності, засобами РЕБ, звичайних озброєнь та ін., здійснюється шляхом зміни, знищення, викривлення інформації та програмного забезпечення, що знаходиться в комп'ютерних мережах та системах, або самих комп'ютерних мереж та систем протиборчої сторони з метою виключення ведення нею деструктивних дій. Динамічна кібероборона – це комплекс дій із забезпечення стійкої роботи комп'ютерних мереж та систем в умовах ведення протиборчою стороною кіберпротиборства. Він включає забезпечення безпеки інформації управління, локалізації кіберзагроз, проведення заходів щодо мінімізації наслідків від проявів кіберзагроз, а також спостереження, виявлення та активне реагування на несанкціоновані дії протиборчої сторони в комп'ютерних мережах та системах. Динамічна кібероборона ґрунтується на загальноприйнятих армійських оборонних принципах – забезпечення максимального кіберзахисту на усю глибину оборони з максимальним використанням наступальних дій, спрямованих на локалізацію кіберзагроз.

Операція з *кіберпідтримки* – це сукупність скоординованих та синхронізованих заходів, які плануються, організовуються та здійснюються з метою підтримання кібероперацій в мережах та кібернетичного протиборства своїх військ шляхом несанкціонованого проникнення в комп'ютерні мережі та системи протиборчої сторони з метою блокування інформації управління,

передачі дезінформаційних повідомлень або виведення з ладу його систем управління та зв'язку.

Проведення операції з кіберпідтримки вимагає обов'язкового її урахування у загальному контексті планування кібероперації та всіх інших операцій, які плануються або проводяться. При цьому обов'язково повинні враховуватися можливі негативні наслідки від таких дій щоб уникнути нанесення шкоди мирному населенню.

3.2.3. Підходи щодо планування кібероперацій

Методологія планування кібероперацій на сьогодні ще перебуває у стадії розробки. Поряд з цим можна визначити основні види планування кібероперацій. Перший вид планування – це завчасне, другий – планування на випадок кризової ситуації. Планування кібероперації повинно здійснюватися з урахуванням багатьох аспектів і повинно передбачати використання усіх ресурсів Збройних Сил, міжвідомчих організацій, а також ресурсів союзників.

Завчасне планування кібероперації здійснюється з метою розробки порядку здійснення кібердій на випадок мирного та воєнного часу та обов'язково повинно враховувати: ступінь ризику кібернетичної протидії протиборчої сторони; можливі наслідки розвитку кіберконфлікту через неузгодженість або недбалість у діях союзників та міжвідомчих організацій тощо.

Планування кібероперації розпочинається з вивчення та усвідомлення задуму операції, цілей і намірів вищого командування. Кібероперація може плануватися, як окремий вид бойових дій, так і у складі системи бойових дій. Основною метою кібероперації є підтримка політичних, економічних та інших зусиль, спрямованих на досягнення визначених цілей.

Основою планування кібероперації виступає:

− всебічне забезпечення стратегічних концепцій операцій в напрямку досягнення коаліційних, національних і стратегічних цілей на визначеному театрі воєнних дій (ТВД);

− забезпечення суворої процедури звітності при прийнятті управлінських рішень;

− досягнення єдності зусиль при проведенні повітряної, наземної, морської, космічної, спеціальної та інших операцій Збройних Сил та якісної взаємодії з міжвідомчими, неурядовими або приватними організаціями, а також з коаліційними силами та представниками міжнародних правозахисних організацій;

− узгодження мети кібероперації з цілями та задачами вищого командування;

− викриття спеціальних сил чи можливостей протиборчої сторони у визначеній зоні відповідальності;

− викриття переліку об'єктів з критичною інформаційною інфраструктурою протиборчої сторони і визначення шляхів їх знищення;

− визначення переліку власних об'єктів та об'єктів союзників з критичною

інформаційною інфраструктурою й організація заходів з їх кіберзахисту;

− встановлення порядку субординації і звітності про виконання кіберзаходів;

− надання зрозумілих даних підлеглим формуванням щодо цілі, мети, задач, сил та засобів здійснення кібероперації.

Забезпечення узгодження та інтеграції кібероперації у систему бойових операцій вимагає чіткого керівництва з боку вищого військового та політичного керівництва держави. Стратегія національної безпеки та національна військова стратегія, що формуються й орієнтовані на забезпечення національної безпеки держави, повинні забезпечувати стратегічне керівництво командувачам відповідних командувань. Командувачі бойовими Командуваннями реалізують стратегічні установки за допомогою своїх стратегій і планів щодо застосування Збройних Сил у взаємодії з різними установами та відомствами, а також коаліційними силами (союзниками). У ході планування командувачі бойовими Командуваннями й об'єднане Командування повинні всебічно оцінювати стратегічну обстановку і визначати всі її позитивні та негативні умови.

Об'єднане командування Збройних Сил повинно забезпечувати підпорядковані їм компоненти Збройних Сил усіма необхідними документами з планування. У цих документах має бути чітко визначено перелік кібердій, які повинні бути виконані обов'язково, а також перелік дій від яких слід утриматися або відмовитися. Крім того, в них повинні бути зазначені ті моменти з планування кібердій на які слід звернути увагу підлеглим самостійно, але у разі їх виконання порядок їх планування повинен відповідати усім встановленим процедурам та вимогам. У таких документах та інструкціях також обов'язково зазначаються межі планування кібероперації, визначаються суб'єкти та об'єкти кібервпливу.

Планування кібероперації вимагає суворого дотримання процедури прийняття рішень. Для планування більшості кібероперацій потрібен досить тривалий період часу, що обумовлений збором вихідних даних, а також узгодженням їх між собою. Для планування кібероперації, виходячи з досвіду кібернавчань, доцільно створювати відповідну групу з планування.

На групу з планування кібероперації слід покласти усі аспекти пов'язані з плануванням операції, у тому числі, й питання з організації забезпечення координації, інтеграції та взаємодії. Під час розробки плану кібероперації група з планування повинна здійснювати обмін інформацією між усіма членами групи за усіма напрямами з планування. На прикладі кібернавчань така взаємодія здійснювалася у формі семінарів, нарад, відеоконференцій тощо. До складу групи з планування слід включати представників усіх органів та підрозділів, задіяних у плануванні кібероперації в інтересах вищого Командування (об'єднаного Командування Збройних Сил).

Завчасне планування кібероперації та планування кібероперації в кризових ситуаціях мають суттєві відмінності, як за кількістю фаз проведення, так і за змістом задач планування на кожному з них (рис. 3.13, 3.14).

Суть етапів планування кібероперації (КбО) полягає в наступному.

На початковому етапі планування здійснюються такі заходи:

− моніторинг обстановки;

− огляд вказівок та оцінок;

− збір групи з планування кібероперації;

− оцінювання ролі й місця кібероперації у системі бойових дій;

− збір, узагальнення та аналіз інформації, що необхідної для планування.

Як результат формуються заявки на постановку задач та здобування необхідної інформації.

Під час уточнення задачі планування:

− визначаються конкретні та передбачувані завдання кібероперації;

− визначаються припущення, обмеження та стримуючі фактори;

− визначаються потреби у забезпеченні планування кібероперації.

Спільними рисами для обох алгоритмів планування кібероперації є етапи (рис. 3.15):

− подаються заявки на забезпечення відповідними вихідними даними для планування;

− розробляються критерії оцінювання ефективності задач планування;

− аналізується стан наявного ресурсного забезпечення;

− визначаються різні аспекти обстановки;

− уточнюються та подаються на затвердження вищому штабу пропозиції на постановку задач планування кібероперації.

Як результат, після другого етапу отримують перелік задач кібероперації, перелік пропозицій, стримуючих факторів та обмежень на планування кібероперації. Також отримують вказівки на планування кібероперації та уточнене формулювання задачі командувача на здійснення планування.

На третьому етапі розробляються різні варіанти дій:

− узгоджуються оцінки за різними варіантами;

− подаються результати оцінювання ризиків за кожним з варіантів дій.

У результаті виконання етапу отримують перелік цілей, що можна досягнути за кожним з варіантів кібероперації наявними засобами.

На наступному, четвертому етапі, аналізуються варіанти дій та здійснюється оцінювання їх ефективності:

− аналізується кожен варіант дій;

− визначаються основні пункти за якими досягаються цілі кібероперації;

− розробляються рекомендації на уточнення виконання задач кібероперації;

− визначається послідовність реалізації розроблених варіантів досягнення цілей кібероперації;

− визначаються найбільш важливі цілі кібероперації.

Заходи в об'єднаній системі оперативного планування та виконання	Дії групи з планування	Результати планування
1	2	3
Фаза 1		
Початковий етап	З'ясовує вимоги, що висуваються до планування	–
Фаза 2		
Розробка задуму операції		
Дія 1		
З'ясування задачі	Визначає потреби в інформаційному забезпеченні, необхідному для планування КбО	Постановка задач на збір і добування необхідної інформації
Дія 2		
Підготовка розпоряджень на організацію планування КбО	Надає допомогу у підготовці розпоряджень командувачу бойовими діями в частині, що стосується планування КбО	Розпорядження командувача на організацію планування КбО
Дія 3		
Проведення штабного оцінювання	Забезпечує проведення штабного оцінювання (розвідувальних даних, обстановки тощо) в частині, що стосується планування КбО	Штабні оцінки в частині, що стосується планування КбО
Дія 4		
Оцінювання обстановки командувачем	Готує дані для оцінювання обстановки командувачем в частині, що стосується планування КбО	Штабні оцінки в частині, що стосується планування КбО
Дія 5		
Визначення задуму КбО командувачем операції	Надає допомогу у підготовці задуму командувача в частині, що стосується КбО	Задум командувача на проведення КбО
Дія 6		
Затвердження задуму КбО командувача вищим штабом	Надання допомоги командувачу КбО у корекції задуму операції з урахуванням зауважень вищого штабу	Затверджений вищим штабом задум командувача операції на проведення КбО
Фаза 3		
Розробка плану КбО	Розробляє комплексний план КбО і елементи плану за кожним елементом КбО у взаємодії з відповідними підрозділами штаба, оперативними підрозділами і підрозділами підтримки	Проект додатку до плану КбО
Фаза 4		
Затвердження плану КбО командувача вищим штабом	Вносить зміни до плану КбО командувача з урахуванням зауважень вищого штабу	Затверджені додатки до плану КбО
Фаза 5		
Підготовка планів забезпечення КбО	Координує роботу та надає допомогу з підготовки підлеглими підрозділами та підрозділами підтримки планів забезпечення КбО	Плани забезпечення КбО

Рис. 3.13. Алгоритм завчасного планування кібероперації

Заходи в об'єднаній системі оперативного планування та виконання	Дії групи з планування	Результати планування
1	2	3
Фаза 1		
1	2	3
Оцінювання розвитку ситуації	Визначає потреби в інформаційному забезпеченні, необхідному для планування КбО відповідно до обстановки, що склалася	Постановка задач на збір і добування необхідної інформації
Фаза 2		
1	2	3
Оцінювання кризової ситуації	Уточнює потреби в інформації, що необхідна для планування відповідно до розвитку обстановки. Надає допомогу командувачу в розробці розпоряджень на планування КбО	Розпорядження командувача на організацію планування КбО. Установка взаємодії з підрозділами і організаціями, які можуть приймати участь у плануванні і проведенні КбО
Фаза 3		
1	2	3
Опрацювання варіантів дій	Дії групи такі самі, як і при проведенні штабного оцінювання при завчасному плануванні	Штабні оцінки
Фаза 4		
1	2	3
Вибір варіанта дій	Надання допомоги командувачу у виборі варіантів та дій і визначенні задуму КбО	Задум проведення КбО, затверджений вищим штабом
Фаза 5		
1	2	3
Планування операції	Розробляє комплексний план КбО і елементи плану за кожним елементом КбО у взаємодії з відповідними підрозділами штаба, оперативними підрозділами і підрозділами підтримки	Затверджені додатки до плану КбО
Фаза 6		
1	2	3
Виконання плану	Контроль за виконанням плану КбО і внесення у нього змін відповідно до кризової ситуації, що відбувається	Відкоригований план на КбО

Рис. 3.14. Алгоритм планування кібероперації в кризовій ситуації

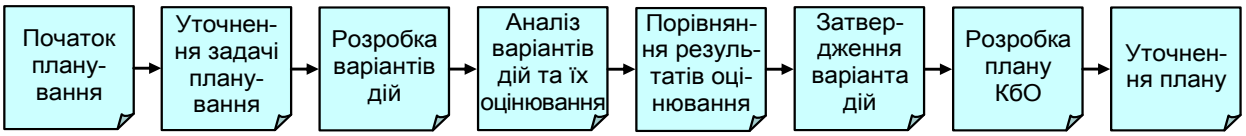

Рис. 3.15. Типові етапи планування кібероперації

Після четвертого етапу формулюють рекомендації для командувача кібероперації на планування кібероперації, порядок її проведення, перелік найважливіших цілей.

На п’ятому етапі відбувається порівняння результатів оцінювання, що передбачає:

− порівняння кожного варіанта дій у відношенні до загальної задачі бойової операції і задачі кібероперації;

− порівняння різних варіантів за потребою ресурсів та їх наявністю;

− встановлення пріоритетів на порядок виконання дій з точки зору досягнення мети кібероперації.

Як наслідок, на п’ятому етапі отримують систему пріоритетів на виконання кібероперації з урахуванням усіх позитивних та негативних сторін у результаті її проведення.

На шостому етапі відбувається процес затвердження варіанта дій. Серед усієї множини запропонованих варіантів обирається найкращий.

Як результат, на шостому етапі розробляється план кібероперації:

− уточнюються задачі кібероперації на основі затвердженого варіанта дій;

− визначення можливих недоліків та знаходження шляхів їх усунення;

− постійне уточнення та інформування усіх органів забезпечення, що розробляють допоміжні плани;

− інформування керівництва органів забезпечення щодо питань планування кібероперації про проблеми під час аналізу та затвердження допоміжних планів.

У результаті розробки плану кібероперації отримують уточнені оцінки ефективності заходів, що плануються у результаті проведення кібероперації за обраним варіантом дій. Також отримують проекти додатків з питань планування кібероперації і таблиці для обґрунтування планів.

На заключному, восьмому етапі планування уточнення до плану кібероперації вносяться адаптовано до критичної ситуації, що відбувається.

3.3. Планування операцій за стандартами НАТО

3.3.1. Загальні підходи до планування операції за стандартами НАТО

Завдання щодо впровадження стандартів НАТО у діяльність Міністерства оборони України та Збройних Сил України, інших складових сил оборони визначені законодавством (Закон України “Про національну безпеку України”) та стратегічними оборонними документами України (Стратегія національної безпеки України, Стратегічний оборонний бюлетень, Воєнна доктрина України тощо).

