МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Ігор ЯКОВІВ

СИСТЕМНІ ОСНОВИ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА НАЦІОНАЛЬНИХ ЕЛЕКТРОННИХ РЕСУРСІВ

Навчальний посібник

Рекомендовано Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського як навчальний посібник для здобувачів ступеню магістр за освітніми програмами "Комп'ютерні системи і технології спеціального зв'язку" спеціальності 122 Комп'ютерні науки та "Спеціальні системи електронних комунікацій" спеціальності 172 Електронні комунікації та радіотехніка.

Київ
ІСЗЗІ КПІ ім. Ігоря Сікорського
2024

УДК 004.056.5 (075.8)
Я14

Розглянуто Вченою радою
ІСЗЗІ КПІ ім. Ігоря Сікорського
(Протокол № 15 від 27.06.2024 р.)

Рецензенти: *І. Ю. Субач, д-р техн. наук, проф.*
А. В. Жилін, кан. техн. наук, доцент.

Ігор ЯКОВІВ
Я14
Системні основи кіберзахисту інформаційних технологій та національних електронних ресурсів: навч. пос. / Яковів І.Б.; ІСЗЗІ КПІ ім. Ігоря Сікорського. 2024.- 238 с.

В навчальному посібнику за допомогою атрибутивно-трансфертного підходу до природи інформації розглянуто системні основи забезпечення кібербезпеки інформаційних технологій та національного сегменту електронних ресурсів. Посібник знайомить курсантів (студентів) з нормативно-правовими та організаційно-технічними аспектами кіберзахисту інформаційно-комунікаційних систем, особливостями складу, структури і функціонування Національної системи кібербезпеки та Національної системи захисту критичної інфраструктури. Окремі розділи знайомлять з принципами формування інфраструктури кіберзахисту та її застосування для проактивної протидії APT атакам, проведення розвідки кіберзагроз і аудиту кібербезпеки.

Навчальний посібник призначений здобувачам вищої освіти за спеціальностями 122 Комп'ютерні науки і 172 Електронні комунікації та радіотехніка.

УДК 004.056.5 (075.8)

ЗМІСТ

ВСТУП

Розвиток інформаційних технологій та їх ефективне застосування безпосереднє залежить від можливості забезпечити заходи протидії атакам в кіберпросторі. Відстань від цієї тривіальної загальної думки до ментальних конструкції рішень про впровадження конкретних заходів кіберзахисту вимірюється комплексом узгоджених фахових знань різного рівня деталізації. Перехід від концепту безпеки інформації комп'ютерних систем до кібербезпеки, що спостерігається з десятих років поточного століття, супроводжується масштабним ростом відповідної інформації різного рівня складності та деталізації. Вирішення проблеми пошуку корисної інформації для організації результативного кіберзахисту інформаційно-комунікаційних технологій є дуже актуальним питанням для будучих фахівців.

Цей посібник направлений на формування у здобувачів вищої освіти таких компетенції, які дозволяють не тільки орієнтуватися в актуальних тенденціях протидії зловмисним діям в кіберпросторі, но і приймати аргументовані організаційно-технічні рішення щодо впровадження результативних заходів циклу керування кібербезпекою.

Логічне поєднання матеріалу посібника забезпечувалось на основі використання методів: 1) системного аналізу складних систем; 2) подолання семантичних невизначеностей засобами термінологічної, графічної та математичної формалізації; 3) представлення заходів кіберзахисту у вигляді інформаційних процесів. Посібник має наступні розділи:

Розділ 1 пояснює визначення базових нормативних термінів з кібербезпеки.

Розділ 2 розкриває базові поняття теорії систем, сутність системного підходу та концепцію атрибутивно-трансферної природи інформації.

Розділ 3 розглядує кіберпростір як фізичне середовище, аналізує співвідношення інформаційно-комунікаційної, інформаційної та комп'ютерних систем, аналізує їх склад та структури, уточнює фізичні основи процесів обробки інформації.

Розділ 4 аналізує сутність безпеки інформації та її зв'язок з кібербезпекою.

Розділ 5 надає формалізовані моделі кіберпростору та кібербезпеки, які безпосереднє можливо застосовувати для формування комп'ютерних процесів кіберзахисту.

Розділ 6 розглядає основи функціонування Національної системи захисту критичної інфраструктури.

Розділ 7 знайомить з системними основами кіберзахисту критичної інфраструктури, практичними заходами щодо протидії кібернападам.

Розділ 8 розглядає принципи комп'ютерного керування промисловими об'єктами, призначення основних компонент.

Розділ 9 пояснює системні основи та особливості кіберзахисту індустріальних систем керування, розглядає цілі захисту та базові стратегії.

Розділ 10 аналізує нормативно-правові основи функціонування Національної системи кібербезпеки, її компоненти та принципи організації. Надається формалізована модель ієрархічної структури.

Розділ 11 розглядає поняття та класифікацію кібератак, уточнює особливості APT атак та сутність проактивної стратегії кіберзахисту. Надається кібернетична модель APT атаки, що дозволяє розробляти відповідні заходи захисту безпосередньої реалізації комп'ютерними засобами.

Розділ 12 пояснює поняття та компоненти інфраструктури кіберзахисту інформаційної системи, зв'язок циклу керування кібербезпекою з компонентами інфрастуктури. Надається графічна модель інфраструктури та її інформаційних процесів.

Розділ 13 показує необхідність, сутність та класифікацію розвідки кіберзагроз. Розглядаються основні моделі порівняльного аналізу поведінки зловмисника та організації відповідної протидії.

Розділ 14 уточнює поняття ІТ аудиту, аудиту безпеки інформації та аудиту кібербезпеки. Розглядаються концепція аудиту кібербезпеки та основні інформаційні процеси в рамках відповідної концептуальної моделі.

Навчальний посібник призначений здобувачам вищої освіти за спеціальностями 122 Комп'ютерні науки і 172 Електронні комунікації та радіотехніка.

1. ВИЗНАЧЕННЯ БАЗОВИХ ТЕРМІНІВ З КІБЕРБЕЗПЕКИ

Закон "Про основні засади забезпечення кібербезпеки України" [1], прийнятий 5 жовтня 2017 року, визначає правові та організаційні основи забезпечення захисту життєва 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.

Закон впроваджує систему термінів необхідних для організації взаємодії фахівців у сфері кіберзахисту. Наведені нижче терміни вживаються в такому значенні:

1) **індикатори кіберзагроз** - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) **інформація про інцидент кібербезпеки** - відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) **інцидент кібербезпеки** (далі - **кіберінцидент**) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) 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;

4) **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;

5) **кібербезпека** - захищеність життєва 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;

6) **кіберзагроза** - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєва важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

7) **кіберзахист** - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

8) **кіберзлочин** (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) **кіберзлочинність** - сукупність кіберзлочинів;

10) **кібероборона** - сукупність 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;

11) **кіберпростір** - 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;

12) **кіберрозвідка** - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) **кібертероризм** - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) **кібершпигунство** - шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) **критична інформаційна інфраструктура** - сукупність об'єктів критичної інформаційної інфраструктури;

16) **Національна телекомунікаційна мережа** - сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення,

оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

17) **національні електронні інформаційні ресурси** (далі - **національні інформаційні ресурси**) - систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєва важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

18) **Національний центр резервування державних інформаційних ресурсів** - організована сукупність об'єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій;

19) **об'єкт критичної інформаційної інфраструктури** - комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на

стале функціонування такого об'єкта критичної інфраструктури;

20) **система управління технологічними процесами** (далі - технологічна система) - автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

21) **системи електронних комунікацій** (далі - комунікаційні системи) - системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних;

22) **система активної протидії агресії у кіберпросторі** - сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак;

23) **активна протидія агресії у кіберпросторі** - дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж,

а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України.

Ця система термінів розроблялась в першу чергу для нормативно-правового регулювання суспільних відношень у сфері кіберзахисту. Тому деякі поняття мають ряд невизначеностей, які можуть стримувати вирішення проблем практичної діяльності технічними фахівцями з кібербезпеки. Наприклад, ключовий термін "кібербезпека" пояснюється через "захищеність життєва важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору". Такий підхід може бути достатнім в рамках юридичної діяльності, але він не дозволяє автоматизованим чином визначати наявність/відсутність стану кібербезпеки в конкретній комп'ютерній системі. Дуже тяжко "пояснити" комп'ютеру за допомогою програмного коду сутність термінів "захищеність" та "важливі інтереси людини і громадянина". Інший приклад. Якщо кіберпостір пояснювати через малозрозумілий термін "віртуальний простір", то аналогічні проблеми можуть виникнути при спробах конкретизувати фізичні параметри кіберпростору. Наприклад, за допомогою "віртуального простору" складно визначити фізичні межі зон відповідальності між організаціями, що співпрацюють в сфері кіберзахисту.

Для організацій ефективної роботи технічних підрозділів кіберзахисту доцільно використовувати системи термінів, які не супроводжуються невизначеностями та дозволяють проводити аналіз проблем забезпечення кібербезпеки з виділенням конкретних складових, що можуть бути зареєстровані фізичними засобами. Таки системи можуть представляти набір професійних термінів, визначення (сенси) яких пов'язані між собою (визначення наступних термінів пояснюється за допомогою раннє визначених термінів). Далі в посібнику (розділ 5) буде представлена така система термінів

для сфери кібербезпеки. Використання таких систем термінів в підрозділах безпеки інформації дозволяє на основі однакого розуміння проблем кіберзахисту швидше формувати рішення для їх подолання та синхронно корегувати визначення термінів у разі необхідності.

Контрольні питання та завдання

1. З чого складається кіберпростір?
2. Різниця між кіберрозвідкою та розвідкою кіберзагроз?
3. Різниця між інформаційною безпекою, безпекою інформації та кібербезпекою?
4. Чим в кіберпросторі відрізняється інцидент кібербезпеки від інформації про інцидент кібербезпеки?
5. Чим відрізняється кіберзагроза від кібератаки?
6. Яку функцію виконує Національний центр резервування державних інформаційних ресурсів?
7. Наведіть приклади конкретних індикаторів кіберзагроз.
8. Наведіть приклади двох кіберінцидентів.
9. Наведіть приклад інформації, що створена, записана, оброблена або збережена у нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів.
10. Наведіть приклад система управління технологічними процесами.

2. ОСНОВИ СИСТЕМНОГО ПІДХОДУ ДО ОПИСУ СКЛАДНИХ ОБ'ЄКТІВ

- **базові поняття теорії систем**
- **системний підхід та формалізація опису складних об'єктів**
- **концепція атрибутивно-трансферної природи інформації**

Постійний розвиток систем інформаційних технології на основі удосконалення та ускладнення комп'ютерних засобів постійно супроводжується значним розширенням можливостей для впровадження більш витончених загроз для цих систем. Однієї з необхідних умов організації ефективного кіберзахисту електронних інформаційних ресурсів є діяльність колективу захисників, яка узгоджена на основі детального розуміння складних процесів в кіберпросторі. Засобами досягнення такої узгодженості можуть бути системний підхід до досліджень складних процесів кіберпростору та формалізований опис цих процесів. В цьому розділі будуть розглянути базові поняття з використання цих засобів в обсязі, який необхідний для розуміння матеріалу цього посібника.

Крім системного підходу в цьому посібнику також буде широко застосовуватися інформаційний підхід, що заснований на такому розумінні сутності інформації, що дозволяє з однакових позицій представити вісь комплекс зазначених процесів. Для цього була обрана концепція атрибутивно-трансферної природи інформації (Attributive-Transfer Nature of Information, ATNI). Ця концепція дозволяє представити основні процеси, що складають сутність кіберзахисту, у вигляді сукупності різних інформацій та операцій з цією інформацією. На відміну від інших підходів до інформації ATNI дозволяє представити конкретну інформацію та її зміст (семантику) в явному вигляді як окремий фізичний об'єкт. В свою чергу, кожне перетворення інформації (інформаційний процес) може бути представлено фізичним процесом з особливими властивостями. Крім цього, ATNI дозволяє кожен

інформаційний об'єкт описати за допомогою математичної мови теорії множин. Такий опис відкриває можливості для подолання невизначеності вербального опису та переходу до формалізованого опису процесів кіберзахисту за допомогою обчислювальних алгоритмів. Це сприяє розробці відповідних програмних засобів автоматизації. Більш детально сутність цього підходу також буде розглянуто в пункті 2.3. цього розділу.

2.1. Базові поняття теорії систем.

Поняття (концепт) – це мислена конструкція, яка поєднує наступні частини:

1) **термін** (група термінів) – це слово, або словосполучення за яким ідентифікується (позначається) об'єкт, явище або процес;

2) **визначення** – це набір слів (термінів), що пояснює сенс поняття.

Формалізовано сутність "поняття" може бути пояснена наступною формулою:

$$\text{“термін”} = \overbrace{\{\underbrace{\text{термін}_1,\ \text{термін}_2,\ \ldots\ \text{термін}_N}_{\text{“визначення”}}\}}^{\text{“поняття”}} \qquad (2.1)$$

Формула 2.1. показує, що поняття складається з "терміну", що позначає об'єкт, та "визначення", що пояснює сенс цього об'єкту. В свою чергу, визначення сформовано з N інших термінів. Приклад поняття "Кібербезпека":

Кібербезпека – це стан інформаційної системи, в якому забезпечуються властивості інформації, що визначені політикою безпеки.

В подальшому всі поняття в посібнику будуть надаватися за цією формулою.

Серед базових понять також будуть використовуватися наступні:

Об'єкт (від лат. *objectum* — «предмет») – все те, на що спрямована практична або познавальна діяльність.

Суб'єкт (від лат. *subjectum* те, що лежить внизу, перебуває в основі) – це об'єкт, який здійснює практичну або пізнавальну діяльність.

Інформація (*від лат. - informātiō «роз'яснення, уявлення, поняття про що-небудь»; - informare «надавати вигляд, форму, навчати; мислити, уявляти»*) – це властивості одного об'єкту, що відображені в іншому об'єкті.

Пояснення: існує багато визначень терміну інформація. Всі вони, як правило, пояснюють сенс інформації через відомості, знання, дані, інтелект та інші різні терміни, які, в свою чергу, пояснюються тільки через інформацію. Такий підхід "замкнутого кола" веде до масштабування семантичних невизначеностей при описі складних систем та заважає досягненню конструктивного результату. В цьому посібнику будемо використовувати запропоноване поняття, яке позбавлено цього недоліку. Більш детальне пояснення цього поняття буде надано в розділі 5, де буде описаний атрибутивно-трансферний підхід до природи інформації.

Ана́ліз (від *грец.* αναλυσις — «розклад», «розчленування») — фізичне чи уявне розкладання на частини об'єкту досліджень.

Синтез (др.-грец. σύνθεσις «з'єднання, складання, зв'язування»; від συν-«спільна дія, співучасть» + θέσις «розстановка, розміщення, розподіл) — процес об'єднання раніше розрізнених речей або понять.

Критерій (від *лат. critērium*, яке зводиться до *грец.* χριτήριον — *здатність розрізнення; засіб судження, мірило*, пов'язаного з *грец.* χρινω — *розділяю, розрізняю*) — ознака, за якою визначають наявність якоїсь властивості.

Оптимізація (*англ. optimization, optimisation*) чи **удосконалення** — процес досягнення

найвигідніших характеристик, співвідношень (наприклад, оптимізація обчислювальних процесів, фінансових витрат на розробку системи, часу реагування на кібератаку тощо).

Проце́с (лат. *processus* — рух, англ. *process*) — послідовна зміна предметів або явищ, що відбувається закономірним порядком; сукупність ряду послідовних дій, спрямованих на досягнення певного результату; послідовна зміна станів об'єкту в часі.

Ефект (лат. effectus — виконання, дія, лат. efficio — виконую, дію) – результат (наслідок) діяльності або фізичне явище.

Ефективність – відношення результату до витрат на цей результат (наприклад, бажана технологія обробки інформації (ТОІ) може бути реалізована на базі двох різних комп'ютерних систем (КС). Ефективність ТОІ буде краще у випадку коли застосовується та КС, що забезпечує менші час та вартість обробки).

2.2. Системний підхід та формалізація опису складних об'єктів

Системний підхід - ефективний спосіб ментальної діяльності, який забезпечує значні досягнення в науці, в техніці та виробництві. Почав активно застосовуватися в другій половині XX століття на основі методів *теорії складних систем* та *системології*. Найбільш розповсюджені методи системного підходу – *системний аналіз* та *системний синтез*. Ознайомимся з відповідними поняттями.

Системний підхід (англ. *Systems thinking* — системне мислення) — метод практичної або пізнавальної діяльності, що оснований на представленні об'єкту досліджень у вигляді системи.

Системний аналіз - прикладний напрям теорії систем, що застосовується для аналізу складних та слабкоформалізуемих об'єктів (проблем).

Системний синтез - процес об'єднання розрізнених об’єктів з метою формування нових складних систем з заданими властивостями.

Система - (від дав.-гр. σύστημα — «сполучення», «ціле», «з'єднання») —об’єкт, що складається з сукупності взаємопов'язаних частин, які окремо не мають деяких властивостей цього складеного об’єкту.

Компонента системи (від лат. *componens, родовий відмінок componentis — складаючий*), підсистема – це складова частина системи, що сама є системою.

Елемент системи – це складова частина системи, що не є системою, або не розглядається як система.

Зв’язок (відношення) між частинами системи – фізичний або уявний процес, що об’єднує частини системи в один об’єкт.

Функція системи – дія (перетворення), яке здійснює система в зовнішньому середовищі.

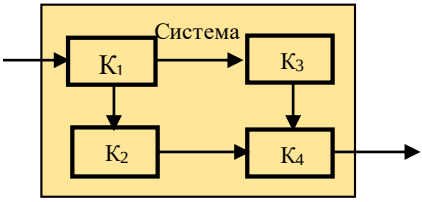
Функція підсистеми (функція компоненти) – дія (перетворення), яке здійснює компонента системи для забезпечення цілісності системи або її функції.

В рамках теорії складних систем визначають більше 1500 властивостей систем. З розвитком методології дослідження систем ця кількість постійно збільшується. Для розуміння матеріалу цього посібника буде достатньо ознайомитися тільки з наступними властивостями.

Склад системи – перелік частин системи.

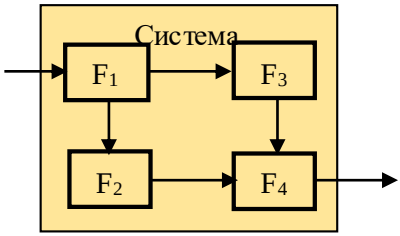
Структура системи – сукупність частин системи та зв’язків між ними.

На малюнку 2.1. в графічному вигляді представлена структура системи ($К_i$ – компонента системи за номером *i*).



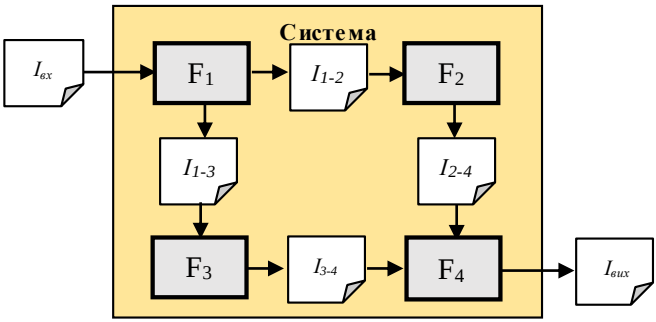
Мал. 2.1. Структура системи

Функціональна структура системи (ФС) – структура системи, в якої компоненти системи представлені у вигляді функцій (F_i) складових підсистем.



Мал. 2.2. Функціональна структура системи

Інформаційно-функціональна структура системи (ІФС) – структура системи, в якої компоненти системи представлені у вигляді функцій складових підсистем, а зв'язки – інформацією (I_m – інформація з індексом m), якою обмінюються підсистеми.



Мал. 2.3. Інформаційно-функціональна структура системи

Емерджентність (англ. *emergence* — виникнення, поява нового) - властивість об'єкта мати ознаки, відмінні від ознак елементів його складових.

Організація системи (від грец. ὄργανον — інструмент) - упорядкованість виконання функцій підсистем в рамках функціональної структурі системи.

Наприклад, в рамках однієї функціональної структури (мал. 2.2.) можливо виділити два варіанти організації (упорядкованості) виконання функцій підсистем (F_1, F_2, F_3, F_4 та F_1, F_3, F_2, F_4).

В більш вузькому сенсі термін "організація" часто використовується для позначення групи людей, які виконують свої посадові обов'язки для досягнення певної колективної мети.

Види систем.

Технічна система – система, що складається з технічних засобів.

Організаційна система – система, функції якої реалізуються колективом людей.