За планування відповідають визначені командири (начальники). Вони організовують та керують процесом планування, використовуючи свої знання, досвід та особисті якості під час взаємодії зі своїм штабом та підрозділами. У той час, коли штаби проводять більш детальний аналіз, готують плани та

накази, командири відіграють головну роль у плануванні, впроваджуючи їхній командирський задум, вимоги командира щодо надання важливої (критичної) інформації та вказівок щодо планування. Ці заходи є орієнтиром для активації роботи штабу та підпорядкованих командирів. Штаби допомагають командирам з координацією та детальним аналізом, необхідними для перетворення командирського задуму, вимог командира щодо надання важливої інформації, а також вказівок командира щодо планування у план або наказ.

Ефективне планування базується на концепції цільового управління (mission command). Цільове управління зосереджене на цілі операції, а не на кожній деталі, які забезпечують досягнення загальної мети. Робота під час цільового управління підпорядкованих командирів в усіх ешелонах, які проявляють розумну ініціативу в межах задуму командира, призводить до успішних результатів. Штаб ініціює роботу підпорядкованих командирів і штабів та підтримує їх, коли віддає бойове розпорядження. Бойові розпорядження – це інструмент для забезпечення виконання бойових наказів. Командування вищого рівня дає підлеглим максимальну свободу щодо планування та дій під час виконання завдань, залишає за ними право прийняття рішення – "яким чином" виконати завдання. Менш ефективним вважається планування, яке базується на використанні концепції детального управління (detail command).

Військові операції є невизначеними та непередбачуваними. Вони є комплексними намаганнями – боротьбою між протилежною людською волею. Командири стикаються із мислячим та адаптивним противником. Вони ніколи не можуть з певністю передбачити як буде діяти та протидіяти противник, або яким чином розвиватимуться події. Навіть дії своїх сил важко передбачити через такі фактори, як, наприклад, людські помилки та наслідки стресу. Командири, які розуміють динаміку змін у часі, враховуючи невизначеність щодо противника та своїх сил, краще пристосовані для розробки ефективних планів. З огляду на характер операцій, об'єктом планування є не усунення невизначеностей, а розробка основи дій серед них.

Повномасштабні операції вимагають гнучкого підходу до планування, який адаптує методи планування до кожної ситуації. Ефективний процес планування структурує мислення командирів і штабів, підтримуючи їх розуміння, творчість та ініціативу. Збройні Сили використовують три різні, але пов'язані з цим процеси, щоб керувати плануванням:

1. Вирішення проблем Збройних Сил.

2. Процес прийняття військового рішення (ППВР, англ. Military Decision-Making Process (MDMP)).

3. Керівні процедури підрозділів (КПП, англ. Troop Leading Procedures (TLP)).

Вирішення проблем Збройних Сил забезпечує стандартний, систематичний підхід до визначення та аналізу проблеми, розробляє та аналізує можливі рішення, вибирає найкраще рішення та реалізує план дій, який вирішує проблему. Вирішення проблем застосовується до всіх видів діяльності

Збройних Сил та забезпечує базову логіку для двох тактичних процесів, які використовуються Збройними Силами: ППВР/MDMP та КПП/TLP. ППВР/MDMP більш підходить для органу військового управління зі штабом. Це забезпечує логічну послідовність рішень та взаємодії між командиром та штабом для проведення оцінювання та розробки ефективних планів та наказів (розпоряджень). У нижчих тактичних ешелонах командири не мають штабів. Командири на рівні роти та нижче використовують КПП/TLP для планування та підготовки до операції.

Прийняття рішення – це вибір курсу, який є найбільш сприятливим для виконання завдання. Планування є формою прийняття рішень. Проте не всі рішення вимагають одного й того ж рівня планування. Командири приймають сотні рішень під час операцій в умовах великої невизначеності, непередбачуваності та постійних змін. Деякі рішення є навмисними, використовуючи ППВР/MDMP й увесь штаб для створення розробленого у повному обсязі та письмового оформлення наказу. Часто командир приймає інші рішення дуже швидко, що призводить до розроблення лише фрагментарного наказу (FRAGO). Під час розробки планів командири зазвичай обирають між аналітичними або інтуїтивно зрозумілими засобами прийняття рішень.

Процес прийняття військового рішення – це модель планування, яка встановлює процедури аналізу завдання, розробку, аналіз та порівняння варіантів дій за визначеними критеріями, вибір оптимального варіанта дій та розробку плану або наказу. ППВР/MDMP застосовується у всьому спектрі конфліктів і ряду військових операцій. Командири зі штабом використовують ППВР/MDMP для організації своїх планових заходів, спільного розуміння завдання, задуму командира та розробки ефективних планів і розпоряджень. Командири відповідають за процес планування. Від початку до кінця їх особиста роль є визначальною. Вони дисциплінують особовий склад органу управління відповідно до вимог часу, методу планування, простоти та рівня деталізації. Вони також оптимізують документи, які розробляються у процесі ППВР/MDMP, щоб забезпечити їх відповідність обстановці та зрозумілість підлеглими. Командири роблять це візуалізуючи, описуючи та керуючи діями особового складу органу управління.

Зусилля штабу під час планування зосереджені на допомозі командиру приймати рішення та розробляти ефективні плани та накази. Колектив штабу робить це шляхом інтеграції інформації, отриманої з доктринальних документів, використовуючи свій досвід (компетенції). Начальник штабу (НШ) керує, координує роботу персоналу, підтримує дисципліну та забезпечує контроль якості. НШ повинен чітко розуміти керівництво та задум командира, оскільки вони контролюють весь процес. Він надає особовому складу штабу розрахунок часу, встановлює терміни і місця розташування, а також надає будь-які інструкції, необхідні для завершення розроблення плану.

ППВР/MDMP призначений для полегшення взаємодії командира, штабу та підлеглих штабів у процесі планування. Ця взаємодія дозволяє одночасно координувати зусилля, що підтримують гнучкість, ефективно використовувати

час і полегшує постійний обмін інформацією. Внутрішня взаємодія дозволяє персоналу отримувати вказівки від командира та вирішувати питання, коли вони виникають. Крім того, це дає змогу створити у штабі необхідну структуру для спільної роботи та складання узгодженого плану [23].

ППВР/MDMP складається з наступних 7 кроків:

Крок 1. Отримання завдання / Receipt of mission.

Вхідні дані:

− завдання, отримане від органу управління вищого рівня, або визначено командиром чи штабом.

Результат:

− попередні вказівки командира;

− попередній наказ.

Крок 2. Аналіз завдання / Mission analysis.

Вхідні дані:

− наказ/план вищого органу управління (ОУ);

− результати оцінювання району дій вищим ОУ;

− розрахунки зроблені штабом.

Результат:

− сформульоване завдання;

− попередній задум командира та вказівки щодо планування;

− попередні вимоги командира щодо надання важливої інформації;

− оновлені штабом розрахунки;

− попередні продукти щодо оцінювання району дій;

− попередній план розвідки;

− підготовчі переміщення.

Крок 3. Розробка варіантів способів дій / COA (course of action) development.

Вхідні дані:

− сформульоване завдання;

− початковий задум командира, вказівки щодо планування та вимоги щодо надання важливої інформації;

− оновлені штабом розрахунки;

− початкові продукти отримані у ході оцінювання району дій.

Результат:

− оновлені штабом розрахунки та продукти;

− описи та схеми варіантів дій;

− уточнені задум та вказівки командира щодо планування.

Крок 4. Аналіз варіантів способів дій (моделювання) / COA analysis.

Вхідні дані:

− оновлені задуми командира та вказівки щодо планування;

− варіанти дій противника;

− описи та схеми варіантів дій.

Результат:

− результати моделювання;

− шаблони підтримки рішення;

− розподіл сил та засобів;
− завдання підпорядкованим підрозділам;
− рекомендовані вимоги командира щодо надання важливої інформації.

Крок 5. Порівняння варіантів способів дій / COA comparison.

Вхідні дані:
− результати моделювання бою;
− критерії для порівняння.

Результат:
− матриця підтримки рішення.

Крок 6. Затвердження варіантів способів дій / COA approval.

Вхідні дані:
− матриця підтримки рішення.

Результат:
− затверджений варіант дій;
− уточнений задум командира;
− уточнені вимоги командира щодо надання важливої інформації;
− список важливих цілей.

Крок 7. Розроблення наказу /Orders production, dissemination, and transition.

Вхідні дані:
− затверджений варіант дій;
− оновлені задуми та вказівки командира;
− оновлені вимоги командира щодо надання важливої інформації.

Результат:
− операційний наказ.

Підготовка та виконання завдання, хоча вони не є частиною ППВР/MDMP, які показані, підкреслюють важливість безперервного планування протягом усього операційного процесу [23].

Під час планування та розробки варіантів дій можна використовувати метод CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability). Цей метод започаткували сили спеціальних операцій США під час вибору найкращих цілей для їх ураження або здійснення на них впливу протягом усього процесу планування визначення цілей та завдань.

У процесі врахування факторів впливу, цим факторам присвоюється чисельне значення, що вказує на бажаність атакувати ціль, при цьому *1* означає низьку бажаність і *10* – високу бажаність для відповідного фактора. Потім ці значення вводять в матрицю. Після присвоєння значень CARVER для кожної цілі або компонента, сума цих значень вказує на ціль чи компонент з найвищим значенням для атаки в межах замислу командира [24].

Критичність/Criticality: розрахунок важливості критичної уразливості (CV) загрози; першочерговий фактор, що враховується при визначенні критичної уразливості загрози як цілі. Уразливість є критично значимою, якщо вона впливає на здатність загрози проводити або підтримувати операції. Критичність залежить від кількох факторів, а саме від:

Часу. Як швидко бажана зміна поведінки цілі вплине на критичну потребу загрози?

Якості. Який відсоток критичної потреби (CR) загрози буде зменшено бажаною зміною в поведінці цілі?

Наслідків. Яким буде вплив на критичну потребу (CR) загрози?

Відносності. Яка кількість наявних там цілей? Яке їхнє розташування? Як визначається відносне значення бажаної зміни поведінки? Яким буде вплив на загальну критичну спроможність загрози?

Доступність/Accessibility. Визначення того, чи доступна критична уразливість для впливу дружніми силами в часі та просторі. Інакше кажучи, чи мають дружні сили ресурси та спроможність вплинути на критичну уразливість загрози?

Відновлюваність/Recuperability. Оцінка того, скільки зусиль, часу та ресурсів загроза повинна витратити на протидію впливу серії військово-інформаційних операцій/заходів (MISO) на поведінку цілі, якщо на критичну уразливість буде здійснено успішний вплив.

Уразливість/Vulnerability. Визначення того, чи мають дружні сили засоби або спроможність вплинути на критичну уразливість завдяки існуючим характеристикам, мотивам або умовам цілі. Масштаб критичної уразливості потребує порівняння з можливістю дружніх сил впливати на неї.

Вплив/Effect. Визначення ступеня досягнутого ефекту, якщо на критичну уразливість здійснено успішний вплив. Результат ураження цілі є мірою можливого військового, політичного, економічного, психологічного та соціологічного впливу на ціль та за її межами. Результат тісно пов'язаний з мірою критичності цілі. Можливі результати можуть бути спекулятивними і повинні бути позначені як такі. Результати однієї і тієї ж продукції чи дій військово-інформаційних операцій (MISO) можуть бути зовсім різними на тактичному, оперативному та стратегічному рівнях ведення воєнних дій.

Розпізнаваність/Recognizability. Визначення того, чи може критична важливість бути ідентифікованою дружніми силами під час операції, якщо вона буде обрана об'єктом впливу, а також визначення міри, до якої можна зібрати показники ураження.

За складовими складається матриця [23].

3.3.2. Методика планування операцій, які включають дії в кіберпросторі

Командир і штаб залучають до процесу планування операції офіцера з планування дій у кіберпросторі (EWO – electronic warfare officer (cyberspace planner)), який є експертом у галузі здійснення впливів у кіберпросторі. Залучення відповідного фахівця на початку планування виконання завдання дозволяє синхронізувати та інтегрувати ці дії з основною місією, її функціями та завданнями (рис. 3.16) [42, 43].

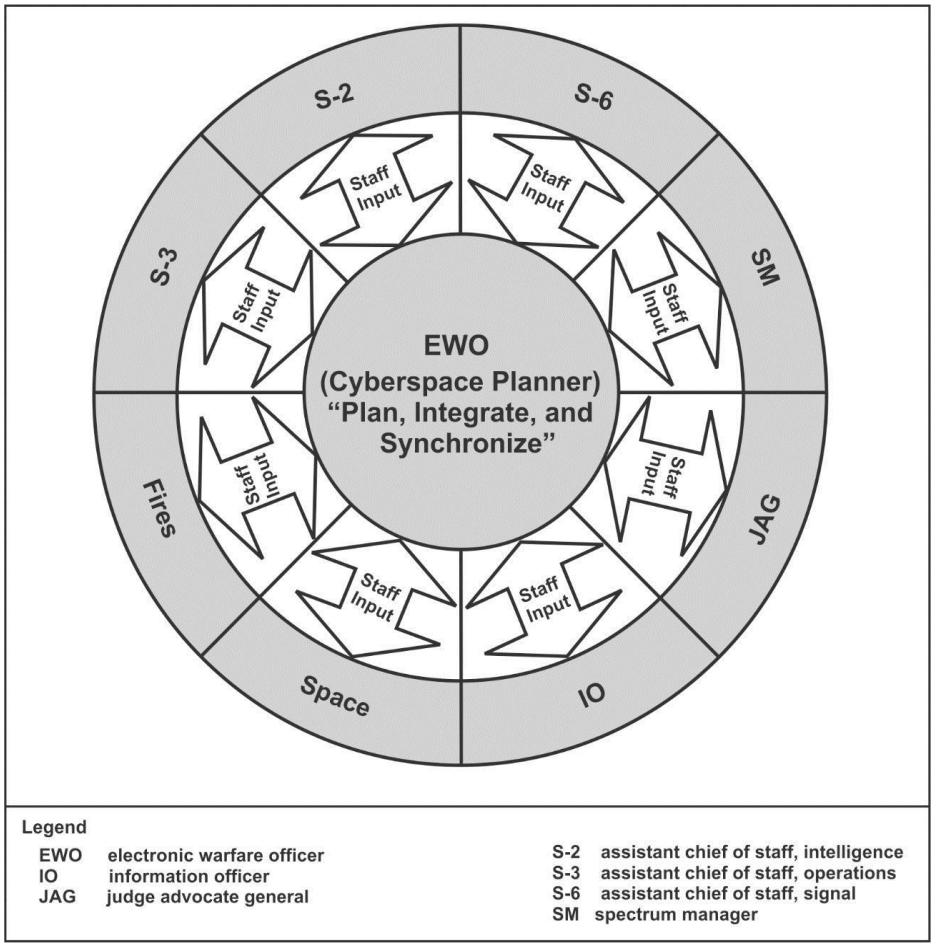

Рис. 3.16. Координація та синхронізація дій у кіберпросторі

Офіцер з планування дій у кіберпросторі (EWO) – офіцер штабу, призначений командиром, який відповідає за планування, інтеграцію, синхронізацію, оцінку та проведення операцій у кіберпросторі. Він співпрацює з іншими офіцерами штабу для інтеграції операції у кіберпросторі в концепцію операції командира. Як відповідальний за дії у кіберпросторі, EWO несе відповідальність за розуміння політики, що стосується кіберпростору, для надання точної інформації командувачу для належного планування, координації та синхронізації операцій у кіберпросторі.

Операційний простір (operational environment) – складається із умов, обставин та впливів, що обумовлюють застосування спроможностей та прийняття рішень командиром (composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander).

Розробка операційного простору передбачає критичне та творче мислення робочої групи для побудови моделей, що відображають поточні умови експлуатаційного середовища (поточний стан) та моделі, що має представляти операційне середовище при завершенні операції (бажаний кінцевий стан). Група планування, яка призначена командиром, визначає, аналізує та узагальнює характеристики операційних показників та розробляє бажані майбутні кінцеві стани, які планується досягти.

Обробка проблеми полягає в розумінні та ізоляції корінних причин конфлікту, обговорюваних та відображених в операційному середовищі. Дійові особи конфлікту можуть бути перешкодою для командирів, коли вони прагнуть досягти бажаних кінцевих результатів. Створення та використання можливостей кіберпростору формує умови в операційному середовищі, що підтримує завдання командира.

Процес прийняття рішення на проведення операції у кіберпросторі

Планування операцій у кіберпросторі інтегровано в програму ППВР/MDMP, циклічну методологію планування, що дозволяє зрозуміти ситуацію та ціль, розробити варіанти дій (COA – course of action) та скласти план відповідних дій. Командир і штаб інтегрують операції у кіберпросторі по всьому ППВР/MDMP. Їх порядок дій підтримуються схемою проведення операцій у кіберпросторі та відповідає вимогам щодо відповідності, доцільності та прийнятності. Персонал штабу, відповідальний за планування та інтеграцію операцій у кіберпросторі, бере участь у заходах ППВР/MDMP та в робочих групах CEMA (cyberspace electromagnetic activities / діяльність у кіберпросторі).

Основні завдання групи CEMA:

– чіткий розподіл повноважень на проведення дій у кіберпросторі;

– розуміння командним складом засад підготовки та ведення дій у кіберпросторі;

– інтеграція дій у кіберпросторі в операції військ (сил) на всіх ешелонах;

– широка координація та взаємодія на всіх ешелонах;

– потреба у підвищених / спеціальних заходах безпеки інформації;

– підготовка штабного персоналу та формування штабних елементів, що відповідають за діяльність у кіберпросторі.

Крок № 1. Отримання завдання

Командири розпочинають процес прийняття рішення після отримання чи очікування завдання операції. Службові особи штабу, відповідальні за планування та інтеграцію операцій в кіберпросторі, організовують взаємодію з вищими штабами для отримання інформації про поточні та майбутні операції в кіберпросторі, поточних показників та інших документів планування операцій в кіберпросторі.

Таблиця 3.1

Процес прийняття рішень, крок № 1: Отримання завдання

Вхідні дані	Необхідні дії	Вихідні дані
План або наказ вищого штабу. Інші планувальні документи вищого штабу, які включають поточну оцінку кіберпростору	Початок оцінки кіберпростору. Збір інструментів для підготовки до аналізу місії, які характерні для операцій в кіберпросторі. Забезпечення операції у кіберпросторі, яке увійде в попереднє розпорядження командира	Оновлена поточна оцінка кіберпростору

Крок № 2. Аналіз завдання

Командири та штаби аналізують завдання операції, щоб краще зрозуміти ситуацію та проблему, визначити, що команда повинна виконати, коли і де це потрібно зробити, і чому (мета операції). Персонал, відповідальний за планування та інтеграцію операцій у кіберпросторі, збирає, аналізує та синтезує інформацію про поточні умови експлуатаційного середовища з акцентом на кіберпростір та інформаційний простір.

Розвідувальна підготовка поля бою – це систематичний процес аналізу показників ворога, місцевості, погоди та цивільних міркувань у сферах, що являють інтерес, для визначення їх впливу на операцію. Розвідувальна підтримка операцій в кіберпросторі починається з інформаційної операції і продовжується протягом всього процесу ведення операцій.

Персонал, відповідальний за планування операцій у кіберпросторі, буде координувати роботу з представниками розвідки для визначення потенціалу противника та супротивника у кіберпросторі, щоб допомогти у розробці моделей, шаблонів ситуацій, шаблонів подій, важливих цілей та районів, які являють інтерес, та інших розвідувальних даних, що містять інформацію про кіберпростір ворога.

Таблиця 3.2

Процес прийняття рішень, крок № 2: Аналіз завдання

Вхідні дані	Необхідні дії	Вихідні дані
Початкове керівництво командира. Методика розробки проведення операції. Плани, накази вищого штабу та інші інформаційні документи	Аналіз вхідних даних та розробка інформаційних вимог. Участь у підготовці розвідки поля-бою. Визначення важливих цілей. Визначення слабких сторін ворога, своїх військ та нейтральних. Визначення конкретних, передбачуваних та важливих завдання операції у кіберпросторі. Визначення обмежень під час проведення операції. Визначення фактів та припущень у кіберпросторі. Визначення критичних інформаційних вимог командувача, пов'язані з кіберпростором. Визначення критичної інформації про кіберпростір. Нанесення даних на оверлей. Участь в аналізі	Список вимог щодо інформаційного забезпечення кіберпростору. Підготовка до розвідки поля бою в інтересах проведення операції в кіберпросторі. Ймовірні й самі небезпечні дії противника. Список конкретних та передбачуваних завдань операції в кіберпросторі. Обмеження при активних діях в кіберпросторі. Перелік припущень при активних діях в кіберпросторі. Актуальна поточна оцінка кіберпростору

Крок № 3. Розробка варіантів способів дій

Розробка варіантів способів дій створює варіанти для подальшого аналізу та їх порівняння так, щоб задовольнити наміри командира та керівництво з планування. Персонал штабу, відповідальний за планування та інтеграцію операцій в кіберпросторі, застосовує знання, отримані на етапі аналізу операції, щоб допомогти в розробці спільних варіантів способів дій. Під час розробки

варіантів способів дій співробітники, відповідальні за планування, розробляють початкову схему операцій в кіберпросторі, що складаються із задач підтримки дій у кіберпросторі. Схема операцій в кіберпросторі описує, як командир має намір використовувати операції у кіберпросторі для підтримки концепції операцій з акцентом на схемі маневру. Після розробки варіантів способів дій необхідно оновлювати багато результатів аналізу операції, а саме стан кіберпростору та іншої інформації, яка може надходити від союзників.

Таблиця 3.3

Процес прийняття рішень, крок № 3: Розробка варіантів способів дій

Вхідні дані	Необхідні дії	Вихідні дані
Початкове керівництво командира, завдання операції та наміри командира. Вимоги командира щодо інформаційного забезпечення операції. Оновлені розвідувальні дані поля-бою. Актуальна оцінка кіберпростору. Плани, накази вищого штабу та інші документи	Розробка вимог до інформації для плану збору інформації. Інтеграція та синхронізація операції у кіберпросторі у схему маневру та в загальну концепцію операції. Аналіз важливих цілей та відпрацювання їх переліку. Нанесення даних кіберпростору на оверлей. Розробка початкової схеми операцій в кіберпросторі. Надання даних щодо проведення операції для розробки спільних варіантів способів дій. Розробка формату запитів кібервпливів. Надання формату запитів кібервпливів	Оновлений перелік вимог щодо інформаційного забезпечення кіберпростору. Актуальна поточна оцінка кіберпростору. Перелік важливих цілей. Проект схеми операцій в кіберпросторі, включаючи цілі та наслідки

Крок № 4. Аналіз варіантів способів дій

Аналіз СОА дозволяє командирам та штабам визначити труднощі або проблеми координації, а також можливі наслідки запланованих дій для кожної розглянутої дії. Персонал штабу, відповідальний за планування та інтеграцію операцій, використовує ці проекти від розробки дій до їх аналізу. Під час аналізу дій вони вдосконалюють свою схему операції у кіберпросторі у відповідності зі схемою маневру.

Таблиця 3.4

Процес прийняття рішень, крок № 4: Аналіз варіантів способів дій

Вхідні дані	Необхідні дії	Вихідні дані
Оновлене початкове керівництво командира. Перелік важливих цілей у кіберпросторі. Проект схеми операцій в кіберпросторі. Актуальна оцінка кіберпростору. Плани, накази вищого	Залучення на брифінг з військової гри. Розробка формату запитів кібервпливів. Надання формату запитів кібервпливів. Доопрацювання схеми операцій в кіберпросторі Надання даних щодо	Доопрацьований перелік критичних інформаційних вимог командира. Доопрацьований перелік важливих цілей. Доопрацьована схема операцій в кіберпросторі. Актуальна поточна оцінка кіберпростору

штабу та інші інформаційні документи. Відгук від наданих форматів запитів кібервпливів	проведення операції у кіберпросторі для розробки матриці підтримки прийняття рішень та шаблону підтримки прийняття рішень. Нанесення даних операції у кіберпросторі на загальний оверлей	

Крок № 5. Порівняння варіантів способів дій

Порівняння порядку дій – це об'єктивний процес для оцінки кожної дії незалежно та від установлених критеріїв оцінки, затверджених командиром та штабом. Персонал штабу, відповідальний за операції в кіберпросторі, не може безпосередньо брати участь у цьому процесі, але може надавати рекомендації для розгляду під час порівняння. Після завершення порівняння, вихідні дані та основний наказ на проведення операції стають остаточним проектом.

Таблиця 3.5

Процес прийняття рішень, крок № 5: Порівняння варіантів способів дій

Вхідні дані	Необхідні дії	Вихідні дані
Результати військової гри. Доопрацьований перелік критичних інформаційних вимог командира. Доопрацьований перелік важливих цілей. Доопрацьована схема операцій в кіберпросторі. Актуальна поточна оцінка кіберпростору. Відгук від наданих форматів запитів кібервпливів	Залучення на брифінг з військової гри. Розробка формату запитів кібервпливів. Представлення формату запитів кібервпливів. Доопрацювання схеми операцій в кіберпросторі. Надання даних щодо проведення операції у кіберпросторі для розробки матриці підтримки прийняття рішень та шаблону підтримки прийняття рішень. Нанесення даних операції у кіберпросторі на загальний оверлей	Доопрацьований перелік критичних інформаційних вимог командира. Доопрацьований перелік важливих цілей. Доопрацьована схема операцій в кіберпросторі. Актуальна поточна оцінка кіберпростору

Крок № 6. Затвердження варіантів способів дій

Під час схвалення COA командир вибирає тільки дії для найкращого виконання операції. Найкращий варіант способів дій повинен бути етичним та найбільш ефективним. Командир видає остаточні вказівки з планування, включаючи наміри командира, вимоги до критичної інформації командира та будь-які інші додаткові вказівки для досягнення поставленої мети.

Таблиця 3.6

Процес прийняття рішень, крок № 6: Затвердження варіантів способів дій

Вхідні дані	Необхідні дії	Вихідні дані
Оновлена оцінка кіберпростору, яка включає продукти для кожної дії. Оцінений перелік дій. Рекомендований курс дій. Плани, накази вищого штабу та інші інформаційні документи. Відгук від наданих форматів запитів кібервпливів	Отримати та відповісти на остаточні вказівки командира. Оцінка наслідків та перегляд дій. Завершення та надання формату запитів кібервпливів. Завершення схеми операцій в кіберпросторі	Затверджений командиром варіант способів дій. Остаточна наступальна (оборонна) операція у кіберпросторі. Остаточна кібератака (оборона). Остаточний проект підтримки РЕБ. Схеми операцій у кіберпросторі. Визначені цілі у кіберпросторі. Оновлена підготовка розвідки поля-бою в інтересах проведення операції у кіберпросторі

Крок № 7. Підготовка наказів, їх доведення та перехід до дій

Кінцевим кроком процесу планування є відпрацювання наказів, їх доведення та перехід до дій. Всі підготовлені плануючі документи повинні мати оцінку кіберпростору та формат запитів кібервпливів. З часом, персонал може проводити більш детальну військову гру обраної дії. Вихідні дані за результатами гри повинні бути узгоджені і схвалені командувачем.

Таблиця 3.7

Процес прийняття рішень, крок № 7: Підготовка наказів, їх доведення та перехід до дій

Вхідні дані	Необхідні дії	Вихідні дані
Затверджений командувачем варіант способів дій та всі його зміни. Затверджені накази. Плани, накази вищого штабу та інші інформаційні документи. Відгук від наданих форматів запитів кібервпливів	Участь у погодженні та зміні планів штабом. Участь у плануванні взаємодії. Надання даних в остаточну оцінку ризиків у кіберпросторі. Завершення та надання формату запитів кібервпливів. Завершення та надання оцінки ефективності формату запитів. Відпрацювання наказів. Брати участь у нарадах та інструктажах	Затверджений командувачем варіант способів дій. Остаточна наступальна (оборонна) операція у кіберпросторі. Остаточна кібератака (оборона). Остаточний проект підтримки РЕБ. Схеми операцій в кіберпросторі. Визначені цілі в кіберпросторі. Оновлена підготовка розвідки поля-бою в інтересах проведення операції у кіберпросторі

Отже, планування є одним із чотирьох основних етапів виконання операції, що відбувається під час процесу прийняття рішення (планування, підготовка, виконання та оцінка). Командири застосовують оперативне мистецтво та науку,

щоб забезпечити виконання завдань основної операції, у тому числі й у кіберпросторі.

Методологія розробки проведення операції є методологією застосування критичного та творчого мислення для розуміння, візуалізації та опису незнайомих проблем та підходів для їх вирішення. Беручи до уваги унікальний та складний характер кіберпростору, командири та штаби отримують перевагу від впровадження даної методики, що, у свою чергу, дозволяє більш детально спланувати заходи під час планування операції. Це передбачає формування операційного середовища, формулювання проблеми та розроблення оперативного підходу до її вирішення [42, 43].

3.4. Оцінки інформаційних ризиків та управління ними

3.4.1. Способи оцінки інформаційних ризиків

Порушення основних властивостей інформації може стати серйозною загрозою для організацій в даний час. Інформацію важче контролювати і вона піддається зростаючому числу загроз й уразливостей, в тому числі комп'ютерного шахрайства, шпигунства, саботажу, вандалізму, пожежі або повені тощо. Інформаційні ресурси, як і матеріальні, володіють якістю та кількістю, мають собівартість і ціну. Оцінка ризиків є важливою частиною будь-якого процесу інформаційної безпеки. Її використовують для визначення масштабу загроз безпеці інформації та ймовірності реалізації загрози.

Процес оцінки ризику оцінює ймовірність і потенційний збиток від виявлених загроз, заходи індивідуального рівня ризику кожного інформаційного активу і як вони ставляться до конфіденційності, цілісності та доступності. Потім вимірюється ефективність існуючих заходів. Результати допомагають організації визначити, які активи є найбільш критичними, служать основою для визначення пріоритетів і рекомендують курс дій для захисту активів.

Існує безліч способів оцінки інформаційного ризику, розглянемо класифікацію існуючих методів і засобів оцінки інформаційних ризиків.