Організаційно-технічна система – система, функціонування якої забезпечується узгодженої діяльністю технічних засобів та людей.

Складна система – система, опис якої є слабоформалізуємий, тобто складно однозначно визнати властивості системи: складові, структуру, організацію, можливі стани, поведінку та інші характеристики.

Кібернетична (керована) система (від дав.-гр. κυβερνήτης — «керманич», «стерновий») – система, яка на основі внутрішнього стану (потреб) та стану зовнішнього середовища визначає та реалізує свою поведінку.

Таки системи можуть мати різну фізичну природу (хімічну, біологічну, технічну, соціальну тощо), та функціонують на основі однакових закономірностей:

- системи складаються з об'єкту та суб'єкту керування;
- суб'єкт керування отримує інформацію про стан об'єкту керування;

- суб'єкт керування приймає рішення про керуючий вплив на об'єкт керування та реалізує його;
- на основі впливу об'єкт керування змінює свій стан.

Синергетична система (англ. *Synergetics*; від грец. син — «спільне» і ергос — «дія») – система, яка створюється та розвивається на основі процесів самоорганізації. Також можуть мати різну фізичну природу (фізичну, хімічну, біологічну, соціальну тощо): хімічні реакції на основі каталізаторів; метеорологічні явища; біологічні організми; штучні нейронні мережі; соціальні системи тощо.

Кібернетичні та синергетичні системи відносяться до класу дисипативних систем, тобто систем, які можуть існувати тільки в умовах обміну енергією, речовиною та інформацією з зовнішнім середовищем.

В рамках досліджень складних систем використовується метод формалізації опису системи (далі – формалізація).

Формалізація – це процес подолання невизначеностей в описі складних систем.

Розрізняють наступні рівні опису:

1) опис на основі мови побутового спілкування (як правило, не застосовуються узгоджені поняття, описи мають багато невизначеностей відносно властивостей об'єкту опису);

2) формалізований опис на основі використання сукупності професійних термінів (тезаурусу). Кожний термін має своє визначення. Кращим вважається такий тезаурус, в якому вся сукупність понять формується на основі групи базових тверджень (аксіом, постулатів). Прикладом тезауруса, що створений на основі аксіоматичного підходу є взаємопов'язані поняття Евклідової геометрії;

3) формалізований опис на основі використання кінцевої множини графічних знаків. Загальний сенс кожного знаку визначений заздалегідь. Наприклад, для опису інформаційно-функціональної структури (мал. 2.3.)

застосовується алфавіт з трьох знаків: “прямокутник” – система (компонента); “стрілка” – процес обміну інформацією; “аркуш” – інформація);

4) формалізований опис на основі використання математичних конструкцій (вищий рівень формалізації). Приклад – математичне представлення інформації (формула 2.1 в пункті 2.3).

2.3. Концепція атрибутивно-трансферної природи інформації

Особливістю концепції ATNI [19] є те, що вона не пояснює інформацію за допомогою поріднених термінів “відомості”, “дані” “знаки”, “знання”, “ментальні представлення”, “семантика”, “інтелект”, “свідомість” та багато інших, що самі часто пояснюються через “інформацію”. ATNI розглядає її тільки як фізичний об’єкт, що сформований особливим чином за допомогою фізичного впливу. Термін “інформація” розкривається за допомогою наступного поняття (концепту):

> ***інформація про об’єкт A в об’єкті B***, *I(A:B)* – це властивість об’єкта *B*, що придбана в результаті фізичної взаємодії з іншим об’єктом *A* і є відображенням властивості цього об’єкту *A*.

Три приклади, що пояснюють цей концепт. Проміні сонця сформували тінь скелі, що повторює форму скелі. Друга ситуація: на вологому ґрунті дика тварина залишає ланцюжок слідів, форма кожного з яких містить унікальні особливості, як виду, так і самої тварини. Третя ситуація: людина – свідок небезпечної події (сильний землетрус в океані, раптове виверження вулкана чи ін.) складає текстове повідомлення. Передане каналами зв'язку повідомлення може призвести до кардинальних змін у житті суспільства (запровадження надзвичайного стану, евакуація населення тощо). Загальне, що

поєднує всі ці різні ситуації – наявність таких фізичних взаємодій між об'єктами, результатами яких є нові придбані властивості об'єктів, що відображають властивість об'єкту, що впливає.

Запропонований концепт може бути “більш суворим”, якщо для його опису використати математичні конструкції теорії множин:

$$I(at_iA{:}B) = (B, at_{J+1}B) \mid f_{map}^{(t1)}:\ at_iA\, I \rightarrow at_{J+1}B, \qquad (2.1)$$

тобто, інформація про властивість (атрибут) at_iA об’єкту A в об’єкті B – це сам об’єкт B з придбаною (в момент часу t_1) властивістю $at_{J+1}B$, яка сформована впливом $f_{map}^{(t1)}$, що відображає властивість at_iA (at_iA=*“півсфера”*) в нової властивості $at_{J+1}B$ ($at_{J+1}B$=*“півсфера”*). У цьому описі кожний об’єкт представляє собою множину його властивостей (атрибутів):

$$A=\{at_iA\},\ i=1,\ \ldots,\ I; \quad B=\{at_jB\},\ j=1,\ \ldots,\ J. \qquad (2)$$

Кожна властивість об’єкту розглядається як впорядкована сукупність елементів цього об’єкту, що дає можливість представити її як підмножину на декартовому добутку множин, що є осями системи координат в місці розташування цього об’єкту. Приклад:

$$\text{“півсфера”} = at_iA \subset X_A \times Y_A \times Z_A, \qquad (3)$$

де X_A, Y_A, Z_A - осі системи координат, що дозволяють визначити місце розташування об’єкту A. Кожний елемент підмножини at_iA – упорядкована трійка відповідних елементів осей координат:

$$(x_A, y_A, z_A) \in at_iA = \text{“півсфера”}. \quad (4)$$

Зрозуміло, що вираз (3) не обмежується застосуванням тільки для властивості *“півсфера”*, яка використовувалась тільки для візуалізації прикладу.

Запропонована парадигма інформації дозволяє визначити наступні супутні поняття:

1) об’єкт *A* - це *джерело інформації* $I(at_iA:B)$;

2) об’єкт *B* – це *носій інформації* $I(at_iA:B)$, який визначає місцеположення інформації в просторі-часі;

3) властивість об’єкту *A* $at_iA = essence[I(at_iA:B)]$ – це *сутність інформації* $I(at_iA:B)$;

4) придбана властивість об’єкту *B* (носій інформації) $at_{J+1}B$ – це *семантика (сенс) інформації* $I(at_iA:B)$, тобто, $at_{J+1}B = semantic[I(at_iA:B)]$. В семантиці інформації відображена властивість об’єкту *A*, шо раніше була визначена як сутність конкретної інформації $I(at_iA:B)$. Якщо розглядаються декілька семантик інформації одного носія *B*, то семантику інформації можливо означати просто як $semantic(A)$;

5) f_{map} – оператор відображення (індекс $_{map}$ – від англійського слова *mapping*, відображення) визначає характер взаємодії об’єктів під час формування інформації.

Розглянута парадигма ATNI була побудована на твердженні, що інформація, як особливий феномен фізичного світу могла, існувати ще до появи життя (біологічних систем). Такий підхід дозволив описати інформацію через терміни, які можна пов'язати із неживою природою: об'єкт, властивість, вплив, відображення. Приклад інформації з часів до появи життя – тінь скелі, що сформована сонячним світлом та повторює форму скелі. Така інформація

$$I(at_iA:B) = I(\text{форма скелі : поверхня}) = \text{тінь скелі}$$

існувала тільки при наявності сонячного світла, яке виконувало роль інфоутворюючого впливу (f_{map}). На той час ця інформація ніде не використовувалася та зникала разом зі світлом. Але у подальшому цей феномен став масштабна використовуватися спочатку в біологічних, а потім, в технічних кібернетичних (керованих) системах для визначення їх поведінки в залежності від впливу зовнішнього середовища. Можливо також впевнено стверджувати, що інформація виконує основну роль в створенні та функціонуванні синергетичних (самоорганізованих) систем.

Для подальшого розгляду інформаційних процесів пропонується впровадити наступне поняття:

інформаційне середовище кібернетичної системи *(далі – інформаційне середовище, Information Environment, IE)* – це набір взаємопов'язаних елементів однакової фізичної природи (далі – операційні елементи, Operating Elements, OE), який дозволяє:

- фіксувати результати інформаційних впливів у вигляді зміни значень властивостей цих елементів (відповідно до парадигми ATNI набуті значення властивостей – це семантики інформації, далі – семантики);
- зберігати семантики інформації;
- формувати різні семантичні конструкції на основі семантики інформації;
- виконувати різні операції над семантиками та семантичними конструкціями (порівняння, об'єднання, аналіз, синтез та багато інших);
- створювати та забезпечувати процеси використання семантики на користь інших систем;
- на основі семантики формувати інформаційні впливи для обміну семантичними конструкціями з іншими кібернетичними системами.

У людини та вищих тварин, яких відносять до біологічних кібернетичних систем, можливо виділити наступні два види найбільш відомих інформаційних середовищ:

- білкове інформаційне середовище (Protein Information Environment, PIE);
- нейронне інформаційне середовище (Neural Information Environment, NIE).

Роль операційних елементів PIE виконують білки, які у своїй структурі відображають та зберігають особливості ділянок ДНК біологічної істоти. У свою чергу, білки є основним будівельним матеріалом для формування та забезпечення функціонування біологічного організму. Основу NIE складають нейрони, в наборах (патернах) яких за допомогою органів почуття (сенсорів) відображаються інформаційні впливи (f_{map}) зовнішнього/внутрішнього середовища біологічного організму. На основі порівняння поточних семантик та набутого досвіду (тобто, раніше сформованих семантик) визначається траєкторія поведінки системи.

Технічні кібернетичні системи, що керуються за допомогою комп'ютерних засобів, використовують комп'ютерне інформаційне середовище (*Computer Information Environment, CIE*). Операційними елементами *CIE* є електронні регістри пам'яті, з'єднані лініями передачі електричних сигналів. Кожен регістр складається із сукупності тригерів. Один тригер – один осередок пам'яті. Тригери - це напівпровідникові пристрої, які під впливом електричного сигналу можуть перемикатися в один із двох можливих станів. Умовні назви значень станів – логічні двійкові одиниці "1" чи "0". За допомогою сенсорів кібернетичних систем (засобів вводу/виводу) формуються семантики *CIE* у вигляді наборів логічних двійкових одиниць (бітів), що зберігаються в регістрах, передаються дискретними електричними сигналами по лініям зв'язку, перетворюються за допомогою арифметично-логічних пристроїв (АЛП) обчислювальних процесорів. АЛП

дозволяють на основі семантик від сенсорів формувати різні семантичні конструкції, які раніше не існували в цьому середовищі.

Висновки за розділом 2

- **Поняття** (концепт) – це мислена конструкція, яка поєднує наступні частини: “термін” = “визначення”.
- **Термін** (група термінів) – це слово, або словосполучення за яким ідентифікується (позначається) об’єкт, явище або процес.
- **Визначення** – це набір слів (термінів), що пояснює сенс поняття.
- **Об’єкт** (від лат. *objectum* — «предмет») – все те, на що спрямована практична або познавальна діяльність.
- **Суб’єкт** (від лат. *subjectum* те, що лежить внизу, перебуває в основі) – це об’єкт, який здійснює практичну або пізнавальну діяльність.
- **Інформація** (*від лат. - informātiō «роз'яснення, уявлення, поняття про що-небудь»; - informare «надавати вигляд, форму, навчати; мислити, уявляти»*) – це властивості одного об’єкту, що відображені в іншому об’єкті.
- **Аналіз** (від грец. αναλυσις — «розклад», «розчленування») — фізичне чи уявне розкладання на частини об’єкту досліджень.
- **Синтез** (др.-грец. σύνθεσις «з'єднання, складання, зв'язування»; від συν-«спільна дія, співучасть» + θέσις «розстановка, розміщення, розподіл) — процес об'єднання раніше розрізнених речей або понять.
- **Критерій** (від лат. *critērium*, яке зводиться до грец. χριτήριον — *здатність розрізнення; засіб судження, мірило*, пов'язаного з грец. χρινω — *розділяю, розрізняю*) — ознака, за якою визначають наявність якоїсь властивості.

• **Оптимізація** (англ. *optimization, optimisation*) чи **удосконалення** — процес досягнення найвигідніших характеристик, співвідношень (наприклад, оптимізація обчислювальних процесів, фінансових витрат на розробку системи, часу реагування на кібератаку тощо).

• **Процес** (лат. *processus* — рух, англ. *process*) — послідовна зміна предметів або явищ, що відбувається закономірним порядком; сукупність ряду послідовних дій, спрямованих на досягнення певного результату; послідовна зміна станів об'єкту в часі.

• **Ефект** (лат. effectus — виконання, дія, лат. efficio — виконую, дію) – результат (наслідок) діяльності або фізичне явище.

• **Ефективність** – відношення результату до витрат на цей результат (наприклад, бажана технологія обробки інформації (ТОІ) може бути реалізована на базі двох різних комп'ютерних систем (КС). Ефективність ТОІ буде краще у випадку коли застосовується та КС, що забезпечує менші час та вартість обробки).

• **Системний підхід** (англ. *Systems thinking* — системне мислення) — метод практичної або пізнавальної діяльності, що оснований на представленні об'єкту досліджень у вигляді системи.

• **Система** - (від дав.-гр. σύστημα — «сполучення», «ціле», «з'єднання») —об'єкт, що складається з сукупності взаємопов'язаних частин, які окремо не мають деяких властивостей цього складеного об'єкту.

• **Компонента системи** (від лат. *componens, родовий відмінок componentis — складаючий*), підсистема – це складова частина системи, що сама є системою.

• **Елемент системи** – це складова частина системи, що не є системою, або не розглядається як система.

- **Зв'язок (відношення)** між частинами системи – фізичний або уявний процес, що об'єднує частини системи в один об'єкт.
- **Функція системи** – дія (перетворення), яке здійснює система в зовнішньому середовищі.
- **Функція підсистеми** (функція компоненти) – дія (перетворення), яке здійснює компонента системи для забезпечення цілісності системи або її функції.
- **Склад системи** – перелік частин системи.
- **Структура системи** – сукупність частин системи та зв'язків між ними.
- **Функціональна структура системи** (ФС) – структура системи, в якої компоненти системи представлені у вигляді функцій (F_i) складових підсистем.
- **Інформаційно-функціональна структура системи** (ІФС) – структура системи, в якої компоненти системи представлені у вигляді функцій складових підсистем, а зв'язки – інформацією, якою обмінюються підсистеми.
- **Емерджентність** (англ. *emergence* — виникнення, поява нового) - властивість об'єкта мати ознаки, відмінні від ознак елементів його складових.
- **Організація системи** (від грец. ὄργανον — інструмент) - упорядкованість виконання функцій підсистем в рамках функціональної структурі системи.
- **Технічна система** – система, що складається з технічних засобів.
- **Організаційна система** – система, функції якої реалізуються колективом людей.
- **Організаційно-технічна система** – система, функціонування якої забезпечується узгодженої діяльністю технічних засобів та людей.
- **Складна система** – система, опис якої є слабоформалізуємий, тобто складно однозначно визнати

властивості системи: складові, структуру, організацію, можливі стани, поведінку та інші характеристики.

- **Кібернетична (керована) система** (від дав.-гр. κυβερνήτης — «керманич», «стерновий») – система, яка на основі внутрішнього стану (потреб) та стану зовнішнього середовища визначає та реалізує свою поведінку.
- **Синергетична система** (англ. *Synergetics*; від грец. син — «спільне» і ергос — «дія») – система, яка створюється та розвивається на основі процесів самоорганізації.

Контрольні питання та завдання

1. Чим синергетична система відрізняється від кібернетичної?
2. Виділити ознаки, за якими людину можливо віднести до синергетичної системи.
3. Виділити ознаки, за якими людину можливо віднести до кібернетичної системи.
4. До якого класу систем відноситься автоматична система на основі мікропроцесору?
5. До якого класу систем відноситься інформаційна система?
6. Можливо лі проводити оптимізацію системи без заданих критеріїв?
7. Для чого потрібні заходи формалізації?
8. В чому сутність системного підходу?
9. Сутність аксіоматичного підходу?
10. Ефективність інформаційної системи?

3. КІБЕРПРОСТІР ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

- **кіберпростір як фізичне середовище**
- **інформаційно-комунікаційна система та її структура**
- **інформаційна система**
- **багаторівнева структура комп'ютерної мережі корпоративної інформаційної системи**
- **фізичні основи процесів обробки інформації в ІКС**

У світовій практиці широке використання термінів “кіберпростір” (“cyberspace”) і “кібербезпека” (“cybersecurity”, “cyberspace security”) почалося з початку 21 століття (в 2005-2007 роках). Вони все частіше стали застосовуватися там, де раніше використовувалися терміни “безпека систем інформаційних технологій” (“Information Technology Systems security”, ITS security) і “комп'ютерна безпека” (“computer security”) [2]. Під терміном *кібербезпека*, як правило, розуміється забезпечення властивостей інформації (конфіденційність, цілісність, доступність та інші) в *кіберпросторі* [3].

У нашій країні з кінця 90-х років минулого століття для позначення розподілених електронних систем, які об'єднують в собі комп'ютерні технології та технології електрозв'язку, застосовувався термін “інформаційно-комунікаційні системи”(ІКС). За минулі роки в рамках формування та реалізації державної політики захисту інформації в ІКС було розроблено значну кількість (понад 200) нормативно-правових документів, які знайшли широке застосування. Очевидно, що нормотворча діяльність в сфері забезпечення кібернетичної безпеки України, що активно проводиться на даний час, повинна враховувати необхідність гармонізації нових регулюючих актів з раніше напрацьованими документами із захисту інформації в ІКС. Для цього потрібно визначити

сутність ІКС та її складових, з'ясувати взаємозв'язок ІКС та кіберпростору

3.1. Кіберпростір як фізичне середовище

Ключовим терміном для розуміння сутності "кібербезпеки" є "кіберпростір". Зазвичай в рамках його пов'язують з:

глобальними розподіленими системами, що реалізовують цифрові комп'ютерні технології обробки інформації;

віртуальним середовищем на основі цих систем, в якому можуть існувати видумані активні об'єкти (різноманітні герої комп'ютерних ігор і цифрової анімації, симуляційні моделі та інше). Ці інформаційні об'єкти, що існують тільки в комп'ютерах, здатні здійснювати реальний сенсорний вплив на психіку людини (візуальний, звуковий та іншій);

можливістю здійснювати приховані (анонімні) інформаційні впливи на людей і різні пристрої;

відсутністю "територіальних кордонів" при комунікаціях людей різних держав (відсутність "кіберкордонів").

Так, наприклад, в міжнародному стандарті "ISO/IEC 27032: 2012 Information technology – Security techniques – Guide lines for cybersecurity" [3] пропонується наступне визначення: "кіберпростір - це складне середовище, сформоване в Інтернеті в результаті взаємодії людей, програмного забезпечення і послуг за допомогою технологічних пристроїв і мереж, підключених до нього, і яке не існує в будь-якій фізичній формі". Таке визначення, по-перше, обмежує кіберпростір ситуаціями використання комп'ютерних технологій тільки в рамках Інтернет. По-друге, відмовляючи йому в наявності фізичної форми, позбавляє його матеріальності і заперечує можливість проведення об'єктивного (інструментального) контролю його станів. Останнє є дуже критичним для забезпечення кібербезпеки.

Багато дослідників все ж представляють кіберпростір таким середовищем, яке утворено цілком фізичними системами і

мережами. Такий підхід дозволяє говорити і про існування фізичних національних "кіберкордонів", які формуються відповідними інженерно-технічними комплексами. В рамках цих кордонів може здійснюватися як фізичний контроль технічного обладнання, так і інформаційних потоків, які перетинають ці межі [4].

У національному законодавстві здебільшого додержуються позицій фізичних засад: "кіберпростір – 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" [1]. Але застосування терміну "середовище (віртуальний простір)" без визначення його фізичної сутності не дозволяє, подолати іншу невизначеність щодо характеру взаємозв'язку між поняттями "кіберпростір" і поняттями "сумісні (з'єднані) комунікаційні системи" та "електронні комунікації".