Оцінка ризику – це процес, який використовується для присвоєння значень наслідків, ймовірності виникнення та рівня ризику.

Вона включає у себе:

1) оцінку ймовірності загроз й уразливостей, які можливі;

2) розрахунок впливу, який може мати загроза на кожен актив;

3) визначення кількісної (вимірної) або якісної (описуваної) вартості ризику.

Треба взяти до уваги те, що ці три змінні майже завжди залежать одна від одної. В області інформаційної безпеки є зв’язок між вартістю активів, впливом і ймовірністю. Наприклад, більш імовірно, що хакер буде використовувати уразливість, яка викликає більший вплив, ніж уразливість з низьким рівнем впливу. Крім того, цінний актив має більшу імовірність компроментації, ніж марний. Таким чином, у цій області повинно прийматися до уваги більше, ніж просто випадкові дії. Необхідно брати до уваги, що за наявності достатнього

часу і рішучості, люди мають можливість обійти майже всі заходи безпеки. Вони можуть бути надзвичайно творчими, коли мотивовані. Таким чином, фактор мотивації повинен бути серйозно розглянутий в процесі оцінки безпеки інформаційного ризику.

На рис. 3.17 показані три способи, за допомогою яких можна проводити оцінку інформаційних ризиків:

1) методи;
2) управляючі документи;
3) інструменти.

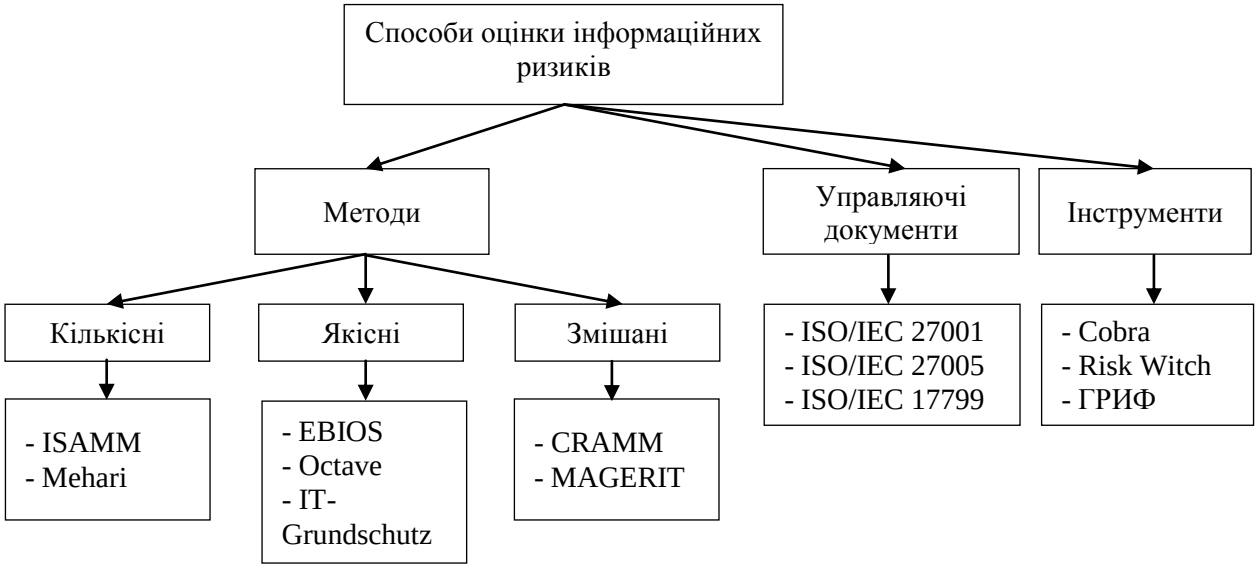

Рис. 3.17. Способи інформаційних ризиків

Розглянемо більш детально кожний.

1. Методи. Метод – це систематизована сукупність кроків, дій, які необхідно зробити для вирішення певної задачі або досягти поставленої мети, в даному випадку провести оцінку ризиків. Тобто метод – це покрокова інструкція плюс інструмент (програмний продукт) для проведення оцінки ризиків в організації.

Всі методи оцінки ризику можна поділити на кількісні, якісні або комбінацію кількісних методів з якісними (змішані).

Кількісні методи використовують вимірні, об'єктивні дані для визначення вартості активів, імовірність втрати і пов'язаних з ними ризиків.

Мета полягає в тому, щоб обчислити числові значення для кожного з компонентів, зібраних у ході оцінки ризиків та аналізу витрат і переваг.

Якісні методи використовують відносний показник ризику або вартості активу на основі рейтингу або поділ на категорії, такі як "низький, середній, високий", "не важливо, важливо, дуже важливо або "за шкалою від 1 до 10". Якісна модель оцінює дії й імовірності виявлених ризиків швидким й економічно ефективним способом. Набори ризиків записані і проаналізовані в якісній оцінці ризику та можуть послужити основою для цілеспрямованої кількісної оцінки.

Раніше кількісні підходи використовувалися частіше. Однак останнім часом використання суворо кількісних управлінь ризиками зазвичай призводить до важкої, тривалої роботи, і немає великих переваг перед якісним методом оцінки ризиків. Комбінація кількісного і якісного методу являє собою змішану сукупність переваг і недоліків вищезгаданих методів.

Далі розглянемо кращі світові методи для проведення повноцінної оцінки ризиків.

ISAMM (виробник: Бельгія) – кількісний метод, який був розроблений на основі Telindus. Це кількісний тип методології управління ризиками, де оцінюються ризики, які виражаються через їх щорічні очікувані збитки у грошових одиницях.

ISAMM дозволяє показувати й моделювати зниження ризику для кожного поліпшеного контролю і порівнювати з його вартістю реалізації. Ефективність методу дозволяє виконувати обґрунтовану оцінку ризику в рамках з мінімальними витратами часу і зусиль. Останньою еволюцією в методології ISAMM є надання активів. Це означає, що він може бути використаний для запуску оцінки ризиків щодо активів або згрупувати набір активів. Цей метод оцінки ризиків складається з трьох основних частин: огляд; оцінка; результат розрахунків та звітність. Немає допоміжних програмних інструментів, але має хорошу керівну документацію.

Mehari (виробник: Франція) – метод, в основі якого лежить модель управління ризиками з модульними компонентами і процесами. Модуль оцінки охоплює, крім інформаційної системи, організацію та її місця розташування в цілому, а також умови роботи, правові та нормативні аспекти. Даний метод відноситься і до якісного, і до кількісного. Має допоміжний програмний інструмент.

EBIOS (виробник: Франція) – якісний метод, який має повний набір посібників. Розроблені кращі практики, а також додатки документів, орієнтовані на кінцевих користувачів у різних контекстах. Цей метод широко використовується, як в державному, так і приватному секторах. EBIOS формалізує підхід до оцінки ризику в області інформаційної безпеки систем. Метод враховує всі технічні об'єкти (програмне й апаратне забезпечення, мережі) і нетехнічні об'єкти (організації, людські аспекти, фізична безпека). Має допоміжні програмні інструменти.

Octave (виробник: США) – якісний метод, який є самостійним підходом і вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації. OCTAVE вимагає аналізу в розгляді відносини між критично важливими активами, загрозами для цих активів й уразливостями (як організаційними, так і технологічними). Він визначає пов’язані з інформацією активи, які важливі для організації, і зосереджує діяльність на ці активи, тому що вони мають найбільш важливе значення для організації (акцент на кілька важливих активів, але не більше п'яти). Існують різні OCTAVE методи, засновані на OCTAVE критеріях: OCTAVE, OCTAVE-S і OCTAVE Allegro. Має допоміжні програмні інструменти.

IT-Grundschutz (виробник: Німеччина) – якісний метод, який пропонує спосіб для створення системи управління інформаційною безпекою. Вона

включає у себе, як загальні рекомендації з забезпечення безпеки ІТ, так і допоміжні технічні рекомендації для досягнення необхідного рівня ІТ безпеки для конкретного домену.

У методі IT-Grundschutz надані каталоги: 1) модулі; 2) каталоги загроз; 3) каталоги захисту. Має допоміжні програмні інструменти.

CRAMM (виробник: Великобританія) – змішаний метод, який досить складно використовувати без CRAMM інструмента. В інструмента така сама назва, як і у методу – CRAMM. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектору. Грамотне використання методу CRAMM дозволяє отримувати дуже хороші результати, найбільш важливим з яких є можливість економічного обґрунтування витрат організації на забезпечення інформаційної безпеки та безперервності бізнесу. Економічно обґрунтована стратегія управління ризиками дозволяє, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат. Має допоміжні програмні інструменти.

Процедура аудиту в методі CRAMM є формалізованою. На кожному етапі генерується досить значна кількість проміжних і результуючих звітів.

Так, *на першому етапі* створюються наступні види звітів:

− модель ресурсів, що містить опис ресурсів, які потрапляють у межі дослідження, і взаємозв’язків між ними;

− оцінка критичності ресурсів;

− результуючий звіт за першим етапом аналізу ризиків, у якому підсумовуються результати, отримані в ході обстеження.

На *другому етапі* проведення обстеження створюються наступні види звітів:

− результати оцінки рівня загроз й уразливостей;

− результати оцінки величини ризиків;

− результуючий звіт за другим етапом аналізу ризиків.

За результатами *третього етапу* обстеження створюються наступні види звітів:

− рекомендовані контрзаходи;

− детальна специфікація безпеки;

− оцінка вартості рекомендованих контрзаходів;

− список контрзаходів, відсортований відповідно до їх пріоритетів;

− результуючий звіт за третім етапом обстеження;

− політика безпеки, що включає опис вимог безпеки, стратегій і принципів захисту ІС;

− список заходів з забезпечення безпеки.

Правильно застосовувати метод CRAMM у змозі тільки висококваліфікований аудитор, що пройшов навчання. Якщо організація не може собі дозволити мати у штаті такого фахівця, тоді найправильнішим рішенням буде запросити аудиторську фірму, що має в розпорядженні штат фахівців, які мають практичний досвід застосування методу CRAMM.

Узагальнюючи практичний досвід використання методу CRAMM при проведенні аудиту безпеки, можна зробити наступні висновки відносно сильних і слабких сторін цього методу.

До сильних сторін методу CRAMM відноситься наступне:

− CRAMM є добре структурованим і широко випробуваним методом аналізу ризиків, що дозволяє отримувати реальні практичні результати;

− програмний інструментарій CRAMM може використовуватися на всіх стадіях проведення аудиту безпеки інформаційної системи (ІС);

− в основі програмного продукту лежить досить об'ємна база знань з контрзаходів в області інформаційної безпеки, що базується на рекомендаціях стандарту BS 7799;

− гнучкість і універсальність методу CRAMM дозволяє використати його для аудиту ІС будь-якого рівня складності і призначення;

− CRAMM можна використати як інструмент для розробки плану безперервності бізнесу і політики інформаційної безпеки організації;

− CRAMM може використовуватися як засіб документування механізмів безпеки ІС.

До недоліків методу CRAMM можна віднести наступне:

− використання методу CRAMM вимагає спеціальної підготовки і високої кваліфікації аудитора;

− CRAMM набагато більшою мірою підходить для аудиту вже існуючих ІС, таких, що знаходяться на стадії експлуатації, ніж для ІС, що знаходяться на стадії розробки;

− аудит за методом CRAMM – процес досить трудомісткий і може потребувати місяців безперервної роботи аудитора;

− програмний інструментарій CRAMM генерує значну кількість паперової документації, яка не завжди виявляється корисною на практиці;

− CRAMM не дозволяє створювати власні шаблони звітів або модифікувати наявні;

− можливість внесення доповнень у базу знань CRAMM не доступна користувачам, що викликає певні труднощі при адаптації цього методу до потреб конкретної організації.

Magerit (виробник: Іспанія) – змішаний метод, який є відкритою методологією аналізу та управління ризиками пропонованою в якості основи і керівництва:

− для того, щоб особи відповідальні за інформаційні системи, знали про існування ризиків і необхідність розглядати їх своєчасно;

− для пропозиції систематичного методу аналізу цих ризиків;

− для опису і планування відповідних заходів з утримання ризику під контролем;

− для підготовки організації з процесу оцінки, аудиту, сертифікації та акредитації.

Має допоміжні програмні інструменти.

2. Управляючі документи. Крім методів оцінки ризиків використовують управляючі документи, де теоретично описуються і даються методичні вказівки

процесу оцінки ризиків, але не дається конкретних технологій. Найвідоміші стандарти, які використовуються на території України: ISO 27001, ISO 27005, ISO 17799.

ISO/IEC 27001. Міжнародний стандарт ISO/IEC 27001 визначає процеси, що дає можливість бізнесу встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему менеджменту інформаційної безпеки. У даному стандарті регламентовані вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки в контексті існуючих бізнес-ризиків організації. Зазначені вимоги реалізуються в рамках документованих процесів менеджменту інформаційної безпеки, структурованих за моделлю PDCA (Plan-Do-Check-Act). Стандарт ISO/IEC 27001 являє наочну модель менеджменту, що дозволяє здійснювати оцінку ризиків, проектування і реалізацію системи інформаційної безпеки, її менеджмент і переоцінку.

ISO/IEC 27005. Цей стандарт призначений для визначення в організації підходу до менеджменту ризиків в залежності, наприклад, від області дії СМІБ, області застосування менеджменту ризиків або сектору промисловості. Забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації. Стандарт підтримує загальні концепції, визначені в ISO/IEC 27001, і призначений для сприяння адекватного забезпечення інформаційної безпеки на основі підходу, пов’язаного з менеджментом ризику. Застосовується для організацій усіх типів (наприклад, комерційних підприємств, державних установ, некомерційних організацій), які планують здійснювати менеджмент ризиків, для компрометації інформаційної безпеки організації.

ISO/IEC 17799. У відповідності зі стандартом ISO 17799, при створенні ефективної системи безпеки особливу увагу слід приділити комплексному підходу до управління інформаційною безпекою. З цих причин як елементи управління розглядаються не тільки технічні, але й організаційно-адміністративні заходи, спрямовані на забезпечення наступних вимог до інформації: 1) конфіденційність; 2) цілісність; 3) достовірність; 4) доступність.

Порушення кожного з них може спричинити за собою значні втрати, як у вигляді збитків, так і у вигляді неотриманого доходу.

3. Інструменти. Крім методів та управляючих документів використовують інструменти для оцінки ризиків. Інструменти являють собою програмне забезпечення з документацією про правила використання. Найвідомішими інструментами, існуючими без методики з покроковою інструкцією, є: Cobra, RiskWatch.

Cobra (виробник: Великобританія) – програмний інструмент, який дозволяє проводити оцінку ризиків у галузі безпеки. Він оцінює відносну важливість усіх загроз й уразливостей, генерує відповідні рішення та рекомендації. Це автоматично пов'язує виявлені ризики з потенційними наслідками для бізнес-одиниці. Крім того, конкретний район або питання може бути розглянуте "самостійно", без будь-яких наслідків для організації.

RiskWatch (виробник: США) – являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів. У RiskWatch як критерії для оцінки та управління ризиками використовуються очікувані річні втрати (Annual Loss Expectancy, ALE) та оцінка повернення інвестицій (Return on Investment, ROI). RiskWatch орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і затрат на створення системи захисту.

Аудит є незалежною експертизою окремих областей функціонування організації, що проводиться за ініціативою її керівництва або акціонерів, або відповідно до плану проведення внутрішнього аудиту. Основними цілями проведення аудиту безпеки є:

− аналіз ризиків, пов’язаних з можливістю здійснення загроз безпеки відносно ресурсів ІС;

− оцінка поточного рівня захищеності ІС;

− локалізація вузьких місць у системі захисту ІС;

− оцінка відповідності ІС існуючим стандартам в області інформаційної безпеки;

− вироблення рекомендацій з впровадження нових і підвищення ефективності існуючих механізмів безпеки ІС.

Роботи з аудиту безпеки ІС включають низку послідовних етапів:

− ініціація обстеження;

− збір інформації;

− аналіз отриманих даних;

− вироблення рекомендацій;

− підготовка звіту за результатами обстеження;

− підходи до проведення аудиту безпеки можуть базуватися на аналізі ризиків, спиратися на використання стандартів інформаційної безпеки, або об'єднувати обидва ці підходи.

3.4.2. Сучасні підходи до оцінки ризиків інформаційних технологій

Управління ризиками кібербезпеки є одним із компонентів управління ризиками установи й особливо важливо в організаціях і підприємствах, які значною мірою залежать від мереж і систем інформаційних технологій (IT) для їх діяльності.

Управління ризиками – це процес виявлення уразливостей і загроз інформаційних ресурсів, що використовуються організацією для досягнення цілей і прийняття рішень про те, які контрзаходи, якщо такі є, повинні приймати по зниженню ризику до прийнятного рівня на основі цінності інформаційного ресурсу для організації.

Основні підходи до управління ризиками інформаційних технологій ґрунтуються на:

− стандарті управління та аудиту інформаційних технологій Cobit v.4.1;
− настановах по управлінню ризиками в інформаційних технологіях NIST 800-30;
− настановах по управлінню ризиками ISO 3100 (вводяться);
− стандарті управління інформаційною безпекою ISO 27005;
− стандарті управління ризиками AS/NZS 4360:2005.

Методика оцінки ризиків NIST

Стандарт США NIST 800-30 "Керівництво з інформаційними ризиками IT-систем" – керівництво з аналізу та управління ризиками був розроблений Лабораторією інформаційної технології (ITL) Національного інституту стандартів і технології (NIST) США і надані рекомендації в керівництві з аналізу та управління ризиками.

Відповідно до NIST SP 800-30 Методологія оцінки ризику охоплює дев'ять основних етапів (рис. 3.18): характеристика системи; ідентифікація загроз; ідентифікація уразливості; аналіз заходів захисту; визначення правдоподібності; аналіз впливу; визначення ризиків; рекомендації до заходів захисту; документація результатів.

У кожному етапі на основі логіки зв'язків з певної вхідної інформації виходить вихідна [47].

Методика оцінки ризиків FAIR

FAIR (факторний аналіз інформаційних ризиків) – це міжнародний кількісний метод оцінки інформаційного ризика. Посилаючись на основні підходи до менеджменту інформаційними ризиками, що прописані у стандартах Cobit v.5.0, NIST SP 800-30, серій ISO/IEC 27000, методика факторного аналізу інформаційних ризиків FAIR передбачає найбільш повне урахування факторів виникнення інформаційних ризиків [48].

FAIR дозволяє отримати опис достатньої кількості факторів, що впливають на оцінку ризику та конкретні значення ризику, яким би могли оперувати керівники підприємств. Основою методики FAIR є аналіз факторів, що впливають безпосередньо на ризик. Аналізуються фактори, що мають вплив на компоненти, які є складовими ризику. Відповідно до зазначеної методики, головними складовими ризику є частота появи інциденту (LEF) та величина збитків від настання зазначеного інциденту (LM) [49]. Кожна із цих складових поділяється на інші фактори: частота появи загрози, уразливість, первинні та вторинні збитки. Відповідно до методики FAIR, основним принципом ефективного керування кіберризиками є кількісний аналіз ризиків.

Рамки FAIR визначають необхідні складові для реалізації ефективних програм управління кіберризиками. В основі будь-якої такої програми лежить здатність кількісно оцінювати кіберризики.

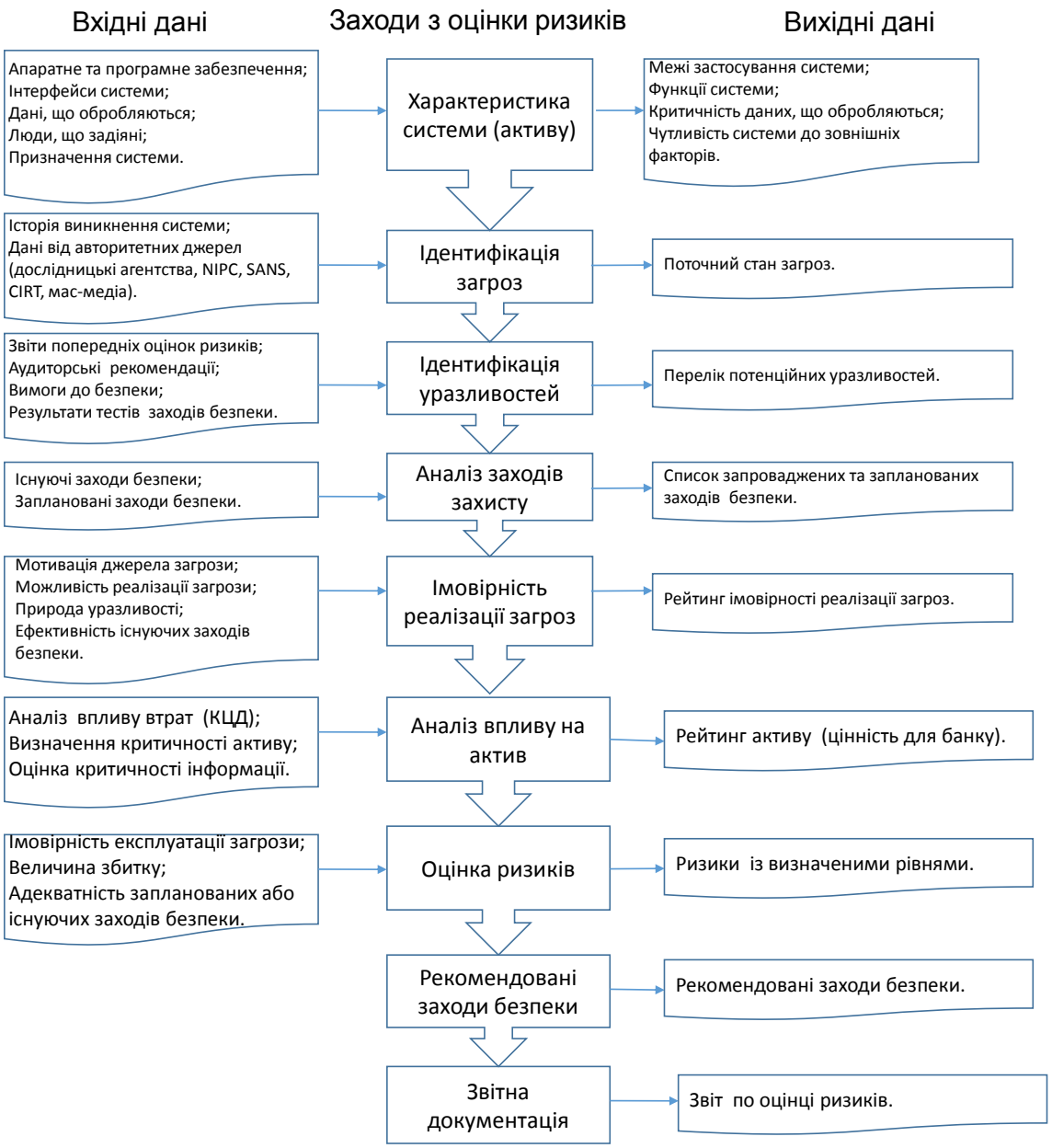

Рис. 3.18 Методологія оцінки ризиків NIST

Система управління ризиками FAIR складається з наступних елементів:

– ризик – функція загроз, активів, контролю та факторів впливу, які впливають на збитки;

– управління ризиками, що складається з прийняття рішень та їх виконання;

– цикл зворотного зв'язку – показники, пов'язані з інформацією про загрозу і збитки та дані аналізу основних ризиків.

Використання FAIR передбачає проведення декількох етапів.

Спочатку необхідно визначити область аналізу і що є його метою. Для точного аналізу важлива чітко визначена область. Першою метою є визначення сценаріїв ризику, оскільки це є основою для структурування подальшого належного аналізу. Для визначення сценарію необхідно: провести опис активу (ідентифікація об’єктів оцінки), загрози (частота появи інциденту) й ефекту

(стосовно конфіденційності/цілісності/доступності), пов'язаного з аналізованим сценарієм.

Тобто на першому етапі проводиться ідентифікація активів, загрози (з визначенням її групи та типу), оцінюється ефект загрози, що може бути застосований до інформаційної системи підприємства. Дані фіксуються в таблицю.

Наступний крок – оцінювання кожного зі сценаріїв. До цього етапу входять аналіз частоти появи загрози, існуючих уразливостей та кількісна оцінка факторів можливих збитків.

Частота появи загрози вимірюється з використанням факторів: “мінімальне значення”, “найбільш ймовірне значення” та “максимальне значення”.

Для оцінки найгіршого варіанта необхідно виконати наступні пункти:

– визначити дію загрози, яка напевно буде результатом найгіршого випадку;

– оцінити величину кожного виду втрат, пов’язаних з дією загрози;

– підсумувати величини всіх видів втрат.

Останнім етапом є розрахунок величини ризику, що відбувається через ідентифікацію сценарію з найвищим показником річних збитків. При розрахунку використовують метод Монте-Карло. Інтерпретація результатів проводиться відповідно до запропонованих таблиць методики.

Методика FAIR являє собою детальний аналіз та оцінку ризиків, отриманий результат має конкретні значення ризику, а отже чіткий та доступний для використання.

Аналіз та оцінка ризиків з використанням методу FAIR складається з чотирьох етапів, що містять десять кроків:

Етап I – Визначення сценаріїв

1. Визначити активи підприємства.
2. Визначити загрози активам, що розглядаються.

Етап II – Визначення частоти появи інциденту (LEF)

3. Оцінити частоту появи загрози (TEF)
4. Виявлення уразливостей (Vulnerability)
5. Оцінка сили загрози (TCap)
6. Оцінка ефективності контрзаходу (RS)
7. Отримання даних частоти появи інциденту (LEF)

Етап III – Оцінка величини збитків (LM)

8. Оцінка втрат від реалізації найгіршого сценарію
9. Оцінка найбільш ймовірних втрат

Етап IV – Визначення величини ризиків

10. Отримання вихідних даних

Слід зазначити, що для кожної загрози треба проводити процедуру аналізу спочатку.

Сучасні методи управління інформаційними ризиками дозволяють оцінити існуючий рівень залишкових інформаційних ризиків організацій. Це особливо важливо в тих випадках, коли до інформаційної системи застосовуються підвищені вимоги в галузі кібербезпеки та безпеки інформації.

3.5. Кіберзброя

3.5.1. Сутність та призначення кіберзброї

У сучасному високотехнологічному суспільстві класифікують такі види зброї – звичайна зброя (вогнепальна, холодна, пневматична та ін.), зброя масового ураження (ядерна, біологічна, хімічна) та нетрадиційна зброя, що базується на нових фізичних принципах (генетична, геофізична, інфразвукова та ін.). Але ще одним із ефективних засобів, який застосовується нині протиборчими сторонами для досягнення стратегічних та політичних цілей, є кіберзброя. Кіберзброя, як стверджується у статті "Nation state sponsored attacks: the offensive of Governments in cyberspace" (листопад 2012 року) головного технічного редактора журнала CyberDefense П. Паганіні, нині розробляється, досліджується та застосовується урядами близько 140 країн світу. Найбільших успіхів при цьому здобули такі країни, як США, Росія, Китай, Великобританія. Незважаючи на це, ні на регіональному, ні на міжнародному рівнях немає однозначного розуміння того, що ж саме слід розуміти під кіберзброєю та як потрібно здійснювати її класифікацію. Таким чином, знехтувати фактами того, що в першій декаді XXI століття на світовій військовій арені при вирішенні міждержавних та внутрішньодержавних конфліктів зароджується новий феномен – кіберзброя, виходить обумовити власну державу та її збройні сили й силові відомства до технологічної відсталості й залежності її від країн, які своєчасно, а інколи й на випередження розробляють нові форми та способи ведення воєн в кіберпросторі, у тому числі, й з використанням кіберзброї.

Термінологічна та правова невизначеність стосовно категорії "кіберзброя", що склалася на сьогодні у світовому масштабі, породжує перед високотехнологічним суспільством низку проблем, як організаційного, так і технологічного плану. З одного боку, це проблеми пов'язані з питаннями правової та політичної відповідальності тієї чи іншої держави у разі застосування нею кіберзброї, з іншого, – привід до розвитку нового витка гонки озброєнь, – кіберозброєнь.

З моменту першого виявлення 17 червня 2010 року вірусу *win32/Stuxnet* почався новий етап у розвитку сфери комп'ютерної вірусології – вірусології військового призначення. Пізніше (липень 2010 року), після ґрунтовного аналізу даного вірусу незалежними експертами, зроблено висновок, що ***дату 17 червня 2010 року можна офіційно вважати початком зародження нової віхи в історії зброї.*** Вперше у світі для досягнення стратегічних та політичних цілей державою, або групою держав проти іншої держави застосовано новітній зразок зброї – вірус *Stuxnet*, який справедливо можна віднести до нового виду зброї, яка отримала назву кібернетичної.

Очевидно причинами, що спонукали експертів до таких висновків були надзвичайна складність даного зразка зброї, розробити який без висококласних професіоналів з різних галузей та без належної державної фінансової підтримки, неможливо. Орієнтування даного зразка зброї на конкретну ціль – зрив технологічних процесів в автоматизованих системах управління

промисловими об'єктами Ірану також підтверджує справедливість даного висновку. При цьому, політичною метою, що переслідувалася державою (державами) розробниками вірусу *Stuxnet,* можна вважати дискредитацію правлячого режиму в Ірані, а стратегічною – зрив темпів виконання національної ядерної програми.