Додатково відносно проблем щодо розуміння сутності кіберпростору важливо відзначити аспект його сприйняття людиною у порівнянні зі сприйняттям звичайного фізичного простору. У звичайному просторі людина сприймає світ через безпосередні контакти з іншими об'єктами (смак, дотик), або - на відстані (зір, слух і нюх). Дистанційне сприйняття здійснюється через природні носії інформації (сонячне світло, акустичні коливання, хімічні сполуки) і обмежується кордонами сприйняття, які залежать від можливостей органів чуття. Поява мови та письма значно розширило ці межі. Однак ці два канали обміну інформацією засновані на наявності посередників між реальною подією і суб'єктом пізнання. Ці посередники за допомогою знаків формують та передають повідомлення про події. Але інтерпретація посередниками переданої інформації часто призводить до порушення її достовірності. Отримане знакове повідомлення взагалі може бути про видумані події. Наслідком цього стає спотворене сприйняття

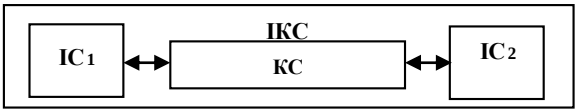
реального світу. Поява та широке застосування інформаційно-комунікаційних технологій не тільки значно розширює межі віддаленого сприйняття, збільшує можливості людини щодо аналізу прийнятої інформації і формуванні нових знань. В таких умовах навіть на інтуїтивному рівні виникає потреба асоціювати "нові можливості в фізичному просторі" і "комп'ютерні (кібернетичні) технології" в рамках нового ментального об'єкту, який назвали "кіберпростір". Однака впровадження нових можливостей віддаленого спілкування не тільки не вирішує проблему "посередника-інтерпретатора", але і породжує додаткову проблему відсутності психологічного контролю за зловмисником. В умовах особистого спілкування людина може спостерігати деталі поведінки співрозмовника, які можуть свідчить про його дійсні наміри. Наприклад, особливі рухи рук, ніг, зміна в положенні тіла, що супроводжують недостовірне повідомлення, допомагають виявити небезпечну людину. В цьому аспекті дистанційне спілкування через "кіберпростір" не дозволяє проводити додатковий психологічний контроль за співрозмовником та значно розширює коло загроз для особи: виманювання грошей за допомогою повідомлень про брехливі події відносно близької людини; отримання PIN коду підставним співробітником банку; вплив на психологічний стан підлітка з метою доведення до самогубства та багато іншого. Захист від цих та ряду інших загроз, які пов'язують з використанням кіберпростору, не можливо забезпечити на основі класичних підходів щодо безпеки інформації, які основані на підтримці тільки її конфіденційності, цілісності та доступності. Необхідне таки визначення кіберпростору та кібербезпеки, які дозволяють охопити перелічені загрози.

Ці та ряд інших семантичних невизначеностей між поняттями у галузі забезпечення кібербезпеки значно звужують можливості щодо розробки методів аналізу і прогнозування складних кібератак, вибору ефективних засобів та заходів кіберзахисту. У подальшому буде розглянуто варіант подолання цієї проблеми через розуміння фізичної сутності кіберпростору, основу якого складає сукупність інформаційно-комунікаційних систем. Далі в цьому розділі будуть визначені сутність, склад та структура таких систем, види їх сервісів. Окремо будуть розглянути характеристики інформаційних та комп'ютерних систем, особливості побудови та функціонування

сучасних корпоративних комп'ютерних мереж з великою кількістю персоналу. На основі цього матеріалу буде представлена концептуальна модель кіберпростору та кібербезпеки (розділ 5), що була розроблена за допомогою засобів термінологічної, графічної та математичної формалізації.

3.2. Інформаційно-комунікаційна система та її структура

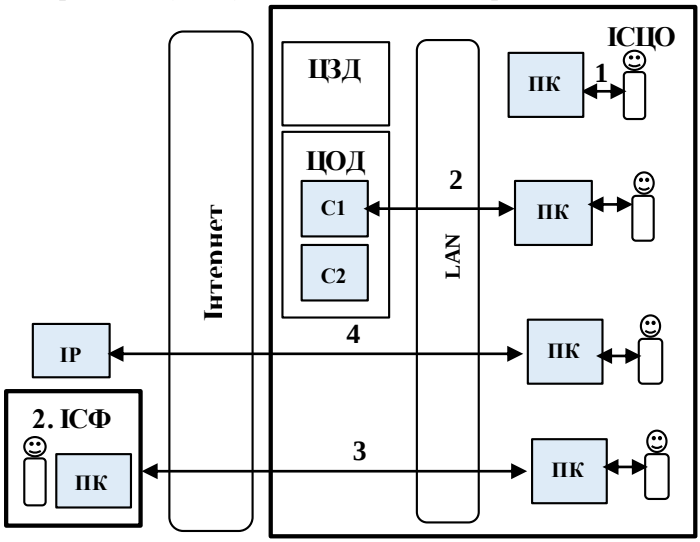
Компонентами сучасних інформаційно-комунікаційних систем (ІКС) є інформаційні системи (ІС) та електронні комунікаційні системи (КС), які у процесі обробки інформації діють як єдине ціле [5]. За допомогою ІС під час обробки інформації виконуються операції її збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації та обміну між структурними компонентами. В свою чергу, КС виконують функції, що забезпечують обмін інформацією між інформаційними системами, які розташовані на віддалених об'єктах. На малюнку 3.1 надається структура елементарної ІКС, що включає в себе дві інформаційні системи (ІС) і комунікаційну систему (КС). Прикладом реалізації такої структури є корпоративна ІКС, в якої локальні комп'ютерні мережі двох філій одної організації об'єднуються за допомогою комунікаційної системи супутникового зв'язку.



Мал. 3.1. Структура елементарної інформаційно-комунікаційної системи

Часто в рамках корпоративних ІКС в якості КС використовується функції обміну даними глобальної системи Інтернет. Під терміном "корпоративна система" будемо розуміти таки системи, які належать власникам, що надає їм можливість самостійно визначать порядок її використання в своїх інтересах (підключення тільки корпоративних користувачів, політика безпеки, політика ефективної експлуатації та інше). На відміну від публічних систем, до послуг яких за гроші можуть бути підключені різні користувачі (наприклад, Інтернет), корпоративні системи забезпечують кращий рівень безпеки інформації, але мають низку економічну ефективність. На малюнку 3.2 представлена типова

структура сучасної корпоративної ІКС, що в якості КС використовує транспортні послуги публічної системи Інтернет.



ІСЦО - ІС центрального офісу
ІСФ - ІС філіалу
ЦОД - центр обробки даних
ЦЗД - центр збереження даних
ІР - Інтернет ресурс

Види сервісів
1 – локальний сервіс
2 – локальний мережевий сервіс
3 –корпоративний Інтернет сервіс
4 – Інтернет сервіс

Мал. 3.2. Структура типової корпоративної інформаційно-комунікаційної системи. Види сервісів.

Така ІКС складається з:
- корпоративних інформаційних систем ІС центрального офісу (ІСЦО) та ІС філіалу (ІСФ, може бути декілька);
- комунікаційної системи КС, функції якої виконує Інтернет.
В свою чергу, ІСЦО складається з:
- комп'ютерної системи ЦО (КСЦО);
- персоналу (на малюнку тільки користувачі);
- та інформації, яка оброблюється в інтересах користувачів.
До складу КСЦО входять:
- локальна мережа (LAN);
- персональні комп'ютери користувачів (ПК);
- комп'ютери, що виконують роль серверів (С);
- центр обробки даних (ЦОД), що об'єднує всі сервери ІС;
- центр збереження даних (ЦЗД).
КСЦО реалізує обробку інформації в інтересах корпоративних користувачів за принципами технології "клієнт-сервер". Тобто, за запитами користувачів (клієнтів) сервери надають послуги (сервіси). З точку зору полегшення подальшого аналізу стану кібербезпеки такої корпоративної ІКС доцільно виділити наступні види сервісів:

1) локальний сервіс (ЛС). Забезпечується програмними застосунками ПК користувача;

2) локальний мережевий сервіс (ЛМС). Забезпечується спеціалізованими серверами ЦОД (наприклад: веб-сервер; поштовий корпоративний сервер; сервер бази даних; ftp-сервер та інші). Примітка: потрібно розрізняти апаратні та програмні сервери. На одному апаратному серверу (комп'ютеру з підвищеною продуктивністю) може бути розміщено декілька програмних серверів;

3) корпоративний Інтернет сервіс (КІС). Забезпечує віддалені запити від корпоративних користувачів через Інтернет спеціалізованими серверами ЦОД;

4) Інтернет сервіс (ІС). Забезпечує корпоративним користувачам доступ до публічних серверів Інтернет (наприклад: доступ браузера до пошукових Інтернет систем; доступ до віддалених баз знань; публічний поштовий сервіс та інше).

Кожний з перелічених видив сервісів має свої особливості, які необхідно враховувати при організації заходів кіберзахисту.

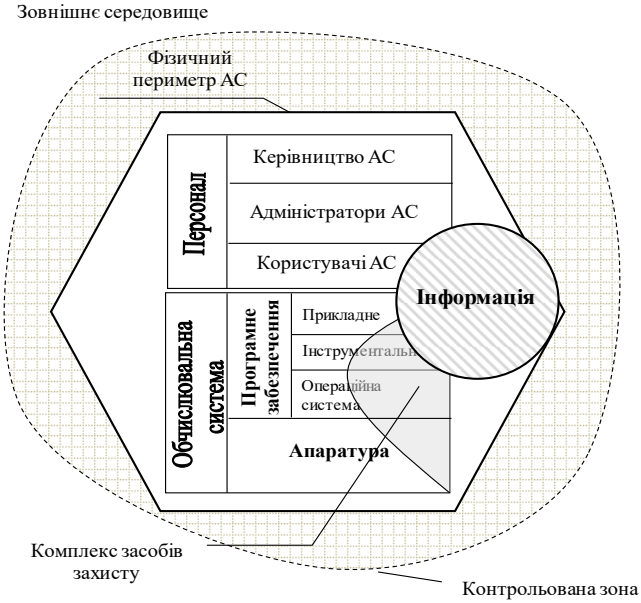
3.3. Інформаційна система

Обробка інформації в інтересах людини реалізується інформаційними (автоматизованими) системами, які є основними компонентами ІКС. Основна мета кібератак – це порушення комп'ютерних технологій обробки інформації рамках інформаційних систем. Для фахівців кіберзахисту важливо розуміти принципи організації та функціонування таких систем, знати фізичні основи перетворення інформації за допомогою комп'ютерних засобів.

В нормативно-правовому національному середовищі Інформаційну (автоматизовану) систему визначають як організаційно-технічну систему, що об'єднує:

- обчислювальну систему (апаратне та програмне забезпечення);
- фізичне середовище (зовнішнє середовище та контрольована зону);
- персонал (керівництво, адміністратори і користувачі);
- оброблювану інформацію та порядок її обробки (тобто, технологію обробки інформації, ТОІ).

На малюнку 3.3. представлена узагальнена структура інформаційної системи [6].

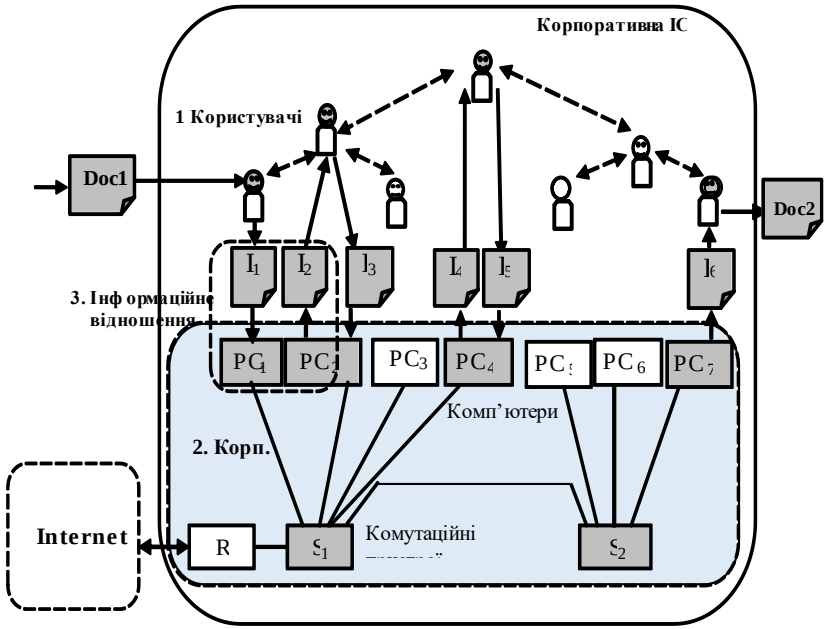


Мал. 3.3. Узагальнена структура інформаційної (автоматизованої) системи

Обчислювальна (комп'ютерна) система і персонал розміщується в конкретному фізичному середовищі (кімната, поверх, будинок, декілька будинків та інше), що має периметр ІС який відділяє внутрішню зону від зовнішньої. В рамках зовнішнього середовища визначається контрольована зона. Під контрольованою зоною (територією) розуміють зону, в рамках якої неможлива несанкціонована поява сторонніх осіб.

Недолік цієї широко розповсюдженої узагальненої структури ІС в тому, що вона не пояснює сутності такої її складової, як "технологія обробки інформації". Значна кількість кібератак направлена на порушення роботи ІС з метою припинення корпоративних бізнес-процесів. Для організації

результативного кіберзахисту доцільно деталізувати сутність ТОІ на рівні візуалізації. За допомогою графічних засобів формалізації більш детально розглянемо сегмент кіберпростору на основі типової корпоративної ІС для обробки документів. На малюнку 3.4 представлена структура такого сегменту.



Мал. 3.4. Типова структура корпоративної ІС і технологія обробки інформації

В рамках структури відображені наступні компоненти:

1) користувачі ІС (співробітники корпорації, технічні пристрої або системи, які використовують сервіси ІС). Пунктирні стрілки – організаційні зв'язки між користувачами (начальник – підлеглий);

2) комп'ютерна система ІС у вигляді корпоративної мережі (КМ);

3) інформаційні ресурси у вигляді даних, які можуть перетворюватися процесорами комп'ютерів, зберігатися в

різних пристроях пам'яті або передаватися за допомогою мережі між комп'ютерами;

4) набір інформаційних сервісів з обробки даних, якими можу скористатися користувачі в своїх інтересах. Можливості сервісів визначаються відповідними програмними застосунками персональних комп'ютерів (РС);

5) інформаційні відносини між користувачами ІС, які можуть виникати підчас обробки інформації. Інформаційне відношення можливо представити як сукупність: вхідних даних від користувача (I_1); відповідного сервісу, що оброблює ці дані (Serv); інформаційного продукту (вихідної інформації, I_2), що формується сервісом в інтересах кінцевого користувача. На малюнку пунктиром показано тільки одне інформаційне відношення (ІВ).

Інтереси користувача можуть бути задані у вигляді вимог до інформаційного продукту. Наприклад, доступ до інформаційний продукту має тільки коло визначених осіб (конфіденційність інформації). Або, набір даних під час передачі файлу по мережі не може бути змінений (цілісність інформації). Можуть бути і інші властивості інформації, які відповідають інтересам користувача (доступність, достовірність, актуальність, релевантність, валідність). В сфері кіберзахисту найбільш часто використовуються конфіденційність (К), цілісність (Ц) та доступність (Д).

У свою чергу корпоративна мережа ІС, що реалізує комп'ютерні технології обробки даних, складається з:

1) електронних комп'ютерних пристроїв (персональних комп'ютерів, РС), що дозволяють зберігати, перетворювати і передавати/приймати дані від інших комп'ютерів (далі – кінцеві вузли мережі, або кінцеві точки, *endpoint*);

2) електронних комутаційних пристроїв, що дозволяють перемикати потоки даних між різними кінцевими вузлами мережі (далі – проміжні (комутаційні) вузли мережі:

комутатори (*switch*) , маршрутизатори (*router*) і шлюзи (gateways);

3) фізичних середовищ поширення електронних сигналів (ФСП), що з'єднують кінцеві і проміжні вузли між собою в єдину мережу (дротові, кабельні або оптоволоконні лінії, різноманітні радіолінії).

Представлена деталізація дозволяє у загальному вигляді описати фізичні процеси роботи комп'ютерної мережі, що є основою корпоративної ІС. Обмін даними між кінцевими вузлами мережі здійснюється шляхом передачі електромагнітних сигналів (електричних, або радіосигналів) за маршрутом (послідовність проміжних вузлів і ФСП між ними). Елементи сигналів відповідають двійковим одиницям (бітам). Дані об'єднуються в пакети. Кожен пакет в своєму заголовку містить унікальні адреси вузла призначення і вузла відправника. Маршрут доставки пакета формується на основі адреси призначення шляхом комутації послідовності ФСП відповідними проміжними вузлами.

Кожна мережа характеризується кількістю вузлів (кінцевих та проміжних) і може бути представлена конфігурацією фізичних зв'язків між ними, які формується на основі ФСП. Як правило, таку характеристику називають топологією мережі. Її можна представити у вигляді графа, в якому вершини відповідають вузлам мережі, а ребра – ФСП між вузлами.

Проведений аналіз складових ІС дозволяє визначити технологію обробки інформації (ТОІ) як послідовність перетворень вхідної інформації інформаційної системи (Doc_1) в вихідну інформацію (Doc_2). Перетворення здійснюють як користувачі, так і сервіси ІС. Перетворення інформації в комп'ютерної системі здійснюють сервіси. В рамках ТОІ між користувачами комп'ютерними сервісами формуються різні інформаційні відношення. Наприклад, на малюнку 3.4.

показано одне інформаційне відношення, яке математично може бути представлено у вигляді наступного кортежу:

$$IB_1 = (I_1, serv_1, I_2). \quad (3.1)$$

В свою чергу, ТОІ також можливо представити кортежом інформаційних відношень:

$$TOI_1 = (IB_1, IB_2, \ldots IB_N). \quad (3.2).$$

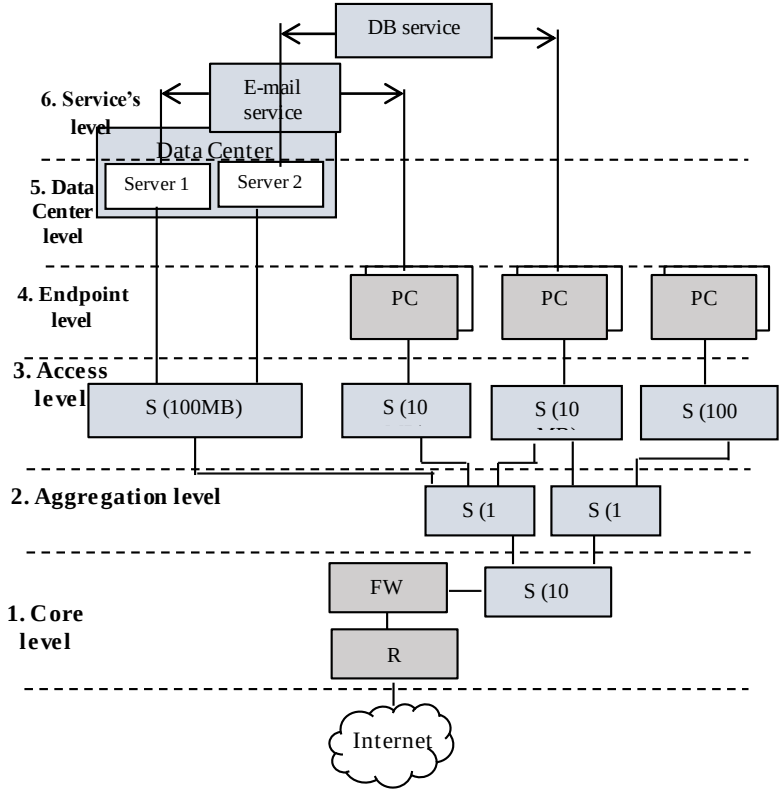
Примітка. Ніжні індекси – номери відповідних об'єктів (інформації, сервісів, інформаційних відношень та технологій обробки інформації). Інформаційна система на основі набору своїх сервісів дозволяє паралельно реалізовувати декілька ТОІ.

Комп'ютерна система корпоративної ІС, що представлена на мал. 3.4, дозволяє об'єднати тільки невелику кількість комп'ютерів користувачів (декілька десятків). Сучасні корпорації у різних сферах діяльності мають від кілька сотень до кілька тисяч співробітників. Для їх об'єднання в рамках інформаційної системи потрібно створювати комп'ютерну систему з більш складної структурою.

3.4. Багаторівнева структура комп'ютерної мережі корпоративної інформаційної системи

На малюнку 3.5. представлена структура системи, що дозволяє на основі комп'ютерних технологій в рамках корпорації організувати сумісну ефективну роботу сотень або тисяч співробітників. Така структура орієнтована на застосування комп'ютерних засобів за архітектурою "клієнт-

сервер" та представляє собою багаторівневу систему. Рівні системи відображають різні аспекти її функціонування. Основними компонентами структури є кінцеві вузли мережі: сервери (server) та комп'ютери персоналу (PC). Проміжними вузлами мережі є комутатори (switch, S), які дозволяють формувати різні маршрути обміну даними між комп'ютерами. Всі вузли з'єднані між собою фізичними середовищами обміну електромагнітними сигналами різного виду (кабель, провід, оптоволокно або лінія радіозв'язку). Більш детально розглянемо ці рівні структури.