У світі, починаючи з 2012 року, спостерігається сплеск досліджень з питань формування нового науково-категоріального апарату, присвяченого тлумаченню дефініцій з приставкою *"кібер"*. Майже одночасно опубліковано низку праць відомими у світовому ІТ-товаристві експертами з кібербезпеки. Це праці:

"Cyber-weapons", опублікована в журналі *RUSI JOURNAL* за лютий/березень професором П. Макберні та його колегою доктором Т. Рідом з Лондонського королівського коледжу. У статті надаються аргументи того, що кіберзброя не може відноситися до класу справжньої зброї, оскільки за позицією авторів вона не спричиняє руйнівних наслідків для об'єктів на які здійснюється кібернапад. Автори стверджують, що чим складніше вірус, а саме програмний код розуміється ними під прототипом кіберзброї, тим глибше він спроможний проникнути у систему і тим менші побічні ефекти матимуть місце на об'єктах, які не є метою кібернападу. Спираючись на точковий ефект від застосування подібних інструментів, а як такі інструменти використовуються бот-мережі для організації DDoS-атак та відповідні програмні продукти з метою проведення кібердій щодо тимчасового порушення доступності інформаційних ресурсів протиборчої сторони, вони мають найменш небезпечний ефект для об'єктів кібернападу. По суті співавтори наголошують на тому, що на сьогодні складається парадоксальна ситуація, яка полягає в існуванні протиріччя між величиною вкладення інтелектуальних та фінансових ресурсів та ефектом, який наступає від застосування подібних інструментів. Тобто, чим більше ресурсів витрачається на розробку інструменту – тим ефект від його застосування менш помітний.

"Cyberweapons aspetti giuridici e strategici" (*у перекладі з італ.* "Кіберзброя – юридичні та стратегічні аспекти"), опублікована у квітні в працях Італійського інституту стратегічних досліджень "Нікколо Макіавеллі" доктором С. Меле. Ним було зазначено, що кіберзброя – це пристрій або комп'ютерна програма, які призначені для незаконного пошкодження комп'ютерних систем та телекомунікаційних мереж, що відносяться до кібернетичної інфраструктури та часткової або повної зміни усталених режимів їх роботи, що, як наслідок, призводить до припинення їх функціонування.

"Cyber-weapons" – доповідь зроблена в жовтні головним технічним редактором журналу *CyberDefense* – експертом з питань безпеки П. Паганіні на Міжнародному Самміті *Cyber Threat Summit 2012* в м. Дублін (Ірландія), який у кіберзброї вбачає пристрій, прилад або набір комп'ютерних команд, що призначені для нанесення шкоди людині через кіберпростір. Тобто, якщо виходити з наведених дефініцій – точки зору експертів розділися.

"Кибервойна и кибероружие", опублікована начальником відділу науково-освітніх розробок Управління інноваційного розвитку Московського

державного інституту міжнародних відносин Міністерства зовнішніх справ Російської Федерації В. Каберніком (грудень 2013 р., веб-сторінка Центру воєнно-політичних досліджень). Автор наголошує на типову помилку, яка припускається західними експертами при тлумаченні терміна «кіберзброя». Об'єктом, на який здійснюється вплив кіберзброєю за В. Каберніком, є кібернетична система, будь-то комп'ютерна система, автоматизована система управління технологічними процесами чи людина, як біологічна система, тобто будь-яка система зі зворотним зв'язком. При цьому наявність зворотного зв'язку у системі управління – це лише необхідна умова, а достатньою умовою залишається вимога щодо збереження керованості об'єкта кібервпливу та передбачуваність його реакцій на такий вплив.

Існують й інші підходи до визначення кіберзброї. Кіберзброю інколи визначають як інструмент кібершпигунства, який побудовано за модульним принципом. Держава власник такої зброї застосовує її, як правило, в наступальних цілях.

Не можна оминути увагою найновітніший і єдиний у світі документ, що регламентує закони ведення кібервійни – *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, який презентовано 5 березня 2013 року в м. Таллінн (Естонія). Дане керівництво підготовлене міжнародною групою з 20 експертів за редакцією професора М. Шмідта у співробітництві з НАТО, Кіберкомандуванням США та Міжнародним червоним хрестом. Встановлюючи міжнародні правила ведення кібервійни в керівництві розроблено 95 правил. Зокрема, у 41 із них зазначається визначення засобів та методів ведення кібервійни.

Кіберзброя – це засоби ведення кібервійни, які призначені для травмування або знищення противника, а також завдання шкоди функціонуванню його об'єктів, що дозволяє характеризувати заподіяні наслідки як факт кібернападу.

У більш вузькому сенсі в Талліннському керівництві стосовно кіберзброї зазначено таке.

Кіберзброя – це засоби ведення кібервійни та системи пов'язані з ними.

Засоби ведення кібервійни – це кіберзброя та системи кіберзброї (техніка, інструменти, механізми, обладнання, програмне забезпечення тощо – це все те, що розроблено та використовується для нанесення кібератак).

Особливий акцент у Талліннському керівництві зроблено на розділенні дефініцій "комп'ютерна система", яка може кваліфікуватися як засіб ведення кібервійни та "об'єкт з інформаційною інфраструктурою", що може бути об'єктом кіберагресії.

Особливістю даного документа є те, що він носить неофіційний характер. Він не прийнятий жодною державою та ніким не затверджений. Але знову ж таки, врахувавши замовника та його виконавців, висновки напрошуються самі собою. Дане керівництво з часом відіграє значну роль при формуванні основ політики стосовно питань кібербезпеки у більшості з розвинених країн світу, і час це покаже.

Отже, на сьогодні чітко можна спостерігати три основні підходи до розуміння кіберзброї (рис. 3.19).

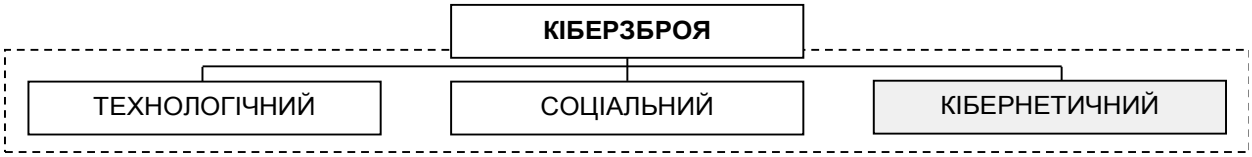

Рис. 3.19. Сучасні підходи до формування дефініції “кіберзброя”

Перший – це *технологічний підхід*. Він полягає у тлумаченні кіберзброї як суто набору технічних та програмних засобів, спрямованих на використання уразливостей у системах передачі, обробки й зберігання інформації. Другий – *соціальний*, що передбачає вплив на соціум через кіберпростір за допомогою приладів, пристроїв або наборів комп’ютерних команд. Тобто у першому випадку акценти розставляються на технологічній складовій, у другому – на соціальній. Третій, останній і по суті єдиний правильний підхід до тлумачення кіберзброї, полягає у розумінні її як засобу впливу на *кібернетичні системи* різної природи.

Третій підхід досить інтенсивно підтримується військовими аналітиками розвинених країн. Його дотримуються, в першу чергу, у військовій адміністрації США, про що відзначається в базових документах щодо побудови національної стратегії кібербезпеки та підтверджується гучними заявами американських генералів.

Зважаючи на вищевикладене, у рамках третього підходу дамо визначення категорії “кіберзброя”.

Кіберзброя – це набір технічних, програмних та інших засобів, спрямованих на порушення процесів управління в кіберпросторі, включаючи соціум, соціотехнічні системи, технічні системи (комп’ютерні системи та мережі, системи зв’язку та автоматизовані системи управління, управляючі елементи систем озброєння і військової техніки та небезпечних об’єктів і об’єктів з критичною інформаційною інфраструктурою, програмне забезпечення, бази даних тощо) у вигляді інформаційних, психологічних та різноманітних фізичних деструктивних впливів.

Ґрунтуючись на аналізі доступних наукових видань, присвячених проблематиці кібербезпеки, у самому загальному вигляді доцільно визначити, по-перше, перелік ознак кіберзброї; по-друге, основні завдання, що покладаються на кіберзброю та, по-третє, перелік можливих об’єктів ураження.

До характерних ознак кіберзброї віднесемо:

− спрямованість кіберзброї на ураження конкретних об’єктів з критичною інформаційною інфраструктурою, а також визначених заздалегідь суб’єктів в управлінській компетенції яких такі об’єкти знаходяться, або які мають доступ до них;

− кіберзброя застосовується скрито. У більшості випадків уражаючі фактори від застосування кіберзброї проявляються значно пізніше факту її застосування;

− кіберзброя застосовується як доповнення до інших воєнних дій, операцій та акцій і, як правило, заздалегідь до їх проведення;

− кіберзброї характерні процеси мутації в часі, що забезпечують їй зміну цілей та задач в процесі бойового застосування, що тягне за собою зміну її структури аж до повної її самоліквідації;

− процес розробки, впровадження та застосування кіберзброї здійснюється за рахунок фінансів державного походження;

− громадянське суспільство, як правило, не інформується про порядок здійснення процедур кіберзахисту у разі спрацювання "ефекту бумеранга" та ін.

Основні завдання, що покладаються на кіберзброю, полягають у наступному:

− тимчасове ускладнення чи вибіркове призупинення шляхом відключення або блокування критично важливих вузлів об'єктів з критичною інформаційною інфраструктурою;

− порушення роботи та виведення з ладу автоматизованих систем управління різного призначення та систем зв'язку;

− фальсифікація, дезінформація управлінської інформації в усіх сферах, у тому числі й критичних для національної безпеки;

− дезорганізація роботи кібернетичних систем.

До можливих об'єктів ураження кіберзброєю можна віднести:

− об'єкти з критичною інформаційною інфраструктурою, що задіяні в забезпеченні функціонування інфраструктури та життєзабезпечення (атомні електростанції, підприємства хімічної, нафтової, газопереробної галузей, водо-, тепло- постачання, автоматизовані системи управління технологічними процесами на стратегічно важливих підприємствах, усі види транспортних мереж тощо);

− інформаційні і комунікаційні ресурси держави (засоби масової інформації (телерадіокомпанії), оператори стільникового зв'язку, провайдери Інтернет, відомчі локальні обчислювальні мережі, глобальна мережа Інтернет, децентралізовані анонімні мережі (ANts P2P, BitBlinder, Filetopia, Freenet та ін.), гібридні анонімні мережі (Psiphon, Tor, Virtual Private Network та ін.), вузькоспеціалізовані анонімні мережі (Java Anonymous Proxy, Mixminion, Veiled та ін.);

− поштова кореспонденція вищих посадових осіб держави та власне такі особи;

− бази даних спецслужб, силових міністерств та відомств, державних та регіональних органів влади, банківських та фінансових установ, які містять інформацію з обмеженим доступом;

− соціум та соціотехнічні системи;

− технічні системи (комп'ютерні системи та мережі; системи урядового зв'язку;

− АСУ та управляючі елементи систем озброєння та військової техніки, програмне забезпечення тощо).

Даний перелік характерних ознак кіберзброї, основних завдань та об'єктів ураження нею постійно доповнюється. У широкому сенсі він повинен включати усі без винятку кібернетичні системи держави, незалежно від їх цільового призначення та форми власності.

Отже, незважаючи на активізацію гонки кіберозброєнь, недооцінювання небезпеки від кіберзброї може мати фатальні для планети наслідки – це у більш широкому сенсі та непередбачувані наслідки для цивільної та військової критичної інформаційної інфраструктури будь-якої держави – у більш вузькому.

3.5.2. Класифікація кіберзброї

Невирішеною остаточно залишалася до сьогодні проблема формалізації простору ознак, належність до яких дозволятиме здійснювати класифікацію кіберзброї. На сьогодні відомо три класифікації кіберзброї: американська, яка розроблена в 2011 році в Пентагоні та є загальноприйнятою у США для всіх силових структур, та дві класифікації розроблені незалежно один від одного експертами П. Пассері та П. Паганіні.

На основі проведеного аналізу відомих класифікацій пропонується узагальнена класифікація, яка може бути використана для опису широкого спектра зразків кіберзброї (рис. 3.20). З урахуванням того, що кіберзброя досить різноманітна, то основним принципом, який можна покласти в основу класифікації, є ознаковий. Вперше такий підхід було реалізовано професором О. Корченко для класифікації кібератак.

Рис. 3.20. Класифікація кіберзброї

Пропонується класифікувати кіберзброю за наступними базовими ознаками: призначення; масштабність застосування; характер вражаючої дії; спосіб доставки; керованість; деструктивний вплив; оперативність; місце

базування; рівень маскування; спосіб виготовлення; спектр дії; об’єкти ураження; рівень впливу на об’єкти ураження; прицільні властивості; інтегральний ефект; тип зв’язків та рівень взаємодії; наслідки; принцип генерування; самоорганізація; тривалість ефекту; латентність.

За призначенням кіберзброя поділяється на:

− розвідувальну;

− захисну;

− зброю кібервпливу.

Розвідувальна зброя призначена для добування інформації з кіберпростору шляхом моніторингу кібернетичних систем та процесів, які в них протікають під час функціонування. Кіберзброя захисту призначена для забезпечення та підтримання заданого рівня кібербезпеки. Зброя, що призначена для здійснення кібервпливу на елементи кіберпростору противника з метою порушення процесів управління в кібернетичних системах, називаються зброєю кібернетичного впливу.

За масштабами застосування кіберзброя може бути:

− глобальна;

− стратегічна;

− тактична.

Застосування кіберзброї несе глобальний характер, коли масштаб від її застосування потенційно може поширюватися на усі країни, в яких функціонують об’єкти з критичною кібернетичною інфраструктурою. Стратегічний масштаб застосування кіберзброї поширюється на міждержавний (регіональний) рівень. Тактична кіберзброя за масштабом застосування орієнтована переважно на застосування на національному рівні.

За характером вражаючої дії кіберзброя поділяються на:

− зброю масового ураження;

− зброю функціонального ураження;

− функціонального придушення;

− функціонального виведення з ладу.

Кіберзброя масового ураження має такий характер вражаючої дії, який співвимірний з наслідками, що виникають внаслідок застосування зброї масового ураження (ядерної, хімічної, біологічної). Застосування кіберзброї функціонального ураження призводить до ураження окремих функцій, що виконуються об’єктом, внаслідок чого він втрачає здатність до виконання цільової задачі. Кіберзброя функціонального придушення передбачає функціональне придушення, що призводить до комплексної дії на об’єкт з критичною кібернетичною інфраструктурою, внаслідок чого він втрачає здатність до виконання цільової задачі протягом заданого інтервалу часу. Результатом функціонального виведення з ладу є генерація необоротних процесів, що призводять до виведення з ладу об’єктів впливу.

За способом доставки кіберзброя може доставлятися:

− природними носіями;

− штучними носіями.

Природним носієм доставки кіберзброї є людина. Наприклад, інсайдер. Штучними носіями є усі інші засоби, що не є об’єктами біологічного походження.

За керованістю кіберзброя поділяється на:

− керовану;

− некеровану.

Керована кіберзброя передбачає постійне або періодичне управління процесом її бойового застосування. Некерована кіберзброя – це зброя, яка не потребує зовнішнього втручання в процесі її цільового застосування.

За деструктивним впливом кіберзброя може бути:

− безпечна;

− небезпечна.

Дана класифікаційна ознака є специфічною. Вона властива тільки кіберзброї, оскільки “зброя” в принципі не буває “безпечною” або “небезпечною”. До безпечної, з точки зору руйнівних властивостей, можна віднести зброю, яка не призводить до фізичних руйнувань інфраструктури об’єкта, а порушує властивості безпеки інформації на ньому. Наприклад, розвідувальна кіберзброя призводить до порушення конфіденційності інформації на об’єкті, що розвідується, але ніяким чином не руйнує його інфраструктуру. Небезпечна – зброя, деструктивний вплив від якої має прояви, як для інфраструктури об’єкта, так і для безпеки інформації, яка на ньому циркулює.

За оперативністю кіберзброя може бути:

− миттєвої дії;

− повільної дії з накопиченням;

− тимчасової дії;

− довгострокової дії.

Миттєва дія кіберзброї співвимірна з масштабом часу, протягом якого вона проявляє деструктивний вплив на об’єкт або суб’єкт впливу. Кіберзброя повільної дії з накопиченням являє собою зразок зброї, корисний ефект від застосування якої поступово накопичується і при досягненні заданого рівня насичення проявляє свої деструктивні властивості. За оперативністю кіберзброя тимчасової дії орієнтована на виконання своїх деструктивних функцій протягом деякого відносно нетривалого інтервалу часу. Довгострокова дія кіберзброї характеризується відносно тривалим інтервалом часу, протягом якого вона використовується за призначенням.

За місцем базування кіберзброя буває:

− космічного базування;

− повітряного базування;

− наземного базування;

− морського базування;

− підземного базування;

− змішаного базування.

Місце базування кіберзброї визначається виходячи, в першу чергу, із того кола задач, які на неї покладаються. Переважно кіберзброя має змішане базування.

За рівнем маскування кіберзброя може бути:

− замаскованою;

− незамаскованою.

Замаскована кіберзброя передбачає застосування елементів маскування.

Незамаскована – навпаки, такі елементи не використовує.

За способом виготовлення кіберзброя поділяється на:

− кустарну;

− промислову;

− змішану.

Кустарне виробництво передбачає виготовлення зразка несерійного характеру, як правило, особою або групою осіб та не передбачає залучення державного фінансування. Кіберзброя промислового виготовлення – це зброя яка виготовляється, як правило, на замовлення держави або групи держав із залученням її промислових потужностей. Кіберзброя за змішаним способом виготовлення поєднує у собі елементи кустарного та промислового виробництва.

За спектром дії кіберзброю можна поділяти на зброю:

− низького потенціалу;

− середнього потенціалу;

− високого потенціалу.

Кіберзброя низького потенціалу призводить до деструктивного впливу, що не призводить до завданню об'єкту впливу безпосередньої шкоди. Прикладом такої зброї є спеціалізоване програмне забезпечення для генерації потужного потоку трафіка з метою тимчасового перевантаження ресурсів системи, що призводить до заподіяння тимчасової шкоди об'єкту впливу без нанесення йому будь-яких фізичних пошкоджень. Кіберзброя середнього потенціалу – це зброя, застосування якої призводить до функціонального ураження або придушення, але не призводить до функціонального виведення з ладу об'єкта впливу. Кіберзброя високого потенціалу – це зброя, що здатна досягати об'єкта впливу шляхом обходу його систем захисту й здатна до його функціонального виведення з ладу.

Цілями ураження кіберзброї можуть бути:

− об'єкти з критичною кібернетичною інфраструктурою;

− суб'єкти управління.

Об'єкти з критичною кібернетичною інфраструктурою – це матеріальні чи віртуальні об'єкти й системи, порушення або припинення функціонування яких призводить до втрати управління, руйнування інфраструктури, незворотних негативних змін або руйнувань економіки країни, суб'єкта або адміністративно-територіальної одиниці, або до впливу на безпеку населення, яке мешкає на цих територіях. Суб'єкт управління як ціль ураження – це особа, група людей або організація, що приймає управлінські рішення та керує об'єктами з критичною кібернетичною інфраструктурою шляхом впливу на них.

За рівнем впливу на об'єкти ураження:

− об'єкти, що підлягають відновленню;

− об'єкти, що не підлягають відновленню.

Вплив кіберзброї на об’єкти ураження може мати дуальний характер: об’єкти можуть підлягати відновленню за деякий часовий термін або ж такому відновленню не підлягають.

За рівнем впливу на суб’єкти ураження кіберзброя може бути:

− смертельної дії;

− несмертельної дії;

− налаштованої дії.

Кіберзброя смертельної дії передбачає завдання смертельних збитків протиборчій стороні у живій силі. Кіберзброя несмертельної дії не призводить до загибелі живої сили протиборчої сторони. Кіберзброя з налаштованою дією – це зброя, властивості якої щодо впливу на живу силу протиборчої сторони налаштовуються у процесі її застосування шляхом виставлення порога кібервпливу.

За прицільними властивостями кіберзброя буває двох видів:

− високоточною;

− неприцільною.

Високоточна кіберзброя призначена для нанесення високоточних ударів по визначених цілях кібервпливу. Неприцільна – це зброя, яка не володіє прицільними властивостями щодо конкретних цілей.

За типом зв’язків та рівнем взаємодії:

− поодинока;

− групова.

Кіберзброя, що відноситься до класу поодинокої передбачає застосування її без залучення додаткових допоміжних модулів. До групової відносять кіберзброю, яка для досягнення своєї цілі використовує додаткові модулі, які у своїй сукупності дозволяють досягнути поставленої перед нею цілі.

Кіберзброя **за наслідками** поділяється на:

− глобальну;

− регіональну;

− локальну.

Застосування кіберзброї несе глобальний характер, коли масштаб від її застосування потенційно може призвести до загибелі людства на Землі.

Стратегічний масштаб застосування кіберзброї означає її здатність до зміни ролі й призначення кібернетичних систем на міждержавному (регіональному) рівні. Тактична кіберзброя за масштабом застосування призначена для вирішення задач тактичного рівня у визначеному регіоні.

За генеруванням кіберзброя може бути:

− самогенеруюча;

− з часовим механізмом;

− за настанням визначеної події.

Самогенеруюча кіберзброя – це зброя, яка не потребує зовнішнього втручання для приведення її в готовність до виконання задач. Генерування за часовим механізмом передбачає приведення в готовність зброї у визначений момент часу. Настання визначеної події інколи також є підставою для виконання кіберзброєю своїх функцій.

За рівнем інтегрального ефекту кіберзброя поділяється на:

− зброю часткового ефекту;

− зброю з повним ефектом.

Інтегральний ефект від застосування кіберзброї має дві форми прояву: часткову, коли ефект має лише локальні частинні наслідки, та повну форму прояву, коли ефект носить глобальний характер.

За самоорганізацією кіберзброя буває:

− самоорганізованою;

− за окремою командою.

Самоорганізованість кіберзброї – це процес упорядкування елементів одного рівня у системі за рахунок внутрішніх закладених функцій, без зовнішнього специфічного впливу. Самоорганізація кіберзброї за окремою командою передбачає реалізацію визначеного вище процесу при надходженні відповідного зовнішнього специфічного впливу – команди.

За часом тривалості ефекту кіберзброя буває:

− миттєвого ефекту;

− відкладеного ефекту.

Миттєвий ефект від застосування кіберзброї проявляється в масштабі часу, співвимірному з часом її цільового застосування. Якщо ефект від застосування кіберзброї проявляється дещо пізніше від моменту початку її застосування за цільовим призначенням, то така зброя є зброєю з відкладеним ефектом.

За латентністю кіберзброя буває:

− негайного прояву;

− відкладеного прояву.

Кіберзброя, яка проявляє себе належним чином у процесі застосування, є зброєю негайного прояву. У протилежному випадку, коли латентний період є досить тривалим – кіберзброя може бути кіберзброю з відкладеним проявом.

Перевагою запропонованої класифікації (див. рис. 3.20), порівняно з відомими, є те, що кіберзброя, яка класифікується за ознаковим принципом може у кожному конкретному випадку при визначенні загального класу мати не тільки одну, але й більше компонент будь-якої з ознак. Крім того, покладений в основу класифікації ознаковий принцип забезпечує розширення множини ознак, за якими можна здійснювати класифікацію.

Наприклад, спираючись на розроблену класифікацію кіберзброї такий зразок, як Stuxnet, може бути визначений наступним чином. Stuxnet – це зразок кіберзброї, призначений для здійснення керованого небезпечного кібервпливу стратегічного характеру, спрямованого на функціональне виведення з ладу об'єктів з критичною інформаційною інфраструктурою. Зразок має довгострокову дію. Характеризується наземним базуванням та доставляється природним носієм. Рівень маскування характеризує його як невидимий зразок промислового походження, спрямований для нанесення кібервпливу з метою невідновлення об'єктів впливу. Stuxnet є високоточним зразком з повним рівнем інтегрального ефекту групового характеру, що має глобальні наслідки й самогенерується. Зброя є самоорганізованою з відкладеним часом тривалості ефекту й відкладеним проявом.

Запропонована класифікація забезпечує формалізацію вимог до новостворюваних зразків кіберзброї. Вона не претендує на закінченість, не є остаточною й буде доповнюватися, уточнюватися і розвиватися в майбутньому з вдосконаленням цієї зброї і способів її застосування. Разом з тим, така класифікація дає можливість більш чітко уявити особливості механізму дії кіберзброї на всі можливі об'єкти ураження, спрогнозувати тенденції її розвитку (наприклад, шляхом комбінації ознак різних класів), а також передбачити заходи щодо захисту від факторів її ураження.

3.5.3. Базові принципи побудови кіберзброї

Відсутність єдиного розуміння сутності феномену кіберзброї породжує низку супутніх проблем, які охоплюють досить широкий спектр питань – від юридичних основ її застосування до питань технічної реалізації. Зважаючи на це, вивчення базових принципів доцільно провести скориставшись методом аналогії. Перед вибором аналога розглянемо основні характеристики, що притаманні кіберзброї, і які, за своїм змістом, суттєво відрізняють її від інших видів зброї.

До основних характеристик кіберзброї можна віднести такі:

− скритність;
− економічна ефективність;
− універсальність;
− масштабність застосування;
− володіння ефектом "ланцюгової реакції";
− складність здійснення міжнародного контролю за розробкою та застосуванням.

Скритність кіберзброї проявляється у можливості укриття процесу її розробки, випробування та застосування від протиборчої сторони.

Економічний ефект кіберзброї проявляється у двох аспектах. По-перше, вартість виготовлення кіберзброї та її застосування, порівняно з іншими зразками зброї, наприклад, високоточної, потребує суттєво менших витрат та не потребує створення інфраструктури для її серійного виробництва. По-друге, застосування кіберзброї може підірвати економіку держави протиборчої сторони значно більше ніж застосування зброї на традиційних принципах дії.

Універсальність кіберзброї полягає у тому, що форми і способи її застосування не залежать від театру воєнних дій, на якому вона застосовується, часу доби та пори року, стану фізичної інфраструктури (стану доріг, мостів тощо).

Масштабність застосування кіберзброї проявляється в можливості її впливу на стаціонарні та мобільні елементи системи управління наземного, морського, повітряного і космічного базування, а також на суб'єкти управління.

Ефект "ланцюгової реакції" кіберзброї проявляється у тому разі, коли поодинокий кібервплив на один з об'єктів з критичною інформаційною інфраструктурою призводить або може призвести до ураження інших елементів кібернетичної системи або системи у цілому.

Міжнародний контроль за розробкою та застосуванням кіберзброї ускладнений з низки причин. По-перше, розробка кіберзброї не потребує створення спеціалізованої інфраструктури. Тобто з використанням технічних засобів моніторингу практично неможливо виявити демаскувальні ознаки інфраструктури де виготовляється кіберзброя.

По-друге, відсутність нормативно закріплених юридичних міжнародних норм фактично стримує міжнародний контроль розвитку кіберозброєнь. По-третє, відсутні, власне, такі міжнародні організації, на які покладено відповідні функції контролю. Таким чином, приведені вище ознаки й класифікація дозволяють стверджувати про те, що кіберзброя є якісно новим зразком зброї.

Вибір аналога. Як аналог оберемо ракетоносій. Умовно він складається з трьох типових елементів: засобу доставки; системи навігації; корисного навантаження. Схожі елементи характерні і для кіберзброї (рис. 3.21).

Рис. 3.21. Базовий принцип побудови зразка кіберзброї

Засобом доставки кіберзброї можуть бути листи електронної пошти зі шкідливим контентом (спамом та скамом), веб-сайти зі шкідливими посиланнями (рекламою). Інколи як засіб доставки може виступати суб'єкт (інсайдер) з відповідним носієм корисного навантаження (флеш-пам'яттю). Підроблене обладнання, шкідливе програмне забезпечення замасковане під ліцензійні продукти відомих брендів ІТ-ринку, радіокомпоненти та ін. також можуть виступати засобами доставки кіберзброї.

Система навігації кіберзброї, подібно до системи навігації ракетоносія, забезпечує досягнення корисним навантаженням визначеного об'єкта кібервпливу або його складової компоненти (рис. 3.22).

Як випливає з рис. 3.22, в основу навігації будь-якого зразка кіберзброї покладено уразливості об'єкта, що піддається кібервпливу. При цьому, слід акцентувати увагу на тому, що уразливості в конфігурації програмного забезпечення, у свою чергу, слугують базою для корисного навантаження кіберзброї.

Корисним навантаженням кіберзброї, подібно до корисного навантаження ракетоносія – боєголовок, може бути спеціалізоване програмне забезпечення, побудоване за модульною структурою у вигляді бойових програмних агентів (рис. 3.23), що виконують задані функції деструктивного впливу.