Мал. 3.5. Типова багаторівнева структура комп'ютерної мережі сучасної корпоративної ІС

1. Рівень ядра (Core level), або магістральний рівень. За допомогою високошвидкісного комутатора S(10 Gbit/s) він забезпечує маршрутизацію агрегованих (об'єднаних) потоків даних (1 Gbit/s). Також на цьому рівні за допомогою маршрутизатору периметру R та файєрволу FW забезпечується корпоративний доступ до Інтернету.
2. Рівень агрегації (Aggregation level). За допомогою комутаторів рівня забезпечується маршрутизація та агрегація низко швидкісних потоків даних (10-100 Mbit/s) в потоки 1Gbit/s.
3. Рівень доступу (Access level). За допомогою портів низко швидкісних комутаторів (10-100 Mbit/s) забезпечується підключення комп'ютерів корпоративних користувачів до мережі. Використовується технологія підключення "duplex" (кожний комп'ютер підключений до окремого порту комутатора, одночасно по окремим парам забезпечується обмін даними на передачу та прийом).
4. Рівень кінцевих точок (Endpoint level). Відображаються всі комп'ютери користувачів та топологія їх підключення до комутаторів доступу.
5. Рівень центру обробки даних (Data Center level). Відображається вся сукупність корпоративних серверів ("ферма серверів"). Як правило, всі сервері розташовані у спеціальному приміщенні (серверне приміщення). Це приміщення має систему кондиціювання (охолодження) та захист від: 1) фізичного несанкціонованого доступу до обладнання; 2) витоку каналами побічних електромагнітних випромінювань; 3) зовнішнього спеціального електромагнітного впливу. Основним засобом захисту від факторів 2-3 є екранування всього приміщення спеціальним металевим покриттям. Для ефективного використання сукупного ресурсу серверів використовуються технології віртуалізації та кластеризації.

6. Рівень сервісів (Service's Level). Відображає від сервісу та відповідні сервер і комп'ютер користувача (клієнта).

Більшість корпоративних мереж відносяться до класу локальних мереж (LAN) та використовують на 1-2 рівнях моделі ISO/OSI різновиди мережевої технології Ethernet (Fast Ethernet (100 Mbit/s); Gigabit Ethernet (1 Gbit/s); 10G Ethernet (10 Gbit/s). На 3-7 рівнях моделі ISO/OSI застосовується стек протоколів *TCP/IP. Для керування роботою засобів мережі використовуються мережеві операційні системи* сімейства Windows Server (найбільш розповсюджені ОС Windows Server 2016, Windows Server 2019, Windows Server 2022). Така ОС розгортається на двох апаратних серверах мережі (основний та допоміжний), що забезпечує високу надійність роботи мережі за рахунок технології "гарячого резервування".

Для зручного адміністрування ресурсами мережі також розгортається Active Directory - служби каталогів Microsoft для операційних систем сімейства Windows Server. Active Directory дозволяє адміністраторам використовувати групові політики для забезпечення подібного налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів встановлювати оновлення ОС, прикладного та серверного ПЗ на всіх комп'ютерах в мережі. Засоби Active Directory дозволяють реалізовувати ефективну політику безпеки інформації щодо протидії загрозам несанкціонованого доступу до електронних ресурсів.

3.5. Фізичні основи процесів обробки інформації в ІКС

Обробка інформації (її зберігання, перетворення, передача і інші операції) в ІКС здійснюється за допомогою електронних, радіоелектронних і/або оптоелектронних технічних пристроїв. Такі пристрої складають загальну технологічну основу для інформаційних процесів, як в інформаційних системах, так і в електронних комунікаційних системах. Робота цих пристроїв заснована на використанні можливостей електромагнітної

взаємодії частинок, що мають електричний заряд. Інформація в сучасних ІКС представляється у вигляді різних комбінацій двох значень *(0* та *1)* елементарної одиниці інформації, яка називається *біт*, або – логічна одиниця. Для того, щоб комп'ютери "розуміли" логічні одиниці необхідний фізичний носії, що пов'язаний зі значеннями бітів. Носіями двійкових одиниць в ІКС є різні електромагнітні дискретні (цифрові) сигнали (електричні, оптичні, радіосигнали). Сигнали електронних пристроїв також беруть участь в процесах запису/зчитування інформації з елементів пам'яті. За їх допомогою відповідно до заданих обчислювальних алгоритмів також здійснюються різні перетворення одних двійкових комбінацій в інші (перетворення інформації).

Для більшого розуміння фізичних процесів в комп'ютерних системах визначимся з сутністю терміну "сигнал":

Сигнал – це структурований фізичний процес.

Фізичний процес (тобто, фізичний об'єкт, який змінюється за часом) буде структурованим, якщо за допомогою технічних/природних заходів будуть сформовані таки параметри цього процесу, значення яких не змінюються (або змінюються по відомому правилу) на протязі відрізку часу спостереження та є можливість їх передбачування.

Зв'язок послідовності бітів з сигналами можливо продемонструвати діаграмами на малюнку 3.6. Носіями двійкової послідовність $b(t)$ з шості бітів у цьому конкретному прикладі будуть два види електромагнітних сигналів $x(t)$ та $s(t)$. Ці сигнал поділяються за часом на елементи сигналів тривалістю Δt (це відрізок часу $\Delta t = t_2 - t_1$, де t_1, t_2 – моменти початку та кінця елементу сигналу). Початок елементу сигналу повторюється з періодом $T = \Delta t$. Кожний елемент сигналу має порядковий номер i (де $i = 1, 2, ..., I$; де I – кількість елементів

сигналу у послідовності). Цей номер пов'язаний з поточним часом послідовності наступною формулою:

$$i = [t/T], \tag{3.1}$$

де функція *[.]* - ціла частина дійсного числа.

Перший сигнал *x(t)* – це приклад двійкового електричного сигналу для передачі даних по дротової парі. Він генерується в залежності від бітової послідовності наступним чином:

$$x(t) = A\ (-1)^{b(t)}. \tag{3.2}$$

Параметр *A* - це амплітуда сигналу, яка на елементі сигналу може приймати тільки два значення (в цьому прикладі приймає значення або *+0,1mV,* або *-0,1 mV* в залежності від біта). Такий сигнал має назву "прямокутний", він швидко затухає (втрачає потужність) та використовується для передачі між складовими комп'ютера та між комп'ютерами по дротовим лініям зв'язку на відстанях до 1-2 км.

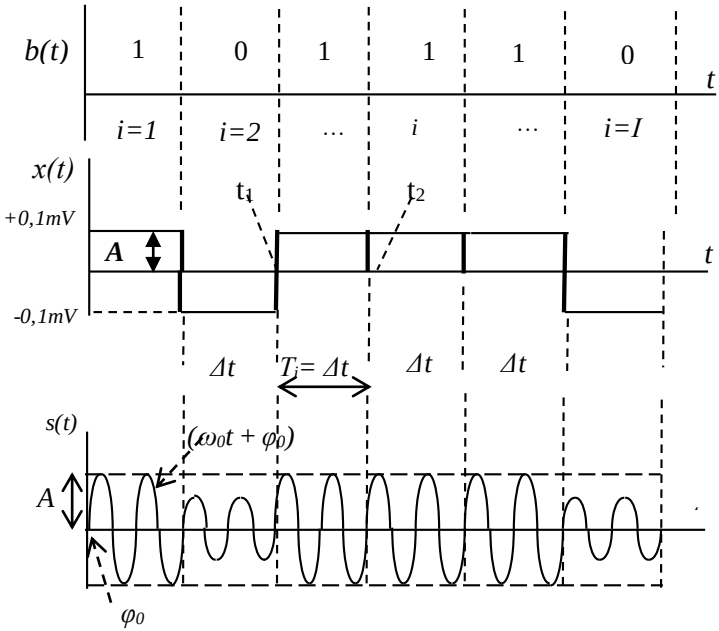
Другий сигнал *s(t)* має назву гармонічного сигналу. Він генерується за функцією *cos(x)* або *sin(x)* наступним чином (3.3):

$$s(t) = A_S\ cos(\omega_0 t + \varphi_0), \tag{3.3}$$

де:

- A_S – амплітуда гармонічного сигналу, яка залежить від значення біту послідовності *b(t)* (тобто, приймає на протязі елементу сигналу тільки два значення, у цьому прикладі: для $b(t)="1" – A_S("1") = 1;$ для $b(t)="0" – A_S = 0,5$);
- $(\omega_0 t + \varphi_0)$ – поточна фаза сигналу, приймає значення на елементі сигналу в діапазоні 0 – 360 градусів;
- $\omega_0 = 2\pi f$ - кругова частота сигналу, де $f=1/T$ – лінійна частота сигналу (вимірюється в *Гц*, 1 *Гц* – це одне коливання на протязі періоду *T*);
- φ_0 – начальна фаза гармонічного коливання (0 – 360 градусів).

Гармонічний сигнал *s(t)* використовується для обміну даними на великі відстані від десятків до тисяч кілометрів в кабельних та радіо лініях зв'язку. В наведеному прикладі сигнал приймає тільки два значення амплітуди (двозначна система зв'язку). В сучасних цифрових системах зв'язку сигнали можуть приймати багато значень кратних 2^n (наприклад, 4, 8, 16, 32 і далі). Це дозволяє будь-які данні представити послідовністю електромагнітних багатозначних сигналів (електричних, оптичних, радіо). Кожний елемент сигналу такої послідовності зіставлений з комбінацією *n* бітів.



Мал. 3.6. Співвідношення сигналів та бітових послідовностей

В таблиці 3.1 надається варіант такого зіставлення для сигналу *s(t)*, що може приймати вісім значень шляхом маніпуляції начальною фазою сигналу φ_0. Такий сигнал позначається як PSK8.

Табл.3.1.
Приклад співвідношення сигналів та бітів

Значення фази елементу радіосигналу	Значення набору бітів
0^0	000
45^0	001
90^0	010
135^0	011
180^0	100
225^0	101
270^0	110
315^0	111

Співвідношення фізичних елементів сигналів та бітів задається на першому (фізичному) рівні моделі ISO/OSI.

Під час аналізу проблем кіберзахисту часто використовують термін "сигнатура", який потрібно відрізняти від терміну "сигнал". Сигнатура - сукупність знаків, яка є характерною ознакою якогось інформаційного процесу. Наприклад, значення IP-адреса відправника трафіку, що здійснює DOS атаку, є сигнатурою цієї атаки. Вона може бути використана фаєрволом периметру для припинення зловмисних дій шляхом заборони прийняття відповідних IP-пакетів. Інший приклад, це хеш-образ шкідливого файлу, сформований за технологією MD5. Таки та інші сигнатури використовуються в якості індикаторів компрометації (*indicators of compromise, IOCs*) інформаційної системи. Більш детально про це буде розкрито в розділах 12, 13.

Висновки за розділом 3

- Фізичну основу національного сегменту кіберпростору складають інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи.

- Компонентами сучасних інформаційно-комунікаційних систем (ІКС) є інформаційні системи (ІС) та електронні комунікаційні системи (КС), які у процесі обробки інформації діють як єдине ціле.
- Інформаційна (автоматизована) система - це організаційно-технічну система, що об'єднує:
- обчислювальну (комп'ютерну) систему (апаратурне та програмне забезпечення);
- фізичне середовище (зовнішнє середовище та контрольована зону);
- персонал (керівництво, адміністратори і користувачі);
- оброблювану інформацію;
- порядок обробки інформації (тобто, технологію обробки інформації, ТОІ).
- Обробка інформації (її зберігання, перетворення, передача і інші операції) в ІКС здійснюється за допомогою електронних, радіоелектронних і/або оптоелектронних технічних пристроїв. Такі пристрої складають загальну технологічну основу для інформаційних процесів, як в інформаційних системах, так і в електронних комунікаційних системах.
- Інформація в сучасних ІКС представляється у вигляді різних комбінацій двох значень *(0* та *1)* елементарної одиниці інформації, яка називається *біт*, або – логічна одиниця. Для того, щоб комп'ютери "розуміли" логічні одиниці необхідний фізичний носії, що пов'язаний зі значеннями бітів. Носіями двійкових одиниць в ІКС є різні електромагнітні дискретні (цифрові) сигнали (електричні, оптичні, радіосигнали).
- *Сигнал* – це структурований фізичний процес. Фізичний процес (тобто, фізичний об'єкт, який змінюється за часом) буде структурованим, якщо за допомогою технічних/природних заходів будуть сформовані таки параметри цього процесу, значення яких не змінюються (або змінюються по відомому правилу) на протязі відрізку часу спостереження та є можливість їх передбачування.

Контрольні питання та завдання

1. Чим відрізняється інформаційна система від комп'ютерної?
2. Які фізичні об'єкти складають основу кіберпростору?
3. Види сервісів, що надає корпоративна ІКС на основі Інтернету?
4. Рівні комп'ютерної мережі сучасної інформаційної системи?
5. Які носії логічних двійкових одиниць (бітів) використовуються під час обміну інформацією між комп'ютерами мережі?
6. Компоненти технології обробки інформації в інформаційної системі?

4. БЕЗПЕКА ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА КІБЕРБЕЗПЕКА

- **взаємозв'язок кіберзахисту з видами систем захисту інформації в ІКС**
- **безпека та захист інформації**
- **властивості інформації, що визначають її безпеку**
- **основні терміни у сфері захисту інформації в інформаційно-комунікаційних системах**
- **вимоги до обробки та забезпечення захисту інформації в ІКС**
- **напрями захисту інформації**

В цьому розділи будуть розглянути нормативно-правові аспекти, які пов'язують кіберзахисту із захистом інформації в ІКС. Також будуть розглянути види систем захисту інформації, сутність безпеки та захисту інформації в ІКС, основи створення комплексних систем захисту інформації з підтвердженою відповідністю.

4.1. Взаємозв'язок кіберзахисту з видами систем захисту інформації в ІКС.

Поняття "кібербезпека" тісно пов'язане із забезпеченням "безпеки інформації". Перше поняття почало широко застосовуватися з середині першого десятиліття двадцять першого століття. Друге поняття почало застосовуватися набагато раніше з часів масштабного розповсюдження телекомунікаційних систем (40-60 роки минулого віку). З початку 90х років минулого століття почала впроваджуватися державна політика у сфері захисту інформації в інформаційно-комунікаційних систем. Юридичну основу цієї політики складає система нормативно-правових актів, яка представляє собою наступну ієрархію:

- конституція та закони України;
- накази Президента України;
- постанови Кабінету міністрів України;

- нормативні документи уповноваженого органу у сфері захисту інформації в ІКС (на цей час обов'язки такого органу виконую Держспецзв'язок);
- відомчі нормативні документи;
- регулюючі документи служби захисту інформації конкретної ІКС.

Особливість цієї ієрархії нормативно-правових актів – вимоги до захисту інформації документів верхнього рівня обов'язкові для урахування в документах нижнього рівня. Основним законом в цієї ієрархії є Закон України "Про захист інформації в інформаційно-комунікаційних системах" (в першої редакції 1994 року - "Про захист інформації в автоматизованих системах"). Діюча редакція цього закону (далі – Закон про захист ІКС) визначає можливість створення двох видив систем захисту в ІКС, що повинні забезпечувати нормативний стан безпеки інформації:

1) комплексна система захисту інформації (КСЗІ);
2) система управління інформаційною безпекою (СУІБ).

В основі організації роботи КСЗІ застосовується стратегія відповідності обраних заходів та засобів захисту комплексу конкретних критеріїв захисту, що нормується відповідним комплексом державних документів [7, 8]. Функціонування СУІБ базується на застосуванні більш ліберальної стратегії захисту на основі циклічного виконання заходів управління ризиками безпеки інформації. Стратегія для СУІБ нормується міжнародними стандартами серії ISO/IEC 27000.

Закон про захист ІКС визначає наступні обов'язкові умови обробки інформації в системі:

1) державні інформаційні ресурси (ДІР) або інформація з обмеженим доступом (ІзОД), вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням ***комплексної системи захисту інформації з підтвердженою відповідністю****;*

2) ДІР та ІзОД, вимога щодо захисту якої встановлена законом, крім державної таємниці, службової інформації та інформації з державних і єдиних реєстрів, створення та забезпечення функціонування яких визначені законом, можуть оброблятися в системі без застосування КСЗІ.

Дозвіл на експлуатацію КСЗІ та СУІБ, що обробляють ДІР або ІзОД, вимога щодо захисту якої встановлена законом, надається за результатами оцінювання відповідності державним вимогам. Для КСЗІ таке оцінювання здійснюється в рамках державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством. КСЗІ з підтвердженою відповідністю надається ***атестат відповідності***. Дозвіл на ввід в експлуатацію СУІБ надається за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо є відповідна угода.

Державна політика щодо кіберзахисту національних електронних інформаційних ресурсів почала розробляться та впроваджуватися з 2016 року. Основним регулюючим документом цієї політики є Закон України "Про основні засади забезпечення кібербезпеки України" (2017 рік). Цей закон розглядає тільки загальні організаційні особливості забезпечення кіберзахисту на національному рівні, але не пояснює технічні аспекти забезпечення кібербезпеки. Більш детально розкриваються технічні аспекти кіберзахисту в рамках "Загальних вимог до кіберзахисту об'єктів критичної інфраструктури", що введені в дію постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. Цей документ

вказує на необхідність впровадження заходів та засобів захисту в рамках двох видів систем:

1) комплексна система захисту інформації :об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

2) система інформаційної безпеки (СІБ) об'єкта критичної інфраструктури.

Перший варіант реалізується у випадку коли на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Другий варіант - не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Цей документ під СІБ розуміє 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. Методичною основою для оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005.

Таким чином можливо стверджувати, що **кіберзахист є частиною комплексу заходів та засобів захисту інформації в ІКС.** На думку автора, особливість кіберзахисту в тому, що він орієнтований на стратегію захисту, яка спрямована на протидію динамічному набору загроз (кількість загроз постійно зростає). Класичний захист в ІКС орієнтовний на статичний набір загроз, який періодично переглядається (наприклад, раз на рік або на 2 рокі).

Для організації ефективної практичної діяльності фахівців сфері забезпечення кібербезпеки необхідно знати:
1) основи захисту ІКС за допомогою КСЗІ з підтвердженою відповідністю (класичний підхід);
2) особливості організації кіберзахисту в рамках КСЗІ.

Далі в розділі будуть уточнені поняття *безпеки* та *захисту інформації* в ІКС. Після цього будуть розглянути основи створення КСЗІ з підтвердженою відповідністю. Таки системи захисту необхідно створювати в більшості державних установ. Вони є невід'ємною частиною національної структури кіберзахисту.

4.2. Безпека та захист інформації

При аналізі інформаційних процесів в ІКС для фахівців кіберзахисту важливо уточнити сутність терміну "безпека інформації". В рамках замовленого інформаційного сервісу користувач пред'являє вимоги до інформаційного продукту (тобто до інформації, яка формується сервісом). Наприклад, при передачі інформації відправник часто зацікавлений в її доставці без порушення конфіденційності та/або цілісності. В іншому випадку, при зверненні до необхідного інформаційного ресурсу користувач зацікавлений в надійній реалізації його права доступу до інформації, тобто забезпечення доступності. Ці та безліч інших можливих прикладів свідчать про існування зацікавленості користувачів ІТС в наданні їм послуг з такою якістю, яка може бути виражена у вигляді набору властивостей інформаційного продукту. Вплив на ІКС різних негативних факторів (природних, техногенних, людських та інших) може призводити до порушення цих властивостей, тобто знижувати якості інформаційного продукту. З позицій організації ефективної протидії серед усіх негативних впливів найбільшу

зацікавленість представляють навмисні дії людини, які при сучасному рівні розвитку технологій можуть носити досить складний та мало прогнозований характер. Вони постійно удосконалюються. Для їх успішної реалізації з боку зловмисник необхідні сильна мотивація, високий рівень знань механізмів роботи ІКС та досвід практичної діяльності в сфері цифрових технологій. З огляду на більш значну передбачуваність (в першу чергу, статистичну) несприятливих техногенних факторів їх доцільно пов'язувати з терміном "надійність ІКС" та планувати заходи забезпечення надійності ще на етапі розробки технології обробки інформації. Так, наприклад, природний вихід з ладу магнітного накопичувача призводить порушення доступності інформації. Однак, знання середнього часу напрацювання на відмову для цього пристрою, дозволяє ще на етапі розробки ІКС запланувати дієві заходи щодо резервування інформації. Виходячи з цих позицій, пропонується уточнити термін "безпека інформації ІКС":

безпека інформації ІКС - такий стан ІКС, який забезпечує задані властивості інформаційного продукту в умовах навмисних несприятливих впливів на ІКС.