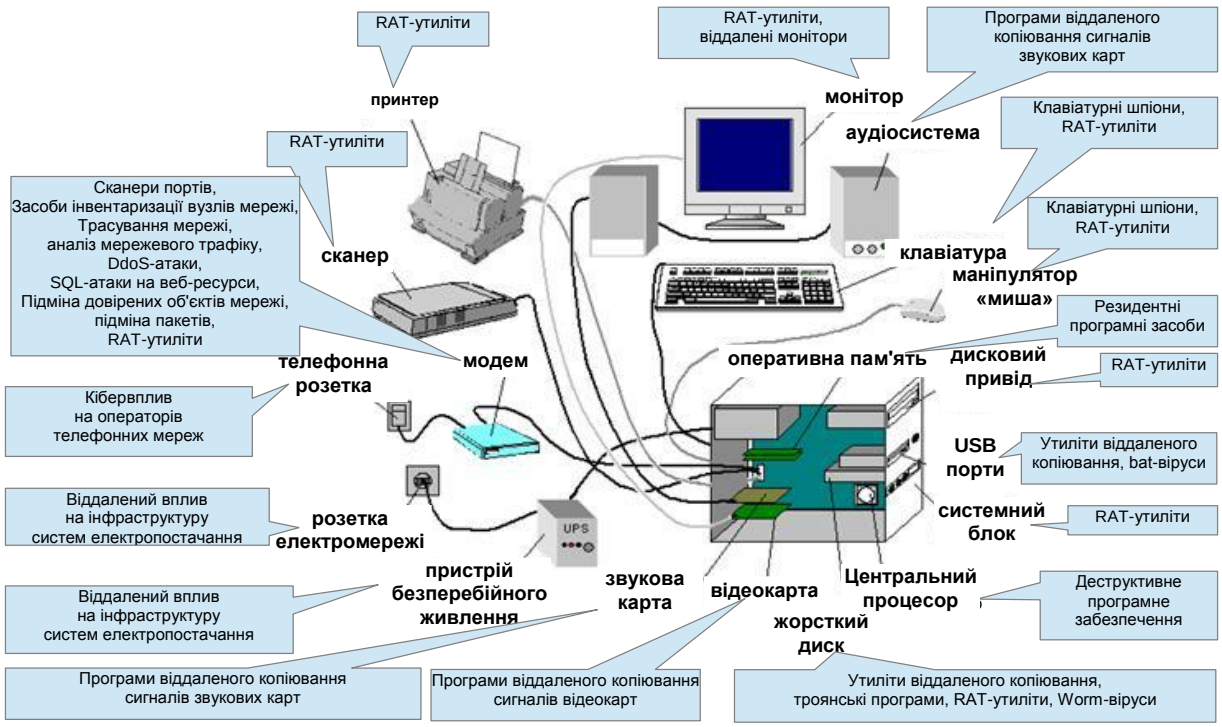

Рис. 3.22. Об’єкт кібервпливу та його складові елементи (на прикладі ПЕОМ)

Ділянка коду, що виконує деструктивні функції у відношенні до об’єктів кібервпливу	Ділянка коду, що забезпечує завчасну закладку «логічних бомб» на об’єктах з критичною інформаційною інфраструктурою	Модуль перехоплення та прихованого віддаленого управління об’єктом з критичною інформаційною інфраструктурою	Модуль реалізації DDoS- атак	Модуль подавлення інформаційного обміну в мережах	Модуль фальсифікації інформації при її передаванні в мережі	Модуль самоліквідації

Рис. 3.23. Типізація компонентів бойової частини корисного навантаження типового зразка кіберзброї

Бойовий програмний агент – це комплекс програмних модулів з деструктивними функціями, що побудовані за принципом комп’ютерного вірусу. Аналіз базової архітектури кіберзброї (рис. 3.16) дозволяє зробити висновок – кіберзброя є зброєю з досить гнучким адаптивним цільовим призначенням. Тобто, залежно від задач, призначення зразка кіберзброї може адаптивно змінюватися її розробником шляхом зміни призначення одного або декількох складових елементів.

Питання самоконтролю

1. Тенденції розвитку інформаційних та кібертехнологій.
2. Особливості високотехнологічних війн.
3. Існуючі системи підготовки фахівців з кібербезпеки та кібероборони у провідних країнах світу.
4. Особливості практичної складової підготовки фахівців з кібербезпеки та кібероборони у провідних країнах світу.
5. Зміст системи підготовки військових фахівців та наукових досліджень за високотехнологічними напрямами.
6. Вимоги до знань фахівців з кібербезпеки та кібероборони.
7. Основні фактори, які впливають на розвиток і впровадження високотехнологічних розробок в інтересах національної безпеки і оборони в Україні.
8. Принципово-інноваційні рішення побудови системи кібербезпеки та кібероборони.
9. Сутність кібероперації.
10. Зміст кібероперації.
11. Типовой сценарій проведення кібероперацій.
12. Сутність складових структури оперативних компонент операції у кіберпросторі.
13. Підходи щодо планування кібероперацій.
14. Алгоритм завчасного планування кібероперації.
15. Алгоритм планування кібероперації у кризовій ситуації.
16. Схема етапів планування кібероперацій.
17. Сутність терміна «кіберзброя».
18. Характерні ознаки кіберзброї.
19. Основні завдання, що покладені на кіберзброю.
20. Об’єкти ураження кіберзброєю.
21. Класифікація кіберзброї.
22. Базові принципи побудови кіберзброї.
23. Загальні підходи планування операції за стандартами НАТО.
24. Процес планування операції в кіберпросторі.
25. Основні способи оцінки інформаційних ризиків.

Інформаційні джерела

1. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19/ed20180621#n24.
2. Кузьменко Б.В., Заіка Ю.О. Кібертероризм: світові й українські реалії // *Науковий вісник Академії внутрішніх справ*. 2012. № 2(81). С. 92-98.
3. Бистрова Б. Рівні забезпечення якості підготовки фахівців з кібербезпеки в закладах вищої освіти США // *Педагогічні науки: теорія, історія, інноваційні технології*. 2019. № 2 (86). С.140-149.
4. URL: https://www.nist.gov (дата звернення 02.12.2019).
5. Castro D. (2018). Boosting the Cyberworkforce. URL: http://www.govtech.com/data/Boosting-the-Cyberworkforce.html
6. Get Involved with the CDM Learning Program! URL: https://www.us-cert.gov/sites/default/files/cdm_files/FNR_CGB_MTG_AprilWebinar.pdf
7. Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. Інформаційна безпека: соціально-правові аспекти: підручник; за заг.ред. Скулиша Є.Д.. 2010. 512 с.
8. Військова Технічна Академія імені Ярослава Домбровського. URL: http://www.wat.edu.pl. (дата звернення 27.12.2019).
9. Королівський військовий коледж Канади. URL: https://www.rmc-cmr.ca/en. (дата звернення 27.12.2019).
10. Universität der Bundeswehr München. URL: https://www.unibw.de/home. (дата звернення 27.12.2019).
11. Кибербезопасность: Типовой учебный план (НАТО). 2016. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/20171004_1610-cybersecurity-curriculum-rus.pdf.
12. Про Стратегічний оборонний бюлетень України: Указ Президента України №240/2016 від 6 червня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/n0006525-16.
13. Даник Ю. Г., Вдовенко С. Г. Концептуальні напрями комплексного вирішення проблеми захисту інформації в системі скритого управління збройних сил // *Сучасні інформаційні технології у сфері безпеки та оборони*, 2017. № 2(29). С. 98–107.
14. Даник Ю. Г., Телелим В. М., Чмельов В. О. Превентивна оборона як вид стратегічних дій // *Наука і оборона*. 2008. № 4. С. 34–41.
15. Даник Ю. Г., Телелим В. М., Чмельов В. О. Основні аспекти стратегії превентивної оборони та її реалізації // *Наука і оборона*. 2010. № 2. С. 15–23.
16. Даник Ю. Г., Телелим В. М., Радецький В. Г. Питання трансформації оборонних структур держави та удосконалення системи військової освіти // *Наука і оборона*. 2009. № 1. С. 15–19.
17. Даник Ю. Г., Супрунов Ю. М. Деякі підходи до формування системи підготовки кадрів для системи кібернетичної безпеки України // *Проблеми створення, випробування та експлуатації складних інформаційних систем: збірник наукових праць*. Житомир : ЖВІНАУ. 2011. Вип. 5. С. 5–22.

18. Даник Ю. Г., Дупелич С. О. Стратегічні аспекти боротьби з робототехнічними комплексами // *Сучасні інформаційні технології у сфері безпеки та оборони*. 2017. № 2(29). С. 16–25.

19. Даник Ю.Г., Корнейко О.В. Основи методології формування кіберкомпетенцій у фахівців сектору безпеки і оборони України // *Information Technology and Security*. 2018. Том 6. № 2(11). С. 105-123

20. Exercise Cyber Coalition 2019 Concludes in Estonia. URL: https://www.act.nato.int/articles/exercise-cyber-coalition-2019-concludes-estonia.

21. Військовослужбовці військ зв'язку Збройних Сил України беруть участь у багатонаціональних навчаннях НАТО "Cyber Coalition — 2019" в Естонії. URL: http://www.mil.gov.ua/news/2019/12/05/vijskovosluzhbovczi-vijsk-zvyazku-zbrojnih-sil-ukraini-berut-uchast-u-bagatonaczionalnih-navchannyah-nato-cyber-coalition-2019-v-estonii/ (дата звернення 27.12.2019).

22. Agency leads NATO team in tough cyber exercise. URL: https://www.ncia.nato.int/NewsRoom/Pages/20190408-Lock-Shields.aspx.

23. Процедури процесу прийняття військового рішення (за стандартами НАТО): навч. посіб. / Колектив авторів. К. : НУОУ ім. Івана Черняхівського. 2018. 140 с.

24. JP 3-05.1 Joint Special Operations Task Force Operations, 26 April 2007. https://fas.org/irp/doddir/dod/jp3_05_01.pdf

25. Даник Ю. Г. Основні аспекти парадигми кібернетичної безпеки. URL: http://jrnl.nau.edu.ua/index.php/IMV/article/view/3171.

26. Nye J. (2003). The Power of Persuasion: Dual components of US leadership. The conversation with J. Nye. – Harvard International Review, Winter.

27. Даник Ю. Г., Катков Ю. І., Пічугін М. Ф. Національна безпека: запобігання критичним ситуаціям: монографія. Київ: МО України; Житомир: Рута. 2006. 388 с.

28. Сунь-Цзи Мистецтво війни; переклад Г. Латника. К.:Арій. 2014. 128 с.

29. Sherr, J. (2013). Hard diplomacy and soft coercion: Russia's influence abroad. Royal Institute of International Affairs.

30. Huang, Y., & Ding, S. (2006). Dragon's underbelly: An analysis of China's soft power. East Asia. 23(4). 22-44.

31. Concept of the Foreign Policy of the Russian Federation, adopted on 12 February 2013; an unofficial English translation is available at. URL: www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/869c9d2b87ad8014c32575d9002b1c38!OpenDocument.

32. Sharp, G. (2012). From dictatorship to democracy: A conceptual framework for liberation. The New Press.

33. Mann, S. R. (1992). Chaos theory and strategic thought. ARMY WAR COLL CARLISLE BARRACKS PA.

34. Говоруха, В. В., Даник, Ю. Г., & Клевець, В. В. (2009). Напрями вдосконалення механізмів функціонування органів державного управління в умовах трансформації технологій зовнішнього інформаційно-психологічного впливу на них // Актуальні проблеми державного управління. (1). 9-16.

35. URL: http://www.ccu.gov.ua/doccatalog/document?id=242321.
36. Різун, В. В. (2008). Теорія масової комунікації: підруч. для студ. галузі 0303 “Журналістика та інформація”. К.: Видавничий центр «Просвіта. 55.
37. Петрик, В. М. (2011). Сугестивні технології маніпулятивного впливу. URL: http://pidruchniki.ws/15440428/psihologiya/dosvid_ukrayini_formuvanni_informatsiyno-komunikativnogo_suspilstva.
38. Грищук Р.В., Даник Ю. Г. Синергія інформаційних та кібернетичних дій // Труди університету. К.: НУОУ. 2014. № 6 (127). С. 132–143.
39. URL: http://infostream.ua/
40. Шнурко-Табакова Э. (2015) Дискредитация украинских генералов: говорит и показывает статистика. URL: http://hi-tech.ua/article/diskreditatsiya-ukrainskih-generalov-govorit-i-pokazyivaet-statistika.
41. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. CS&CS, 2019. Issue 1(13). С.17-29.
42. FM 3-12 Cyberspace and Electronic Warfare Operations, April 2017.
43. JP 3-12 Cyberspace Operations, 8 June 2018.
44. Даник Ю. Г., Грищук Р. В. Основи кібернетичної безпеки: монографія; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ. 2016. 636 с.
45. Task force on strategic communication. January 2008. - Washington, 2008. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a476331.pdf.
46. Ліпкан В. А. Роль стратегічних комунікацій в протидії гібридній війні проти України http://goal-int.org/rol-strategichnix-komunikacij-v-protidii-gibridnij-vijni-proti-ukraini/.
47. NIST 800 – 30 Risk Management Guide for Information Technology Systems.
48. Луцкий М.Г., Иванченко Е.В., Казмирчук С.В. Базовые понятия управления риском в сфере информационной безопасности // Защита информации. 2011. 194 с.
49. Freund J., Jones J. Measuring and managing information risk. A FAIR approach [Текст]: Jack Freund, Jack Jones. – Oxford:Butterworth of Elsevier. 2017. 391 с.

ВИСНОВКИ

У більшості країн світу з метою своєчасного реагування на виклики і загрози сьогодення і майбутнього їх запобігання, стримування та нейтралізації оборонний сектор держав включає дві основні компоненти: потенціал стримування, який складається з традиційних видів Збройних Сил та потенціал ведення війн нового типу, основу якого складають сили і засоби спеціальних операцій, кібербезпеки та кібероборони, інформаційних та психологічних операцій, радіоелектронної боротьби, розвідки, інформаційно-аналітичного забезпечення, оперативного управління силами і засобами, інфокомунікацій, підрозділи, які оснащені робототехнічними комплексами і засобами боротьби з ними та інші високотехнологічні сили і засоби.

Це знаходить досить чітке своє відображення в національних оборонних концепціях, стратегіях, воєнних доктринах та при трансформації і розвитку їх Секторів безпеки у вигляді комплексних високотехнологічних змін на політичному, організаційному, процесуальному, кадровому рівнях.

Тому серед загроз національній безпеці у воєнній сфері багато країн уже сьогодні вбачають не тільки відставання в розробленні та прийнятті на озброєння нових високотехнологічних засобів озброєння і військової техніки. Ще більшою мірою це стосується якості підготовки фахівців у сфері кібербезпеки та кібероборони.

При розробці методології освіти фахівців за напрямом кібербезпеки та кібероборони необхідно враховувати низку особливостей, притаманних сучасним інформаційним технологіям: швидку зміну їх поколінь; постійне зростання можливостей впливу на складові кібернетичних систем та об’єкти критичної інформаційної інфраструктури; необхідність постійного оновлення знань з питань кібербезпеки; різні рівні здатності і готовності до навчання тих, хто навчається; особливості курсу кібербезпеки; значну кількість специфічних складових кібербезпеки і кібероборони тощо.

Зміст підручника “Основи кібербезпеки та кібероборони” дозволяє підвищити рівень обізнаності слухачів в питаннях щодо:

− основ забезпечення кібербезпеки та кібероборони держави;

− складу сил і засобів кібербезпеки та кібероборони, їх завдань, можливостей, форм та способів застосування;

− основ підготовки і ведення кібероборони держави та операцій у кіберпросторі і через кіберпростір;

− методів роботи посадових осіб під час підготовки і ведення кібероборони держави та спеціальних операцій у кіберпросторі;

− методів аудиту та оцінки стану кібербезпеки на державному рівні.

Навчальне видання

Даник Юрій Григорович,
Воробієнко Петро Петрович,
Чернега Володимир Миколайович

ОСНОВИ КІБЕРБЕЗПЕКИ ТА КІБЕРОБОРОНИ

Підручник
Видання друге

Редактор – Кодрул Л.А.
Комп'ютерне верстання – Трифонова К.В.

Підписано до друку 15.11.2019 р.
Формат 60/88/16. Обсяг 20,0 друк. арк.
Тираж 50 прим. Зам. № 6430

Видавець і виготовлювач ОНАЗ ім. О.С. Попова
м. Одеса, вул. Кузнечна, 1
Свідоцтво суб'єкта видавничої справи ДК № 3633 від 27.11.09