У свою чергу, через це поняття можна визначити і наступні пов'язані терміни:

захист інформації в ІКС - це дії, які спрямовані на досягнення та підтримання безпеки інформації ІКС;

вразливості ІКС - такі її властивості, використання яких зловмисником може призвести до порушення безпеки інформації;

загрози ІКС – сукупності вразливостей та можливих (потенційних) заходів зловмисника по їх використанню щодо порушення безпеки інформації.

4.3. Властивості інформації, що визначають її безпеку

Після визначення терміну "безпека інформації ІКС" необхідно уточнити перелік властивостей інформації, через які визначається її безпека. Історично першими широкого поширення набули електронні комунікаційні системи (телекомунікаційні системи), в яких основною послугою є передача інформації (обмін інформацією). Ця послуга і визначила основні властивості, забезпечення яких на той час складала сутність безпеки інформації. Такими властивостями були конфіденційність, цілісність, доступність (далі - К, Ц, Д). Вони визначаються наступним чином [7]:

Конфіденційність інформації (information confidentiality) - властивість інформації, яка полягає в тому, що інформація не може бути отримана особою несанкціонованим образом.

Цілісність інформації (information integrity) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована несанкціонованим шляхом.

Доступність інформації (availability) – властивість інформації, яка полягає в тому, що користувач, який володіє відповідними повноваженнями відносно доступу до неї, може їх реалізувати відповідно до правил, встановлених політикою безпеки інформації.

З появою, розвитком і поширенням інформаційних систем ситуація з вимогами до інформації змінилася. Застосування комп'ютерів і інших цифрових електронних пристроїв значно розширило спектр інформаційних послуг, що надаються. Це, в свою чергу, призвело до розширення набору необхідних властивостей інформаційного продукту. Поняття "безпека інформації" стали також пов'язувати із забезпеченням актуальності, достовірності, релевантності, валідності і деяких інших властивостей інформації. Тут слід зазначити нову

особливість додаткових властивостей, яка більш чітко проявляється в рамках атрибутивно-трансфертного підходу до сутності інформації [12]. Цей підхід виділяє набуту властивість носія інформації в результаті інформаційного впливу від іншого об'єкту. Ця набута властивість відображає якусь властивість об'єкту, що впливає, та називається "семантикою інформації". Наприклад, фотопортрет особи, що відображає особливості її обличчя, є семантикою інформації про особу. З цих позиції забезпечення К, Ц, Д не пов'язано з семантикою вихідної інформації і залежить тільки від коректної реалізації сервісів передачі інформації, її зберігання, поширення і деяких інших. У той же час, забезпечення актуальності і достовірності залежить від семантики (змісту) вихідної інформації. Якщо ця семантика інформаційного продукту не відповідає актуальності і достовірності дійсних подій, які відображаються, то навіть коректні сервіси ІКС не забезпечать ці властивості інформаційного продукту.

Додатково слід підкреслити те, що з урахуванням широкого застосування в ІКС сервісів перетворення інформації на основі заданих обчислювальних алгоритмів, актуальною стає необхідність врахування і властивості коректності реалізації заданого алгоритму перетворень (далі - коректність перетворень даних). Багато відомих кіберзагроз пов'язано з порушенням алгоритму перетворень або з його повною заміною.

Як правило, необхідні властивості визначаються на етапі формування політики безпеки інформації для ІКС.

4.4. Основні терміни у сфері захисту інформації в інформаційно-комунікаційних системах

Національні нормативно-правові акти у сфері захисту ІКС вживають наведені нижче терміни в такому значенні:

автентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора;

ідентифікація - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою;

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

витік інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації - фізична або юридична особа, якій належать права на інформацію;

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-комунікаційна система - сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) - фізична або юридична особа, яка в установленому

законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

електронна комунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

резервна копія державних інформаційних ресурсів - копія інформації, яка міститься в державних інформаційних ресурсах, що перебувають у володінні або розпорядженні органів

державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, та є критичною для їх сталого функціонування, створюється, записується, обробляється або зберігається у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів з метою подальшого відновлення цієї інформації;

резервування державних інформаційних ресурсів та систем - сукупність заходів, спрямованих на забезпечення створення резервної копії (резервних копій) та зберігання державних інформаційних ресурсів та систем з метою забезпечення безперервності їх роботи та подальшого відновлення інформації, що міститься в державних інформаційних ресурсах та системах.

4.5. Вимоги до обробки та забезпечення захисту інформації в ІКС

Відповідно до вимог закону України «Про захист інформації в інформаційно-комунікаційних системах» умови обробки інформації в системі визначаються власником системи згідно договору з власником інформації, якщо інше не передбачено законодавством.

В той же час цей закон також визначає наступну обов'язкову умову:

державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням **комплексної системи захисту інформації з підтвердженою відповідністю.**

Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами **державної експертизи**, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому

законодавством. КСЗІ, що пройшла державну експертизу, отримує ***атестат відповідності.*** У подальшому будемо розглядати тільки такі КСЗІ.

Вимоги до забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України. Обов'язки уповноваженого органу у сфері захисту інформації в системах виконує центральний орган виконавчої влади у сфері криптографічного та технічного захисту інформації. Таким органом на момент написання цього посібника є Державна служба спеціального зв'язку та захисту інформації (далі – Держспецзв'язок).

Уповноважений орган у сфері захисту інформації в системах:

- розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;
- визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;
- здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Державні органи в межах своїх повноважень за погодженням з уповноваженим органом у сфері захисту інформації встановлюють особливості захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом. Особливості

захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює ***службу захисту інформації*** (далі – СЗІ) або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє уповноважений орган у сфері захисту інформації.

Для створення комплексної системи захисту інформації з підтвердженою відповідностю використовуються тільки засоби захисту інформації, які мають ***сертифікат відповідності*** або ***позитивний експертний висновок*** за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації.

4.6. Напрями захисту інформації

Істотна частина проблем забезпечення захисту інформації в ІКС може бути вирішена організаційними заходами. Проте, з розвитком інформаційних технологій спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту.

Відповідно до нормативних актів Кабінету Міністрів України [9] та нормативних документів технічного захисту інформації [6, 7] до складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:
- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень (ПЕМВН), акустоелектричні та інші канали. Основу технічного

каналу витоку (ТКВ) складає небезпечний сигнал (тобто, сигнал, що не передбачений комп'ютерною технологією та виникає за допомогою різних шкідливих факторів);

- несанкціонованих дій та несанкціонованого доступу (канал НСД) до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та інше. Основу каналу НСД складає технологічний сигнал (тобто, сигнал, що визначений ще на етапі розробки комп'ютерної технології);

- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів великої потужності з метою порушення цілісності інформації або руйнування системи захисту.

Також ряд нормативних документів технічного захисту інформації [13, 14] визначають:

- заходи організаційного забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) в ІКС та здійснення контролю за її функціонуванням. В рамках цих заходів створюється і функціонує служба захисту інформації (СЗІ). На СЗІ покладається виконання робіт з визначення вимог з захисту інформації, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в ІТС;

- заходи та засоби, що забезпечують захист від несанкціонованого доступу до фізичного середовища функціонування ІКС (будівлі, окремі приміщення тощо) та фізичних носіїв інформації технічних пристроїв ІКС (магнітні та оптичні диски, флеш запам'ятовуючі пристрої, карти пам'яті тощо).

За допомогою зазначеного матеріалу можливо визначити наступні напрями захисту, що забезпечує КСЗІ:

1) захист від несанкціонованих дій та доступу (захист від НСД);
2) захист від витоку технічними каналами (захист від витоку ТК);
3) захист від спеціального впливу на інформацію (захист від СВ);
4) організаційне забезпечення захисту інформації (організаційний захист, ОЗ);
5) захист від несанкціонованого фізичного доступу (захист від НСФД).

Напрямки 1-3 безпосередньо пов'язані з обробкою інформації електронними засобами ІКС. Нормативні акти, що регулюють заходи захисту від СВ знаходяться в стадії розробки. Напрямки 4-5 більше пов'язані з організацією роботи персоналу щодо безпечного функціонування ІКС.

Захист інформації від витоку технічними каналами забезпечується в ІКС у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації.

Захист інформації від НСД забезпечується в усіх ІКС.

Захист інформації від спеціального впливу на засоби обробки забезпечується в системі, якщо рішення про необхідність такого захисту прийнято розпорядником інформації.

Залежність обов’язкових напрямів захисту КСЗІ від виду інформації, що оброблюється в ІКС [9], відображається в таблиці 4.1.

Залежність обов'язкових напрямів захисту КСЗІ від виду інформації, що оброблюється в ІКС Таблиця 4.1.

Від інформації		Напрями захисту в КСЗІ		
		Захист від ТКВ	Захист від НСД	Захист від СВ
1. Відкрита		*	+	*
2. Конфіденційна		*	+	*
3. Службова		*	+	*
4. Таємна	*державна таємниця*	+	+	*
	інша *таємниця*	*	+	*

+ - обов'язковий характер; * - визначається розпорядником інф.

З точки зору інтегрування засобів та заходів кіберзахисту в структуру КСЗІ важливо розуміти до якої частини її структури вони будуть належати. Так як кібератаки на інформацію в кіберпросторі здійснюються на основі використання комп'ютерних технологій, що реалізуються технологічними електромагнітними сигналами, то кіберзахист необхідно віднести до захисту від НСД. Особливість кіберзахисту – він направлений на динамічна змінюваний набір загроз. Це забезпечується сукупністю засобів кіберзахисту (інфраструктурою кіберзахисту), що реалізують циклічний процес з наступних етапів:

1) ідентифікація загроз;
2) інсталяція комплексу відповідних засобів захисту;
3) визначення (детектування) кібератак та кіберінцидентів;
4) прийняття рішення про відповідь на атаку (інцидент);
5) реалізація рішення шляхом внесення змін в роботу комплексу засобів захисту.

Більш детально етапи циклу буде розглянуто в розділі 7.

Висновки за розділом 4

- Закон України "Про захист інформації в інформаційно-комунікаційних системах визначає можливість створення двох видив систем захисту в ІКС, що повинні забезпечувати нормативний стан безпеки інформації:
  1) комплексна система захисту інформації (КСЗІ);

2) система управління інформаційною безпекою (СУІБ).

- В основі організації роботи КСЗІ застосовується стратегія відповідності обраних заходів та засобів захисту комплексу конкретних критеріїв захисту, що нормується відповідним комплексом державних документів.
- Стратегія для СУІБ нормується міжнародними стандартами серії ISO 27000.
- державні інформаційні ресурси (ДІР) або інформація з обмеженим доступом (ІзОД), вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням **КСЗІ з підтвердженою відповідністю.**
- ДІР та ІзОД, вимога щодо захисту якої встановлена законом, крім державної таємниці, службової інформації та інформації з державних і єдиних реєстрів, створення та забезпечення функціонування яких визначені законом, можуть оброблятися в системі без застосування КСЗІ.
- Дозвіл на експлуатацію КСЗІ та СУІБ, що оброблюють державні інформаційні ресурси або інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом, надається за результатами оцінки відповідності державним вимогам.
- Для КСЗІ таке оцінювання здійснюється в рамках державної експертизи. КСЗІ з підтвердженою відповідністю надається атестат відповідності.
- Дозвіл на експлуатацію СУІБ надається за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою.
- Процедура оцінювання СУІБ проводиться органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо є відповідна угода.
- Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 ввела в дію "Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури". Цей документ вказує на

необхідність впровадження заходів та засобів кіберзахисту в рамках двох видів систем:

1) комплексна система захисту інформації об'єкта критичної інформаційної інфраструктури (ОКІІ) об'єкта критичної інфраструктури (ОКІ);
2) система інформаційної безпеки (СІБ) об'єкта критичної інфраструктури.

- Перший варіант - коли обробляються державні інформаційні ресурси або інформація з обмеженим доступом (ІзОД), вимога щодо захисту якої встановлена законом.
- Другий варіант - не обробляються державні інформаційні ресурси або ІзОД, вимога щодо захисту якої встановлена законом.
- СІБ - сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на ОКІІ з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів.

- **Безпека інформації ІКС** - такий стан ІКС, який забезпечує задані властивості інформаційного продукту в умовах навмисних несприятливих впливів на ІКС.
- **Захист інформації в ІКС** - це дії, які спрямовані на досягнення та підтримання безпеки інформації ІКС.
- **Вразливості ІКС** - такі її властивості, використання яких зловмисником може призвести до порушення безпеки інформації.
- **Загрози ІКС** – сукупності вразливостей та можливих (потенційних) заходів зловмисника по їх використанню щодо порушення безпеки інформації.
- **Конфіденційність інформації** (information confidentiality) - властивість інформації, яка полягає в тому, що інформація не може бути отримана особою несанкціонованим образом.
- **Цілісність інформації** (information integrity) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована несанкціонованим шляхом.

- **Доступність інформації** (availability) – властивість інформації, яка полягає в тому, що користувач, який володіє відповідними повноваженнями відносно доступу до неї, може їх реалізувати відповідно до правил, встановлених політикою безпеки інформації.
- **Комплексна система захисту інформації** - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.
- Напрями захисту, що може забезпечувати КСЗІ:
  1) захист від несанкціонованих дій та доступу (захист від НСД);
  2) захист від витоку технічними каналами (захист від витоку ТК);
  3) захист від спеціального впливу на інформацію (захист від СВ);
  4) організаційне забезпечення захисту інформації (організаційний захист, ОЗ);
  5) захист від несанкціонованого фізичного доступу (захист від НСФД).
- Захист інформації від витоку ТК обов'язково забезпечується коли обробляється інформація, що становить державну таємницю.
- Захист інформації від НСД забезпечується в усіх ІКС.

Контрольні питання та завдання

1. Види систем захисту в ІКС?
2. Коли створюється КСЗІ з підтвердженою відповідністю?
3. Як перевіряється відповідність КСЗІ нормативним вимогам?
4. Який документ отримує КСЗІ з підтвердженою відповідністю?
5. Яким чином можна отримати дозвіл на експлуатацію для СУІБ?
6. В якому випадку обробка ДІР або ІзОД, якої встановлена законом, може оброблятися в ІКС без застосування КСЗІ?
7. В рамках яких видів систем можуть впроваджуватися заходи кіберзахисту ОКІІ?
8. Система інформаційної безпеки ОКІІ?
9. Коли для кіберзахисту ОКІІ може створюватися *Система інформаційної безпеки (СІБ)?*

5. КОНЦЕПТУАЛЬНА МОДЕЛЬ КІБЕРПРОСТОРУ ТА КІБЕРБЕЗПЕКИ

- **базовий набір понять для визначення сутності кіберпростору**
- **графічна модель кіберпростору**
- **кібербезпека та її математична модель**

Після проведеного аналізу складу сучасних корпоративних ІКС (розділ 3) та принципів їх захисту за допомогою КСЗІ (розділ 4) перейдемо до більш детального ознайомлення зі структурою кіберпростору та сутністю його безпечного використання. Для цього розглянемо концептуальну модель (парадигму) кіберпростору та кібербезпеки, яка сформована за допомогою засобів формалізації (розділ 2). Ця модель складається з наступних частин:

1) базовий набор узгоджених понять (тезаурус):
2) графічна модель кіберпростору;
3) кібербезпека та її математична модель.

Така модель уточнює деякі аспекти співвідношення термінів "ІКС – кіберпростір - кібербезпека". Модель направлена на практичне її застосування в сфері організації ефективної системи кіберзахисту та автоматизації її процесів.

5.1. Базовий набір понять для визначення сутності кіберпростору

Проведений в попередніх розділах аналіз складу ІКС, її структури та особливостей застосування комп'ютерних технологій дозволив уточнити такі поняття: "інформація в ІКС"; "технологія електронної (цифрової) обробки інформації"; "інформаційний сервіс ІКС"; "інформаційний продукт" і його якість; "користувачі ІКС", " інформаційні відносини" між користувачами ІКС; властивості і безпека інформації ІКС; взаємозв'язок понять у ланцюжку "людина - фізичний простір - ІКС – кіберпростір". Результати цього аналізу дозволяють

сформулювати наступний набір взаємоузгоджених визначень, що направлений на організацію ефективної діяльності в сфері кіберзахисту.

Кіберпростір - це сукупність інформаційних відносин між користувачами ІКС, які формуються за допомогою комп'ютерних послуг (сервісів) цих систем.

Пояснюючі визначення:

Інформація про об'єкт А в об'єкті В, І(А:В) - це властивість (атрибут) об'єкту В, що придбана (перенесена) в результаті фізичної взаємодії з об'єктом А та є відображенням властивості цього об'єкту А.

Носій інформації - об'єкт, в якому відображені властивості іншого об'єкту.

Користувач ІКС - це людина або технічний об'єкт (система), які використовують інформаційний продукт ІКС в своїх інтересах (цілях).

Інформаційний продукт ІКС - це інформація із заданими користувачем властивостями, яка формується інформаційним сервісом (послугою).

Інформаційний сервіс (послуга) - це сукупність дій з вихідною інформацією, що формує інформаційний продукт із заданими властивостями.

Властивості інформації - це ті якості інформації, які потрібні користувачу інформації.

Інформаційне відношення - це сукупність вхідної інформації, обраного інформаційного сервісу та сформованого інформаційного продукту.

Особливість цього набору в тому, що термін "кіберпростір" пояснюється тільки за допомогою ієрархії понять, на першому рівні якої застосовуються тільки термін "інформація" (в розумінні атрибутивно-трансфертного підходу до її сутності) та формалізований опис знань про інформаційно-комунікаційні, інформаційні та комп'ютерні системи.

5.2. Графічна модель кіберпростору

Вербальний опис сутності кіберпростору, зроблений за допомого ієрархічного набору пояснюючих термінів, дозволяє

провести візуалізацію у вигляді графічної моделі кіберпростору (малюнок 5.1.).

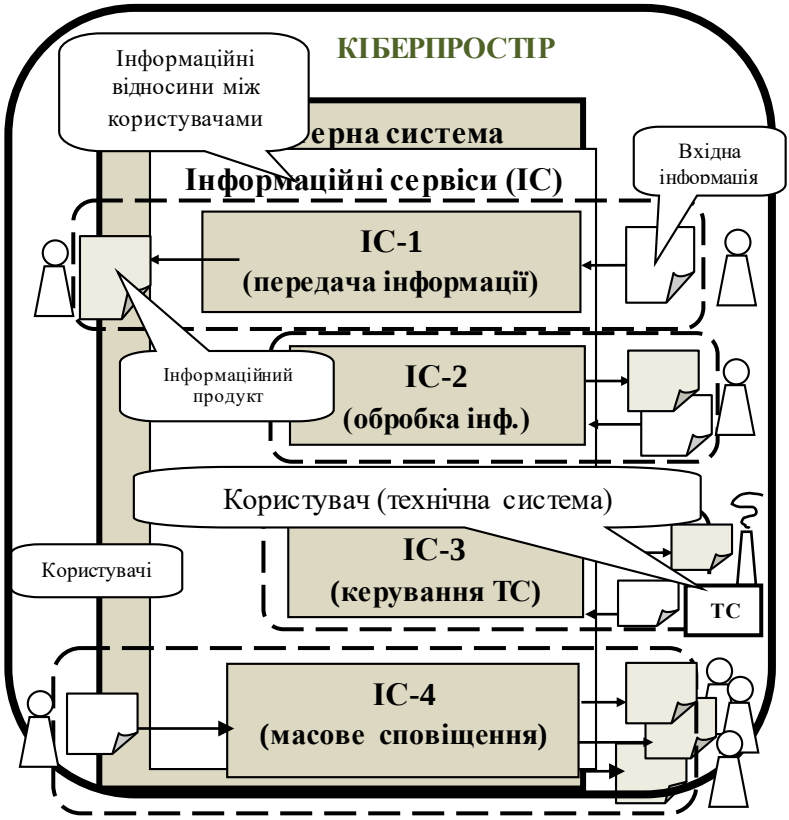
Модель відображає структуру кіберпростору, яка складається з наступних значущих компонентів інформаційно-комунікаційної системи:

- комп'ютерна система;
- інформаційні сервіси, що можуть бути створені на основі ресурсів комп'ютерної системи;
- користувачі інформаційно-комунікаційної системи (людина або технічна система);
- інформаційні відносини, що формуються на основі конкретного сервісу, вхідної інформації від користувача та інформаційного продукту, що формується за результатами роботи сервісу;

Таке формалізоване представлення кіберпростору дозволяє розглядати його кібербезпеку через забезпечення інтересів користувачів, які можливо сформулювати за допомогою властивостей інформації. На відміну від класичного підходу до безпеки інформації (забезпечення конфіденційності, цілісності та доступності) ця модель вводить поняття інформаційного відношення між користувачами кіберпростору на основі комп'ютерного сервісу. Це дозволяє диференціювати інформацію кіберпростору на вхідну інформацію сервісу та інформаційний продукт (вихідну інформацію сервісу). Такий розподіл дозволяє описувати інтереси користувачів в кіберпросторі шляхом визначення не тільки вимог до якостей інформаційного продукту (класичний підхід), але і завданням вимог до якості вхідної інформації (на приклад, до достовірності, або шкідливого впливу семантики вхідної інформації).

Запропонований підхід щодо завдання вимог до вхідної інформації є перспективним с точки зору формалізованого аналізу кіберзагроз, що пов'язані з вразливостями психологічного стану людини. Розробка програмних засобів, що в автоматичному режимі будуть аналізувати семантику вхідної інформації на предмет ознак небезпеки для користувача (наприклад, за допомогою сигнатурної фільтрації знакового змісту повідомлення) представляється перспективним напрямом розвитку заходів кіберзахисту.

Представлений концепт інформаційного відношення є інтересним і з іншого боку. Якщо обчислювальний алгоритм, що визначає сутність комп'ютерного сервісу, розглядати як інформацію, в якої відображені семантичні конструкції розуму програміста, то з'являється додатковий інструмент для класифікації та формалізованого аналізу кіберзагроз, шо пов'язані з використанням в кіберпросторі сильного штучного інтелекту.



Мал. 5.1. Графічна модель сегменту кіберпростору на основі корпоративної інформаційної системи

5.3. Кібербезпека та її математична модель

Вищезазначені поняття та модель кіберпростору дозволяють сформулювати наступне формалізоване визначення сутності кібербезпеки:

кібербезпека – це стан інформаційно-комунікаційної системи, при якому навмисні несанкціоновані дії у кіберпросторі не порушують для користувачів послуг задані властивості інформації.

В рамках отриманого поняття доцільно пояснити наступне:

1) інтереси користувачів послуг кіберпростору можливо виразити в заданих властивостях до інформації в рамках інформаційних відношень користувача;

2) вимоги до необхідного рівня захисту від більшості кіберзагроз, які не пов'язані з психологічним впливом на користувача, задаються наступними властивостями інформаційного продукту: конфіденційність; цілісність; доступність;

3) у випадках організації протидії кіберзагрозам, що не пов'язані з порушенням конфіденційності, цілісності та доступності оброблювальної інформації, необхідно задавати вимоги до вхідної інформації та/або до джерела цієї інформації;

4) на основі представленої моделі кіберпростору можливо виділити наступні об'єкти кіберзахисту:

- інформаційно-комунікаційні системи (ІКС);
- інформаційні ресурси ІКС (інформаційні продукти, проміжна і технологічна інформація);
- інформаційні сервіси ІКС, комп'ютерне апаратне та програмне забезпечення;
- користувачі ІКС.

Наданий вище набір термінів, визначення яких ієрархічно узгоджені між собою за допомогою атрибутивно-трансфертного підходу до інформації, комплексу формалізованих знань про інформаційно-комунікаційні, інформаційні та комп'ютерні системи, дозволяє представити наступний спосіб математичного опису стану кібербезпеки та процесів кіберзахисту, необхідних для його досягнення. Такий інструмент математичної формалізації може бути застосований для подолання ряду існуючих невизначеностей в сфері роз'яснення актуальних проблем організації ефективного кіберзахисту. Наприклад, він може бути застосований для детального

математичного опису складної кібератаки (APT-атаки, що відноситься до атаки 0-day) та розробити відповідний спосіб кіберзахисту. Другий приклад – це представлення заходів корпоративної системи кіберзахисту у вигляді циклічного процесу. Ці та інші приклади практичного застосування цього способу математичного опису будуть детально представлені в наступних розділах посібника.

Для початку розглянемо сегмент кіберпростору, який сформований інформаційно-комунікаційною системою IKS. Така система в процесі використання може бути представлена у вигляді кінцевої множини

$$IKS = \{IA_i\},\ i=1,\dots,I \qquad (5.1)$$

де:

- елемент множини IA_i – це i-те інформаційне відношення (Information Attitude , IA);
- I - кількість інформаційних відношень (потужність множини) на етапі спостереження тривалістю T.

В свою чергу кожне інформаційне відношення може бути представлене через впорядковану трійку елементів наступним чином

$$IA_i = (In_i^*, f_i, In_i), \qquad (5.2)$$

де елементи:

- In_i – вхідна інформація i-того сервісу;
- f_i - i-тий сервіс;
- In_i^*- інформаційний продукт, який формується i-тим сервісом.

Взаємозв'язок між елементами i-того інформаційного відношення може бути відображений у вигляді наступного представлення

$$In_i^* = f_i(In_i). \qquad (5.3)$$

Таким чином, сегмент кіберпростору на основі конкретної ІКС може бути представлений у вигляді виразів 1-3. Для формального представлення стану кібербезпеки цього сегменту необхідно представити властивості інформаційного продукту In_i^* в кожному інформаційному відношенні IA_i. З цією метою виділимо алфавіт властивостей A, які користувач ІКС може вимагати до інформаційного продукту In_i^* в рамках інформаційного відношення IA_i:

$$A = \{a_n\},\ n=1,\ldots,N, \qquad (5.4)$$

де: a_n – одна із заданих властивостей; N – кількість властивостей (потужність множини). Тоді для кожного поточного інформаційного відношення можна виділити наступний набір властивостей:

$$A_i = \{a_{n,j}^{(i)}\} \subset A,\ j=1,\ldots,J, \qquad (5.5)$$

де $a_{n,j}^{(i)}$– n-та властивість із алфавіту A, що задана користувачем в рамках інформаційного відношення IA_i, j – поточний номер властивості в наборі A_i, потужність якого J.

Нехай властивість $a_n^{(i)}$ може приймати одне з декількох можливих значень $v_k^{(n)}$, що належать множині $V_n=\{v_k^{(n)}\}$, тобто користувач може задати вимогу до інформаційного продукту в рамках IA_i інформаційного відношення:

$$a_n^{(i)} = v_k^{(n)}. \qquad (5.6)$$

Так як заданих властивостей може бути декілька, то вони можуть бути представлені вектором

$$\boldsymbol{v}_i = (v_{1.}, \ldots, v_j, \ldots, v), \qquad (5.7)$$

де v_j – задане значення j-тої властивості в наборі властивостей A_i.

Завдяки цього представлення надається можливість формально описати критерії кібербезпеки інформаційного відношення сегмента кіберпростору, сформованого на основі сервісів інформаційно-комунікаційної системи *IKS*. Для цього введемо *функцію кібербезпеки інформаційного відношення CyberSecurity (.)*, яка задається наступним чином

$$CyberSecurity(IA_i,) = \begin{cases} 1, \text{ (кібербезпека забезпечена), якщо } \boldsymbol{v}_i^* = \boldsymbol{v}_i; \\ 0, \text{ (кібербезпека відсутня), якщо } \boldsymbol{v}_i^* \neq \boldsymbol{v}_i, \end{cases} \quad (5.8)$$

де :

$\boldsymbol{v}_i$ – вектор заданих значень властивостей інформаційного продукту;

$\boldsymbol{v}_i^*$ – вектор отриманих значень властивостей інформаційного продукту.

Зрозуміло, що критерієм забезпечення кібербезпеки всього сегменту кіберпростору на основі всіх актуальних послуг *IKS* буде виконання заданих вимог в рамках всіх інформаційних відносин, тобто:

$$CyberSecurity(ITS)=CyberSecurity(IA_1,)\&CyberSecurity(IA_2,)\& \ldots \& CyberSecurity(IA_I,) = 1. \quad (5.8)$$

Приклад опису конкретної ситуації.

Нехай ІКС повинна забезпечити наступні сервіси:

1) передачу одного файлу з вимогами забезпечення конфіденційності (*confidentiality*) та цілісності (*integrity*). Тобто задано інформаційне відношення IA_1;

2) перетворення іншого файлу за допомогою заданої програми за вимоги коректності її виконання (correctness). Тобто задано інформаційне відношення IA_2.

Для *сервісу передачі файлу даних* відповідно до (5.7) задані властивості будуть відображені наступним вектором

$$\boldsymbol{v}_1 = (v_{conf}=1, v_{integrity}=1).$$

Для сервісу *перетворення даних файлу* задані властивості будуть відображені наступним вектором

$$\boldsymbol{v}_2 = (v_{\text{correctness}}=1).$$

Кибербезпека заданого сегменту кіберпростору буде забезпечуватися коли для любих несанкціонованих навмисних дій буде виконуватися наступна умова

$$CyberSecurity(ITS)=CyberSecurity(IA_1,)\&CyberSecurity(IA_2,)=1, \quad (5.10)$$

тобто вектори заданих та отриманих значень властивостей інформаційних продуктів у кожному інформаційному відношенні мають співпадати (принцип «що хотіли, те й отримали»)

$$\boldsymbol{v}_1^*=\boldsymbol{v}_1; \boldsymbol{v}_2^*=\boldsymbol{v}_2.$$

Таким чином математична модель кіберпростору (5.1 – 5.7) і критерії кібербезпеки (5.8, 5.9) доповнюють показані раніше результати термінологічної та графічної формалізації.

Висновки за розділом 5

- ***Інформація про об'єкт А в об'єкті В, I(A:B)*** - це властивість (атрибут) об'єкту В, що придбана (перенесена) в результаті фізичної взаємодії з об'єктом А та є відображенням властивості цього об'єкту А.
- **Носій інформації** - об'єкт, в якому відображені властивості іншого об'єкту.

- **Користувач ІКС** - це людина або технічний об'єкт (система), які використовують інформаційний продукт ІКС в своїх інтересах (цілях).
- **Інформаційний продукт ІКС** - це інформація із заданими користувачем властивостями, яка формується інформаційним сервісом (послугою).
- **Інформаційний сервіс** (послуга) - це сукупність дій з вихідною інформацією, що формує інформаційний продукт із заданими властивостями.
- **Властивості інформації** - це ті якості інформації, які потрібні користувачу інформації.
- **Інформаційне відношення** - це сукупність вхідної інформації, обраного інформаційного сервісу та сформованого інформаційного продукту.
- **Кіберпростір** - це сукупність інформаційних відносин між користувачами ІКС, які формуються за допомогою комп'ютерних послуг (сервісів) цих систем.
- **Кібербезпека** – це стан інформаційно-комунікаційної системи, при якому навмисні несанкціоновані дії у кіберпросторі не порушують для користувачів послуг задані властивості інформації.

Контрольні питання та завдання

1. Які компоненти кіберпростору впливають на стан кібербезпеки?
2. Інформаційний продукт ІКС?
3. Інформаційний сервіс?
4. Інформаційне відношення?
5. Кіберпростір?
6. Кібербезпека?

6. БЕЗПЕКА НАЦІОНАЛЬНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

- **складові критичної інфраструктури**
- **категорії критичності об'єктів критичної інфраструктури**
- **реєстр об'єктів критичної інфраструктури**
- **національна система захисту критичної інфраструктури**

В цьому розділі буде розглянуто правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури. Кіберзахист інформаційно-комунікаційних систем, які є основою управління сучасними соціальними або технічними системами, становить важливу компоненту у забезпечені безпеки національної критичної інфраструктури.

6.1. Складові критичної інфраструктури

Захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України. Закон України "Про критичну інфраструктуру" [11] визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. Цей закон визначає терміни, що пов'язані із кіберзахистом критичної інфраструктури, наступним чином:

об'єкт критичної інфраструктури - системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєва важливим національним інтересам;

критична інфраструктура - сукупність об'єктів критичної інфраструктури;

безпека критичної інфраструктури - стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури;

захист критичної інфраструктури - всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації;

національна система захисту критичної інфраструктури - сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій - у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури;

критична технологічна інформація - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об'єктів критичної інфраструктури.

Закон "Про основні засади забезпечення кібербезпеки України" доповнює важливими, з точки зору, впровадження заходів кіберзахисту, поняттями:

об'єкт критичної інформаційної інфраструктури (ОКІІ) - комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

система управління технологічними процесами (далі - технологічна система) - автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від

наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних.

Таким чином, національна критична інфраструктура (НКІ) складається з об'єктів критичної інфраструктури (ОКІ), частиною яких є об'єкти критичної інформаційної інфраструктури (ОКІІ). Кожний ОКІІ забезпечує функцію керування в рамках ОКІ. Всі сучасні системи керування реалізовані на основі використання комп'ютерних технології. Тобто, ОКІІ – це ІКС, яка є основою кіберсегменту ОКІ. З точки зору виду об'єкту, яким здійснюється керування в рамках ОКІ, необхідно виділяти ІКС, що застосовується для управління персоналом (адміністративні ІКС, в англомовному просторі – системи інформаційних технологій, IT-system. У випадках, якщо ІКС використовується для управління технічними системами або технологічними процесами, то таки системи називають автоматизованими (або – автоматичними) системами управління технологічними процесами (АСУ ТП). В англомовному просторі таки системи мають назву індустріальні (промислові) системи управління (Industrial Control Systems, ICS).

Для організації ефективного забезпечення безпеки і стійкості критичної інфраструктури з урахуванням специфіки забезпечення окремих життєва важливих функцій та/або послуг визначаються сектори критичної інфраструктури. Для секторів критичної інфраструктури визначаються особливості реалізації державної політики у сфері захисту критичної інфраструктури. Формування та реалізацію державної політики у відповідних секторах здійснюють секторальні органи у сфері захисту критичної інфраструктури.

Секторальні органи у сфері захисту критичної інфраструктури складають та ведуть секторальні переліки об'єктів критичної інфраструктури. Перелік секторів критичної інфраструктури та суб'єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах

національної системи захисту критичної інфраструктури (далі - Перелік), визначається Кабінетом Міністрів України. У разі необхідності внесення змін до Переліку Кабінет Міністрів України переглядає та змінює його виходячи з критеріїв критичності.

До життєва важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належить діяльність у наступних секторах критичної інфраструктури [11]:

1) урядування та надання найважливіших публічних (адміністративних) послуг;

2) енергозабезпечення (у тому числі постачання теплової енергії);

3) водопостачання та водовідведення;

4) продовольче забезпечення;

5) охорона здоров'я;

6) фармацевтична промисловість;

7) виготовлення вакцин, стале функціонування біолабораторій;

8) інформаційні послуги;

9) електронні комунікації;

10) фінансові послуги;

11) транспортне забезпечення;

12) оборона, державна безпека;

13) правопорядок, здійснення правосуддя, тримання під вартою;

14) цивільний захист населення та територій, служби порятунку;

15) космічна діяльність, космічні технології та послуги;

16) хімічна промисловість;

17) дослідницька діяльність.

6.2. Категорії критичності об'єктів критичної інфраструктури

Для визначення рівня вимог щодо забезпечення захисту об'єктів критичної інфраструктури відповідно до рівня їх важливості для забезпечення окремих життєва важливих функцій у межах секторів критичної інфраструктури здійснюється категоризація об'єктів критичної інфраструктури

відповідно до категорій критичності[11].Установлюються такі категорії критичності об'єктів критичної інфраструктури:

1) І категорія критичності - особливо важливі об'єкти, які мають загальнодержавне значення, значний вплив на інші об'єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

2) ІІ категорія критичності – життєва важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

3) ІІІ категорія критичності - важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

4) IV категорія критичності - необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

Категоризація об'єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури відповідно до секторальної специфіки та вимог секторального законодавства.

Секторальні органи разом з операторами критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до Методики категоризації об'єктів критичної інфраструктури, що затверджується Кабінетом Міністрів України, а в банківській та фінансовій системах - Національним банком України

6.3. Реєстр об'єктів критичної інфраструктури

Для цілей узгодження дій суб'єктів національної системи захисту критичної інфраструктури формується Реєстр об'єктів критичної інфраструктури (далі - Реєстр).

Збирання, узагальнення, попередній аналіз даних щодо об'єктів критичної інфраструктури та пропозиції щодо включення таких об'єктів до Реєстру в межах визначених секторів здійснюються секторальними органами у сфері захисту критичної інфраструктури. Реєстр формується та ведеться уповноваженим органом у сфері захисту критичної інфраструктури України на основі пропозицій суб'єктів національної системи захисту критичної інфраструктури.

Після включення об'єкта до Реєстру секторальні органи у сфері захисту критичної інфраструктури повідомляють про це оператора об'єкта критичної інфраструктури для забезпечення паспортизації та захисту об'єкта критичної інфраструктури відповідно до вимог [14].

Інформація про об'єкти критичної інфраструктури, що міститься в Реєстрі, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом. Розпорядник забезпечує цілодобовий доступ до відкритої інформації Реєстру на своєму офіційному веб-сайті.

Для посадових осіб суб'єктів національної системи захисту критичної інфраструктури інформація з Реєстру у зв'язку із здійсненням ними повноважень, передбачених законом, надається за суб'єктом права чи за об'єктом критичної інфраструктури в електронній формі шляхом безпосереднього доступу до Реєстру, за умови ідентифікації відповідної посадової особи у порядку, встановленому Законом України "Про електронні довірчі послуги".

6.4. Національна система захисту критичної інфраструктури

Для формування та реалізації державної політики у сфері захисту критичної інфраструктури України створюється **національна система захисту критичної інфраструктури** (НСЗКІ), що є сукупністю:

- органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій - у разі утворення),

- органів місцевого самоврядування,

- операторів критичної інфраструктури,

на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури.

Суб'єктами національної системи захисту критичної інфраструктури є:

1) Кабінет Міністрів України;

2) Апарат Ради національної безпеки і оборони України;

3) Центральна виборча комісія;

4) Національний банк України;

5) Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг;

6) Адміністрація Державної служби спеціального зв'язку та захисту інформації України;

7) Фонд державного майна України, інші центральні органи виконавчої влади із спеціальним статусом;

8) уповноважений орган у сфері захисту критичної інфраструктури України;

9) центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту;

10) секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади;

11) Служба безпеки України;

12) правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності;

13) Збройні Сили України, інші військові формування, утворені відповідно до законів України;

14) місцеві органи виконавчої влади (військово-цивільні адміністрації - у разі утворення);

15) органи місцевого самоврядування;

16) оператори критичної інфраструктури;

17) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури.

Безпосереднє впровадження заходів захисту на ОКІ здійснює **оператор критичної інфраструктури** - юридична особа будь-якої форми власності та/або фізична особа-підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування.

Забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:

штатний режим - функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

режим готовності та запобігання реалізації загроз - секторальними та функціональними органами у сфері захисту критичної інфраструктури: проводиться перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

режим реагування на виникнення кризової ситуації - суб'єктами національної системи захисту критичної інфраструктури із застосуванням заходів реагування на кризову ситуацію. Функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступ до об'єктів;

режим відновлення штатного функціонування - суб'єктами національної системи захисту критичної

інфраструктури: застосовуються заходи щодо повернення параметрів функціонування критичної інфраструктури до штатного режиму. Функціонування інфраструктури здійснюється з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи.

Висновки за розділом 6

- **Об'єкт критичної інфраструктури** - системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєва важливим національним інтересам.
- **Критична інфраструктура** - сукупність об'єктів критичної інфраструктури.
- **Безпека критичної інфраструктури** - стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури.
- **Захист критичної інфраструктури** - всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації.
- **Національна система захисту критичної інфраструктури** - сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій - у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури.

- **Критична технологічна інформація** - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об'єктів критичної інфраструктури.
- **Об'єкт критичної інформаційної інфраструктури** (ОКІІ) - це ІКС, яка забезпечує функцію керування в рамках ОКІ.
- **І категорія критичності** - особливо важливі об'єкти, які мають загальнодержавне значення, значний вплив на інші об'єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення.
- **ІІ категорія критичності** - життєва важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення.
- **ІІІ категорія критичності** - важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення.
- **IV категорія критичності** - необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

Контрольні питання та завдання

1. Об'єкт критичної інфраструктури?
2. Критична інфраструктура?
3. Об'єкт критичної інформаційної інфраструктури?
4. Категорія критичності?
5. Безпека критичної інфраструктури?
6. Захист критичної інфраструктури?
7. Національна система захисту критичної інфраструктури?

7. КІБЕРЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

- **рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури**
- **загальні вимоги до кіберзахисту об'єктів критичної інфраструктури**

У 2022 році Верховною Радою України ухвалено Закон України «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України». Відповідно до внесених змін, на Держспецзв'язку покладене виконання функцій уповноваженого органу з питань захисту критичної інфраструктури України. З цією метою у складі Адміністрації Держспецзв'язку було утворено новий Департамент (Департамент захисту критичної інфраструктури Адміністрації Держспецзв'язку).

На кінець 2023 року структура, сутність та порядок впровадження заходів кіберзахисту об'єктів критичної інформаційної інфраструктури (тобто ІКС, що застосовуються для управління об'єктами критичної інфраструктури) визначається наступними документами:

1) Методичні рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601 [15];

2) Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518 [16].

Ці документи описують кіберзахист у вигляді циклічного процесу застосування відповідних заходів та механізмів, порядок впровадження та контролю цього процесу з метою підвищення рівня кібербезпеки критичної інформаційної інфраструктури.

7.1. Методичні рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури

Цей документ (далі – Рекомендації) розроблено з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity[1]), виданої у 2014 році та оновленої[2] у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology) [17]. На національному рівні ці принципи кіберзахисту також відображені в ДСТУ ISO/IEC TS 27110:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанови щодо розроблення інфраструктури кібербезпеки (ISO/IEC TS 27110:2021, IDT) [18].

7.1.1. Загальні характеристики

Для опису процесу кіберзахисту Рекомендації застосовують наступні підходи:

- всі заходи кіберзахисту поділяються на 5 етапів;
- послідовне виконання функції цих етапів складає цикл кіберзахисту;
- безперервність кіберзахисту забезпечується послідовним повторюванням циклів (циклічний процес);
- в основі кожного циклу застосовується концепція управління ризиками загроз (ідентифікація та оцінювання ризиків загроз, визначення фактів реалізації загроз, обробка ризиків загроз до прийнятного рівня);
- для опису комплексу заходів кіберзахисту кожного етапу застосовується принцип ієрархічної декомпозиції:
  a) всі заходи поділяються на окремі блоки:
  b) всі блоки розміщуються на різних рівнях ієрархії;
  c) кожний блок заходів вищого рівня реалізується послідовністю (набором) блоків нижнього рівня;

d) більш загальний опис заходу вищого рівня деталізується в описах блоків нижнього рівня.

Структура Рекомендацій складається з трьох основних частин:

- система (таксономія) заходів кіберзахисту;
- рівнів упровадження заходів кіберзахисту;
- профілі кіберзахисту.

Розглянемо всі частини по черзі.

7.1.2. Система (таксономія) заходів кіберзахисту

Система (таксономія) заходів кіберзахисту (далі – СЗКЗ) – це впорядкований набір заходів з кіберзахисту, бажаних результатів кіберзахисту та відповідних нормативних та інформативних посилань, що є загальними в усіх галузях критичної інфраструктури. СЗКЗ базується на нормативних документах, національних та міжнародних стандартах, усталеній практиці захисту інформації та забезпечення кібербезпеки, що розвиваються разом з технологіями забезпечення кібербезпеки. Це забезпечує ефективність реалізації заходів кіберзахисту та можливість підтримки нових технологій і методів забезпечення кібербезпеки.

Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п’яти функцій кібербезпеки (мал. 7.1): 1) ідентифікація ризиків; 2) кіберзахист; 3)виявлення кіберінцидентів; 4) реагування; 5) відновлення поточного стану кібербезпеки.

формує цикл управління кібербезпекою, який складається з п’яти функцій кіберзахисту (мал. 7.1): 1) ідентифікація ризиків; 2) кіберзахист; 3)виявлення кіберінцидентів; 4) реагування; 5) відновлення поточного стану кібербезпеки.

Мал. 7.1. Цикл управління кібербезпекою

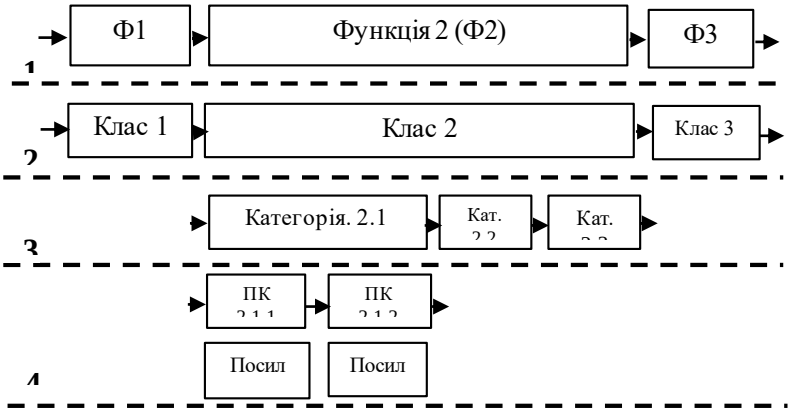
Функції циклу управління кібербезпекою забезпечують:

- прийняття рішення з управління ризиками кібербезпеки на ОКІІ;
- вибір та впровадження заходів кіберзахисту;
- реагування на загрози кібербезпеки;
- удосконалення кіберзахисту, враховуючи набутий досвід.

Опис змісту заходів кіберзахисту, що реалізують всі функції циклу управління кібербезпекою, складається з чотирьох компонентів:

- клас заходів кіберзахисту;
- категорій заходів кіберзахисту;
- підкатегорії заходів кіберзахисту;
- інформаційні посилання.

Логічний зв'язок між всіма функціями циклу управління кібербезпекою та компонентами опису заходів кіберзахисту може бути представлений чотирьох рівнявою ієрархічною структурою (мал. 7.2).



Мал. 7.2. Чотирьохрівнява ієрархічна структура системи заходів кіберзахисту

Кожної функції відповідає один клас заходів кіберзахисту. В свою чергу, кожний клас поділяється на декілька категорій (Кат.) заходів кіберзахисту, які уточнюють їх сутність. Подальше уточнення заходів забезпечується під категоріями (ПК.). З кожною під категорією зв'язані посилання на інформаційні джерела, за допомогою яких можливо визначити конкретні техніки та процедури.

Запропонована ієрархічна структура дозволяє перейти від загального вербального опису заходів кіберзахисту до формалізованого опису на рівні застосування комп'ютерних технологій.

7.1.3. Класи заходів кіберзахисту

Клас заходів кіберзахисту визначає сутність заходів організовує заходи кіберзахисту на системному рівні та визначає зміст циклу управління кібербезпекою. Рекомендаціями визначено п'ять класів заходів кіберзахисту:

ідентифікація ризиків кібербезпеки;

кіберзахист;

виявлення кіберінцидентів;

реагування на кіберінциденти;

відновлення поточного стану кібербезпеки.

Кожний клас заходів кіберзахисту має свій ідентифікатор, що складається з двох літер.

Клас заходів кіберзахисту «Ідентифікація ризиків кібербезпеки» (ID) передбачає заходи, реалізація яких спрямована на поглиблення знань керівництва та персоналу ОКІІ щодо наявних ризиків, способів управління ризиками кібербезпеки для інформаційних систем, активів, даних, що використовуються для надання життєва важливих послуг та функцій. Реалізація заходів кіберзахисту класу «Ідентифікація ризиків» є чинником для ефективного використання Рекомендацій, розуміння умов, ресурсів, що підтримують надання життєва важливих послуг та функцій, а також пов'язаних ризиків кібербезпеки, обґрунтованого вибору конкретних заходів для впровадження. Це дозволяє визначити пріоритетність ризиків кібербезпеки потребами надання життєва важливих послуг та функцій, а також розподіляти ресурси і зусилля відповідно до встановлених пріоритетів.

Клас заходів кіберзахисту «Кіберзахист» (PR) визначає діяльність із розробки та впровадження відповідних методів, засобів, процедур кіберзахисту для забезпечення стійкого, безперервного та безпечного надання життєва важливих послуг та функцій ОКІ. Ці заходи дозволяють обмежити або стримати вплив кіберінцидентів.

Клас заходів кіберзахисту «Виявлення кіберінцидентів» (DE) містить заходи своєчасного виявлення кіберінцидентів.

Клас заходів кіберзахисту «Реагування на кіберінциденти» (RS) містить заходи реагування на кіберінциденти та кібератаки. Реалізація заходів спрямована на зниження потенційного негативного впливу кіберінциденту (кібератаки) на надання життєва важливих послуг та функцій.

Клас заходів кіберзахисту «Відновлення стану кібербезпеки» (RC) визначає діяльність щодо забезпечення

спроможностей ОКІІ щодо стійкого, надійного та безперервного надання життєва важливих послуг та функцій, які були порушені внаслідок кіберінциденту (кібератаки). Ці заходи забезпечують своєчасне відновлення штатної роботи ОКІІ та зменшення негативного впливу кіберінциденту (кібератаки).

7.1.4. Категорії, підкатегорії заходів кіберзахисту та інформаційні посилання

Категорія заходів кіберзахисту являє собою складову класу заходів кіберзахисту. Всі заходи кіберзахисту в рамках категорії упорядковані за цільовими результатів забезпечення кібербезпеки. Прикладами категорій заходів кіберзахисту є «Управління активами», «Управління доступом» тощо. Кожна категорія заходів кіберзахисту має власний ідентифікатор, який складається з ідентифікатора класу заходів кіберзахисту (перші дві літери) та ідентифікатора категорії (останні дві літери). Наприклад, управління активами – ID.AM.

Підкатегорія заходів кіберзахисту являє собою складовий елемент категорії заходів кіберзахисту. Підкатегорії заходів кіберзахисту містять сукупність конкретних заходів кіберзахисту, які сформульовані у вигляді конкретного результату, що має бути досягнутий під час упровадження заходів кіберзахисту. По суті це набір результатів, які, хоча і не є вичерпними, але допомагають досягти цільових результатів забезпечення кібербезпеки за кожною категорією заходів кіберзахисту. Прикладами підкатегорій є «Зовнішні інформаційні системи задокументовано», «Дані, що зберігаються, захищено», «Повідомлення систем виявлення вторгнення досліджено». Кожна підкатегорія заходів кіберзахисту має свій власний ідентифікатор, що складається з ідентифікатора категорії заходів кіберзахисту та порядкового номера підкатегорії. Наприклад: ID.AM-1

І*нформаційне посилання* являє собою елемент системи заходів кіберзахисту, який містить посилання на стандарти, нормативні документи, рекомендації та загальноприйняті практики, поширені у галузях (секторах) критичної інфраструктури для забезпечення безпеки ОКІІ. Ці посилання ілюструють методи, способи та технології досягнення цільових результатів (показників) для кожної підкатегорії заходів кіберзахисту. Інформаційні посилання, наведені в Рекомендаціях, є довідковими та не є вичерпними. Нормативні посилання базуються на національних стандартах, нормативних документах, прийнятих в Україні. Довідкові посилання базуються на міжнародних і регіональних стандартах, нормативних документах інших країн. У таблиці 1 наведено систему заходів кіберзахисту.

Таблиця 7.1. Система заходів кіберзахисту

Категорія заходів кіберзахисту	Опис	Заходи кіберзахисту

1	2	3
	Клас заході в кіберзахисту «Ідентифікація ризиків кібербезпеки» (ID)	
ID.AM Управління активами	Описуються дані, персонал, пристрої та носії інформації, інформаційні системи, що дозволяють забезпечити надання життєва важливих послуг та функцій до рівня важливості для організації відносно життєва важливих послуг та функцій, а також описується політика управління ризиками.	ID.AM-1 ID.AM-2 ID.AM-3 ID.AM-4 ID.AM-5 ID.AM-6

ID.BE Середовище надання життєва важливих послуг та функцій	Формування обов'язків персоналу щодо забезпечення кібербезпеки, а також рішень з управління ризиками у сфері кібербезпеки.	ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5
ID.GV Управління безпекою	Формування правил, процедур і процесів для управління й моніторингу впроваджених нормативних, екологічних та експлуатаційних вимог, а також вимог щодо забезпечення кібербезпеки.	ID.GV-1 ID.GV-2 ID.GV-3 ID.GV-4
ID.RM Стратегія управління ризиками організації	Визначення пріоритетів, обмежень, допустимого рівня ризику для підтримки рішень щодо зниження ризиків кібербезпеки.	ID.RM-1 ID.RM-2 ID.RM-3
ID.SC Управління ризиками системи постачання	Визначення пріоритетів, обмежень, допустимого рівня ризику щодо системи постачання для підтримки рішень щодо ризиків, пов'язаних із системою постачання послуг третіми особами.	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4
	Клас заходів кіберзахисту «Кіберзахист» (PR)	
PR.AC Управління ідентифікацією, автентифікацією та контроль доступу	Забезпечення доступу до фізичних і логічних ресурсів ОКІ та пов'язаних з ними об'єктів тільки для авторизованих користувачів, адміністраторів або процесів. Управління здійснюється з урахуванням встановленого допустимого рівня ризику несанкціонованого доступу.	PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6

PR.AT Обізнаність та навчання	Забезпечення інформування та обізнаності організації та партнерів організації щодо питань кібербезпеки. Співробітники мають освіту або пройшли спеціалізовану підготовку для покращення інформованості з питань кібербезпеки, пройшли належну підготовку для виконання своїх обов'язків щодо забезпечення кібербезпеки відповідно до встановлених політик, правил, процедур та угод.	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5
PR.DS Безпека даних	Забезпечення управління інформацією та документацією, з метою захисту конфіденційності, цілісності та доступності інформації.	PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-4 PR.DS-5 PR.DS-6 PR.DS-7 PR.DS-8
PR.IP Процеси та процедури кіберзахисту	Забезпечення підтримання та управління політикою (правилами) безпеки, процесами та процедурами, які використовуються для управління захистом інформаційних систем і активів організації.	PR.IP-1 PR.IP-2 PR.IP-3 PR.IP-4
		PR.IP-5 PR.IP-6 PR.IP-7 PR.IP-8 PR.IP-9 PR.IP-10
PR.MA Технічне обслуговування	Технічне обслуговування та ремонт компонентів системи управління виробничими процесами, компонентів інформаційно-комунікаційних систем виконуються	PR.MA-1 PR.MA-2

	з дотриманням правил та процедур безпеки.	
PR.PT Технології кіберзахисту	Управління технічними рішеннями (технологіями) кіберзахисту з метою забезпечення безпеки та стійкості систем і активів організації з дотриманням правил, процедур з безпеки.	PR.PT-1 PR.PT-2 PR.PT-3 PR.PT-4 PR.PT-5
	Клас за ходів кіберзахисту «Виявлення кіберінцидентів» (DE)	
DE.AE Аномалії та кіберінциденти	Своєчасне виявлення аномальної активності та передбачення потенційного впливу кіберінцидентів.	DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5
DE.CM Безперервний моніторинг кібербезпеки	Відстеження безпеки інформаційних систем та активів організації через дискретні інтервали для виявлення кіберінцидентів та перевірки ефективності заходів кібербезпеки.	DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-4 DE.CM-5 DE.CM-6 DE.CM-7 DE.CM-8
DE.DP Процеси виявлення кіберінцидентів	Підтримання і тестування процесів й процедур виявлення кіберінцидентів для забезпечення своєчасного та адекватного оповіщення про аномальні кіберінциденти.	DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5
	Клас заходів кіберзахисту «Реагування на кіберінциденти» (RS)	

RS.RP Планування реагування	Процеси та процедури реагування на кіберінциденти виконуються та підтримуються з метою забезпечення своєчасного реагування на виявлені кіберінциденти.	RS.RP-1
RS.CO Комунікації	Координація заходів з реагування між внутрішніми та зовнішніми партнерами організації (у разі доцільності).	RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5
RS.AN Аналіз	Проведення аналізу кіберінцидентів для забезпечення адекватних заходів реагування та підтримки відновлення.	RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4
RS.MI Мінімізація наслідків.	Виконання заходів з метою запобігання розширенню кіберінциденту, мінімізації його наслідків та унеможливлення його повторення.	RS.MI-1 RS.MI-2 RS.MI-3
RS.IM Удосконалення	Удосконалення заходів з реагування шляхом врахування досвіду з поточних або виконаних заходів виявлення/реагування.	RS.IM-1 RS.IM-2
	Функція кібербезпеки «Відновлення стану кібербезпеки» (RC)	
RC.RP Планування відновлення	Процеси та процедури відновлення виконуються та підтримуються з метою своєчасного відновлення систем або активів, постраждалих від кіберінцидентів.	RC.RP-1
RC.IM Удосконалення	Планування відновлення та процеси відновлення удосконалюються шляхом урахування отриманого досвіду.	RC.IM-1 RC.IM-2

RC.CO Комунікації	Заходи з відновлення координуються з внутрішніми та зовнішніми партнерами організації, такими як координаційні центри, оператори, провайдери телекомунікацій, власники атакуючих систем, інші групи реагування на інциденти, пов'язані з інформаційною та/або кібербезпекою (CSIRT), та постачальники.	RC.CO-1 RC.CO-2 RC.CO-3

Повну класифікація заходів кіберзахисту наведено у додатку 1 до Рекомендацій.

7.1.5. Рівні впровадження заходів з кіберзахисту

Рівні впровадження заходів кіберзахисту характеризують ступінь практичного впровадження організацією заходів із кіберзахисту, здатність організації досягти запланованих результатів кіберзахисту та надають інструментарій оцінювання ступеня впровадження процесів управління кібербезпекою. Визначаються чотири рівні впровадження заходів кіберзахисту:

1) рівень – частковий;
2) рівень – ризик-орієнтований;
3) рівень – повторюваний;
4) рівень – адаптивний.

Кожний вищий рівень відображає більш досконалий характер впровадження заходів кіберзахисту. Особливості рівнів впровадження циклу управління кібербезпеки наступні.

1 рівень. Заходи кіберзахисту впроваджені, але їх опис не формалізований Обмежене розуміння ризиків кіберзагроз (відсутня модель загроз). Відсутній оперативний обмін інформацією в секторі кібербезпеки сектору критичної інфраструктури.

2 рівень. Заходи кіберзахисту впроваджені, їх опис частково формалізований.

Існують розуміння ризиків та модель загроз. Відсутній формалізований процес управління ризиками. Існує оперативний обмін інформацією в секторі кібербезпеки сектору критичної інфраструктури, але цей процес не формалізований.
3 рівень. Заходи захисту впроваджені на основі формалізованих моделей ризиків, кіберзагроз та процесів управління ризиками. Взаємодія з іншими ОКІ діє на основі формалізованого процесу. Відсутні формалізовані процеси по оперативному реагуванню на зміну стану кібербезпеки.
4 рівень. Існує формалізований опис процесів оперативного реагування на зміну стану кібербезпеки. Практика кіберзахисту адаптується на основі практичного досвіду, актуальної інформації про нові загрози та показників стану безпеки.

7.1.6. Профіль кіберзахисту ОКІІ

Система (таксономія) заходів кіберзахисту є основою для вибору набору конкретних заходів, що враховують особливості окремої ОКІІ. Набір цих заходів відображається в Профілі кіберзахисту. Цей документ розробляється також з урахуванням:

- вимог галузевих стандартів, керівних принципів безпеки, політик безпеки та практик організації;
- особливих вимог до кожного ОКІІ або ОКІ;
- вимог до захисту інформації.

Профіль кіберзахисту дозволяє розробити план впровадження заходів кіберзахисту з метою зниження ризиків кібербезпеки, узгоджений з цілями ОКІ та галузі (сектору) критичної інфраструктури, врахувати законодавчі та нормативні вимоги та передовий галузевий досвід із забезпечення кібербезпеки, а також відображає пріоритети управління ризиками кібербезпеки. Оскільки більшість ОКІІ мають складну організаційно-технічну структуру, використовують різні інформаційні, інформаційно-комунікаційні та автоматизовані системи управління технологічними процесами для надання

життєва важливих послуг та функцій, можна розробляти кілька профілів кіберзахисту, узгоджених з конкретними системами, процесами та потребами ОКІІ, що призначені для надання життєва важливих послуг та функції.

7.1.7. Види профілів кіберзахисту

Профіль кіберзахисту використовують для опису поточного стану реалізованих заходів кіберзахисту на ОКІІ (поточний профіль кіберзахисту) або бажаного цільового стану реалізації конкретних заходів кіберзахисту (цільовий профіль кіберзахисту).

Поточний профіль кіберзахисту зазначає заходи та результати ефективності їх впровадження на поточний час.

Цільовий профіль кіберзахисту зазначає заходи та цільові показники забезпечення кібербезпеки, необхідні для досягнення бажаних цілей управління ризиками кібербезпеки.

Профілі підтримують стратегічні цілі ОКІ та допомагають обмінюватися даними про ризики кібербезпеки всередині ОКІІ та між ОКІІ всередині сектору критичної інфраструктури та об'єктами, що належать різним секторам критичної інфраструктури.

Профіль кіберзахисту рекомендується розробляти відповідно до вимог галузевих нормативних документів із захисту інформації та практичного досвіду забезпечення інформаційної безпеки та кібербезпеки ОКІ з урахуванням особливостей забезпечення кібербезпеки у відповідній сфері або галузі.

Порівняння профілів кіберзахисту (наприклад, поточного та цільового профілів) сприяє виявленню недоліків, що повинні бути усунуті для досягнення цілей управління ризиками кібербезпеки. Рекомендовано використання плану усунення недоліків як складової частини плану захисту інформації (плану кіберзахисту) ОКІІ. Пріоритетність заходів усунення недоліків

базується на потребах ОКІ щодо надання основних послуг і процесах управління ризиками.

В таблицях 7.3. та 7.4. надаються приклади фрагментів поточного та цільового профілю кіберзахисту.

Таблиця 7.3. Приклад поточного профілю кіберзахисту ОКІІ

Функція кібербезпеки	Категорія заходів кіберзахисту	Заходи кіберзахисту	Профіль кіберзахисту (Поточна практика захисту інформації)
Організація, що використовує вимоги стандартів			
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	У разі реалізованої СУІБ відповідно до ДСТУ ISO/IEC 27001. Контроль віддаленого доступу здійснюється відповідно до вимог ДСТУ ISO/IEC 27001: A.6.2.1; A.6.2.2; A.11.2.6; A.13.1.1; A.13.2.1. Рівень упровадження – другий рівень – ризик-орієнтований.
			У разі побудованої КСЗІ. Контроль віддаленого доступу реалізовано відповідно до вимог НД ТЗІ 2.5-004-99: ДР-2, ДС-1, НР-2, НИ-2, НО-2, НЦ-1, НТ2, НВ-1.

			Рівень гарантій – Г2. Рівень упровадження – третій рівень – повторюваний.
			У разі побудованої системи захисту інформації на основі галузевих стандартів. Система захисту інформації побудована відповідно до вимог міжнародного стандарту IEC 62443: IEC 62443-2-1:2015: 4.3.3.6.6. IEC 62443-3-3:2016: SR 1.13; SR 2.6. Рівень упровадження – другий рівень – ризик-орієнтований.

Таблиця 7.4. Приклад цільового профілю кіберзахисту ОКІІ

Функція кібербезпеки	Категорія заходів кіберзахисту	Заходи кіберзахисту	Поточний профіль кіберзахисту	Цільовий профіль кіберзахисту
Організація, що використовує власні заходи кіберзахисту				
Кіберзахист (PR)	Управління ідентифікацією, автентифікацією та контроль доступу (PR.AC)	PR.AC-3: здійснюється контроль віддаленого доступу	Комутований доступ для здійснення технічного обслуговування персоналом постачальника надається у разі потреби	Комутований доступ для здійснення технічного обслуговування персоналом постачальника надається у разі потреби

			та відключається, коли таке обслуговування завершується. Віддалений доступ дозволено лише через VPN. Діяльність під час надання віддаленого доступу записується та контролюється. Доступ до VPN надається виключно для визначених організацією пристроїв. Усі спроби несанкціонованого підключення до VPN реєструються. У разі звільнення працівника негайно скасовується його VPN-акаунт. Рівень упровадження – другий рівень –	та відключається, коли таке обслуговування завершується. Віддалений доступ дозволено лише через VPN. Діяльність під час надання віддаленого доступу записується та контролюється. Доступ до VPN надається виключно для визначених організацією пристроїв. Усі спроби несанкціонованого підключення до VPN реєструються. У разі звільнення працівника негайно скасовується його VPN-акаунт. Огляд авторизованого списку облікових записів VPN

			ризик-орієнтований.	рекомендується здійснювати двічі на рік.* Цільовий рівень упровадження – другий рівень – ризик-орієнтований

7.1.8. Порядок розробки та впровадження профілю кіберзахисту ОКІІ

Розробку та впровадження профілю кіберзахисту рекомендується проводити за такими етапами:

І етап. Визначення пріоритетів та сфери застосування Рекомендацій. Визначаються цілі та організаційні пріоритети щодо надання життєва важливих послуг та функцій. За допомогою отриманої інформації приймається рішення щодо реалізації заходів кіберзахисту та визначається обсяг інформаційних систем та активів, які підтримують надання цих послуг та функцій. Рекомендації можуть бути адаптовані для підтримки різних напрямів діяльності, процесів та систем (інформаційно-комунікаційних систем, інформаційних систем, комп'ютерних систем, автоматизованих систем управління технологічними процесами тощо), необхідних для надання життєва важливих послуг та функцій;

ІІ етап. Аналіз середовища для надання життєва важливих послуг та функцій. Визначаються відповідні системи та активи, що безпосередньо забезпечують надання життєва важливих послуг та функцій, аналізуються нормативні вимоги та загальний підхід до управління ризиками для цих систем. На цьому етапі необхідно провести консультації із суб'єктами забезпечення кібербезпеки та отримати інформацію щодо визначення загроз та вразливостей, що застосовуються саме для цих систем та активів і притаманні їм;

III етап. Створення поточного профілю кіберзахисту. Розробляється поточний профіль кіберзахисту, вказуючи, які заходи кіберзахисту, що містяться в Рекомендаціях, реалізовані на цей час. По суті розробка поточного профілю кіберзахисту є етапом самоаналізу, який дозволяє ОКІІ з'ясувати, які заходи захисту інформації впроваджено на ОКІІ та на якому рівні вони реалізовані;

IV етап. Проведення оцінки ризику. Оцінка ризику кібербезпеки має базуватися на процесі оцінки ризику, який вже впроваджено на ОКІІ або на основі результатів попередньої оцінки ризиків (наприклад, отримані під час створення КСЗІ, СУІБ, системи інформаційної безпеки або проведення аудиту безпеки). Аналіз середовища експлуатації інформаційних систем та активів проводиться з метою визначення ймовірності настання кіберінцидентів/реалізації кібератак та оцінки наслідків, які можуть настати у результаті настання такої події. Важливо враховувати нові ризики, дані про загрози та вразливості, що сприяє надійному розумінню ймовірності та наслідків кіберінцидентів;

V етап. Створення цільового профілю кіберзахисту. Розробляється цільовий профіль кіберзахисту, що базується на аналізі заходів кіберзахисту цих Рекомендацій. Цільовий профіль кіберзахисту описує бажані результати із забезпечення кібербезпеки ОКІІ. Організація може впроваджувати власні заходи кіберзахисту з метою врахування унікальних ризиків, що притаманні системам і процесам надання життєва важливих послуг та функцій. При створенні цільового профілю кіберзахисту мають бути розглянуті та враховані вплив та вимоги з кібербезпеки зовнішніх партнерів організації. Методичні рекомендації щодо розробки цільового профілю кіберзахисту наведено у додатку 3 до цих Рекомендацій.;

VI етап. Визначення, аналіз та пріоритизація недоліків. Проводиться порівняння поточного профілю кіберзахисту із цільовим профілем кіберзахисту для визначення недоліків. Далі

рекомендується розроблення Плану дій щодо усунення виявлених недоліків, який відображає завдання, результати аналізу витрат/вигоди, а також ризики досягнення результатів цільового профілю кіберзахисту. Далі ОКІІ може визначити необхідні ресурси (фінансові, матеріальні, людські), потрібні для усунення недоліків;

VII етап. Реалізація плану удосконалення заходів кіберзахисту. Визначається, які дії слід вживати для усунення виявлених недоліків. Під час реалізації плану постійно відстежуються відповідність поточної практики кіберзахисту цільовому профілю кіберзахисту. При цьому визначаються стандарти, нормативні документи, у тому числі ті, що стосуються сектору критичної інфраструктури та впроваджуються для забезпечення кібербезпеки.

Визначені етапи повторюються з метою постійної оцінки стану кібербезпеки та вдосконалення практики кіберзахисту. Термін повторення етапів встановлюється організацією, але рекомендується це робити не рідше одного разу в рік. Відстеження прогресу проводиться шляхом ітеративного оновлення поточного профілю кіберзахисту, а потім порівняння його із цільовим профілем кіберзахисту.

7.2. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури.

Загальні вимоги до кіберзахисту ОКІ (далі - 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. Цей документ впроваджує два нових поняття:

1) система інформаційної безпеки (СІД) - сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на ОКІІ з метою:

- запобігання кіберінцидентам, виявлення та захисту від кібератак:

- протидії порушенням конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на ОКІІ;

- запобігання порушенню режиму функціонування та/або недоступності служб (функцій) ОКІІ, порушенню функціонування компонентів ОКІІ;

- забезпечення спостережності за діями користувачів ОКІІ та функціонуванням засобів захисту;

2) 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.

Кіберзахист ОКІ забезпечується шляхом впровадження на ОКІІ:

- або комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю:

- або системи інформаційної безпеки (СІБ) з підтвердженою відповідністю.

КСЗІ з підтвердженою відповідністю створюється у випадку, якщо на ОКІІ обробляються державні інформаційні ресурси (ДІР) або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом. Створення КСЗІ з підтверджено. відповідністю на ОКІІ та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

СІБ з підтвердженою відповідністю створюється у випадку, якщо на ОКІІ не обробляються ДІР або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом. Створення СІБ ОКІІ здійснюється відповідно до вимог технічного завдання.

Технічне завдання формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на ОКІІ. Методичною основою для оцінки ризиків на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005.

Власник та/або керівник ОКІ організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

Державні органи отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту, через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними КСЗІ з підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними КСЗІ з підтвердженою відповідністю. Ця вимога не поширюється на інформаційно-комунікаційні системи закордонних дипломатичних установ України.

Власник та/або керівник ОКІ з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує створення резервних копій інформаційних ресурсів ОКІІ та критичних бізнес/операційних процесів ОКІ для оперативного їх відновлення у разі пошкодження або знищення.

Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій

інформаційних ресурсів, підключення до системи захищеного доступу державних органів до Інтернету Державного центру кіберзахисту використовують ресурси Національної телекомунікаційної мережі.

Налаштування та конфігураційна інформація програмних та апаратних компонентів ОКІІ, інформація про параметри та режими їх функціонування, журнали реєстрації подій (логі) та дані аудиту компонентів, інформація про облікові записи користувачів, їх атрибути та права доступу, об'єкти захисту та їх атрибути доступу, інша інформація, яка розкриває параметри та особливості функціонування компонентів ОКІІ, є інформацією з обмеженим доступом.

7.2.1. Вимоги щодо загальної політики інформаційної безпеки

На ОКІ необхідно затвердити політику інформаційної безпеки, яка визначає:

мету та основні принципи забезпечення захисту інформаційних ресурсів, критичних бізнес/операційних процесів тощо на об'єкті критичної інфраструктури;

опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, які задіяні в цьому процесі;

вимоги до порядку визначення, надання, зміни та скасування прав доступу користувачів та адміністраторів до служб (функцій), інформації та компонентів об'єкта та порядок контролю (аудиту) використання прав доступу користувачами та адміністраторами;

політику фізичної безпеки та захисту ОКІІ від навколишнього природного середовища;

вимоги до забезпечення інформаційної безпеки під час взаємодії з постачальниками;

політику управління обліковими записами в програмному та апаратному забезпеченні ОКІІ. Політика повинна визначати порядок створення, блокування та зупинення облікових записів користувачів та адміністраторів в компонентах об'єкта;

вимоги до порядку формування, надання, скасування та контролю (аудиту) за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних, для доступу до служб (функцій), інформації та компонентів ОКІІ. Повинні бути визначені також вимоги до складності паролів та періодичності їх зміни, умови блокування роботи користувача, порядок поводження із зовнішніми носіями автентифікаційних даних тощо;

політику забезпечення безперебійної роботи ОКІІ, зокрема порядок резервування даних та компонентів об'єкта, зберігання резервних копій даних, відновлення даних з резервних копій та заміни компонентів об'єкта у випадку виходу їх з ладу тощо;

порядок дій персоналу ОКІІ у випадках відмов або збоїв ОКІІ в цілому або окремих його компонентів;

порядок використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ;

політику мережевого захисту, зокрема щодо сегментації мережі ОКІІ, захисту від вірусів, зловмисного коду, шкідливого програмного забезпечення, встановлення та налаштування засобів мережевого захисту тощо;

політику проведення модернізації (оновлення) компонентів об'єкта, внесення змін до складу та в налаштування компонентів об'єкта;

опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів ОКІІ, які задіяні в цьому процесі;

політику управління оновленнями (порядок отримання, перевірки, розповсюдження та застосування оновлень програмного забезпечення компонентів об'єкта);

політику реєстрації та аудиту подій, що реєструються компонентами об'єкта. Політика повинна містити перелік подій, які реєструються кожним компонентом об'єкта, параметри ведення журналів (логів) реєстрації подій та їх архівування, порядок та періодичність аудиту журналів (логів) реєстрації подій адміністраторами ОКІІ на предмет виявлення ознак кібератак або кіберінцидентів;

політику управління інцидентами кібербезпеки, яка повинна містити перелік подій, що кваліфікуються як кіберінциденти, описи дій користувачів та адміністраторів у разі їх виникнення, порядок інформування посадових осіб об'єкта критичної інфраструктури, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди реагування на комп'ютерні надзвичайні події);

політику використання електронної пошти користувачами ОКІІ;

політику проведення внутрішнього аудиту інформаційної безпеки ОКІІ.

Політика інформаційної безпеки може затверджуватися окремими рішеннями за підписом власника та/або керівника ОКІІ. Повинен бути встановлений порядок внесення змін до таких документів.

7.2.2. Вимоги щодо управління доступом користувачів та адміністраторів до об'єктів захисту ОКІІ

Механізм розподілу прав доступу до ОКІІ повинен:

- охоплювати всі інформаційні ресурси ОКІІ (інформацію, яка зберігається та обробляється, технологічну інформацію програмного та апаратного забезпечення, журнали реєстрації подій тощо);

- визначати права на виконання операцій для всіх користувачів та адміністраторів (за необхідності також активних процесів) над інформаційними ресурсами ОКІІ (читання, модифікація, створення, видалення тощо);

- визначати права доступу користувачів та адміністраторів до служб (функцій) ОКІІ.

7.2.3. Вимоги щодо ідентифікації та автентифікації користувачів та адміністраторів ОКІІ

Користувачі та адміністратори ОКІІ (за необхідності також активні процеси) повинні отримувати доступ до служб (функцій), інформації та компонентів об'єкта в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) користувача і деякої інформації, що вводиться користувачем (пароль), та/або фізичного ідентифікатора, що надається користувачем (ключ, сертифікат, токен тощо).

Засоби ОКІІ повинні надавати можливість ідентифікації кожної операції користувача та адміністратора на об'єкті та їх протоколювання в журналах реєстрації подій.

Для надання доступу до служб (функцій) та інформації ОКІІ повинна використовуватися багатофакторна автентифікація користувачів та адміністраторів. Допускається використання двофакторної автентифікації тільки в тому програмному забезпеченні компонентів об'єкта, яке не підтримує багатофакторну автентифікацію.

На ОКІІ повинні бути заблоковані або змінені облікові записи адміністраторів та їх паролів, встановлені за замовчуванням, в усіх компонентах об'єкта. Забороняється використовувати облікові записи та паролі за замовчуванням в програмному та апаратному забезпеченні.

На ОКІІ повинні бути видалені або заблоковані неперсоналізовані і гостьові облікові записи користувачів і адміністраторів та використовуватися виключно персоналізовані облікові записи користувачів і адміністраторів в усіх компонентах об'єкта. Під час звільнення з посади

працівника його обліковий запис повинен бути негайно заблокований або видалений в усіх компонентах об'єкта.

Обладнання, яке підключається до системи управління технологічними процесами об'єкта критичної інфраструктури, повинно бути ідентифіковане (наприклад, за IP-адресою, MAC-адресою тощо), а також повинні бути вжиті заходи, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.

7.2.4. Вимоги щодо забезпечення мережевого захисту компонентів та інформаційних ресурсів

На об'єкті критичної інформаційної інфраструктури повинні використовуватися засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів. Повинно бути забезпечене централізоване управління цими засобами захисту.

Доступ адміністраторам до компонентів об'єкта повинен надаватися виключно з IP-адрес (робочих станцій), які визначені для адміністрування об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

У разі неможливості фізичного розділення зовнішньої мережі та ОКІІ на межі (периметрі) між зовнішніми мережами, іншими ІКС, що обслуговують ОКІ, та ОКІІ повинні бути встановлені засоби мережевого захисту, що виконують щонайменше такі функції захисту:

захист від атак "нульового дня" (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення;

фільтрація трафіку та розмежування доступу між мережею об'єкта критичної інфраструктури та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів,

портів, мережевих адрес, мережевих з'єднань, небажаних веб-сайтів тощо. Блокування трафіку та з'єднань, які не відповідають визначеним критеріям;

фільтрація та аналіз трафіку за визначеними відповідно до політики інформаційної безпеки критеріями;

моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики інформаційної безпеки критеріями;

виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію ОКІІ;

захист від атак типу "відмова в обслуговуванні";

захист від несанкціонованого доступу через Інтернет;

балансування навантаження;

маскування структури і мережевих адрес мережі;

завершення з'єднання з вузлом у разі атаки;

здійснення реєстрації подій, що мають відношення до безпеки.

Для захисту ОКІІ повинні використовуватися програмно-апаратні засоби, потужність яких визначається виходячи із потужності трафіку, який передбачається в мережі, з урахуванням його потенційного збільшення.

На ОКІ необхідно здійснити розподіл ОКІІ на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням між мережевих екранів або аналогічних за функціональністю засобів мережевого захисту.

Реалізована архітектура ОКІІ повинна надавати можливість розподілу мережі щонайменше на такі частини/зони:

зовнішня зона (DMZ-zone): зона із зовнішніми діапазонами адресації мережі для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів ОКІІ;

зона прикладних застосувань ОКІІ (APP-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення серверів застосувань, доступна для виконання функціональних запитів користувачів інформаційних сервісів;

зона сховищ даних ОКІІ (DB-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення баз даних, для доступу за запитами прикладних застосувань зони (APP-zone);

зона прикладних застосувань системи безпеки (Security-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення сервісів та служб захисту інформації;

тестова зона (Test-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення ОКІІ, перед тим як впровадити їх в промислову експлуатацію на ОКІІ.

Сервери та обладнання, що забезпечують функціонування сервісів та віддалений доступ клієнтів / користувачів ОКІІ із зовнішніх мереж, повинні бути розміщені в зовнішній зоні ОКІІ. З'єднання серверів та обладнання, які розміщені в зовнішній зоні, із серверами та обладнанням внутрішньої мережі об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури повинні захищатися між мережевим екраном.

Робочі станції, з яких виконуються дії щодо адміністрування програмного та апаратного забезпечення ОКІІ, а також серверні частини засобів захисту інформації повинні бути розміщені в зоні прикладних застосувань системи безпеки (Security-zone) мережі, захищеної за допомогою між мережевого екрана.

Сегмент інформаційної інфраструктури ОКІІ об'єкта критичної інфраструктури, в якому перебуває система керування технологічними процесами, повинен бути

відокремленим від інших систем об'єкта критичної інфраструктури. У випадку логічного відокремлення на межі сегмента повинен бути встановлений між мережевий екран.

Повинні бути визначені та відключені (заблоковані) програмні порти компонентів ОКІІ, які є небезпечними.

Власник/керівник ОКІ зобов'язаний проводити перевірку ефективності заходів щодо захисту ОКІІ від зовнішнього проникнення шляхом виконання періодичних (не рідше одного разу на рік) тестів на проникнення (Penetration test). У разі отримання негативних результатів після проведення тестів необхідно вжити заходів для усунення їх причин.

На ОКІІ передача даних бездротовими мережами повинна здійснюватися виключно захищеними з'єднаннями із забезпеченням її конфіденційності та цілісності. Забороняється використання на ОКІІ технологій Wi-Fi та Bluetooth.

Для захисту даних, які передаються через незахищене середовище між віддаленими користувачами, адміністраторами та ОКІІ, між компонентами об'єкта (поза контрольованою територією ОКІ), між ОКІІ та іншими (зовнішніми) інформаційно-комунікаційними системами, необхідно використовувати захищені з'єднання із

Систему управління технологічними процесами об'єкта інфраструктури дозволяється підключати до глобальних мереж передачі даних, зокрема до Інтернету, тільки у випадку неможливості функціонування технологічного процесу без підключення до Інтернету та за умови впровадження всіх заходів захисту відповідно до Загальних вимог до кіберзахисту об'єктів критичної інфраструктури або конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об'єкта критичної інфраструктури, який відноситься до відповідної сфери управління.

До глобальних мереж передачі даних, зокрема Інтернету, ОКІІ повинні підключатися через тих постачальників електронних комунікаційних мереж та/або послуг, які мають

захищені вузли доступу до глобальних мереж передачі даних із створеними КСЗІ з підтвердженою відповідністю. У договорі з надавачем цих послуг зазначаються зобов'язання щодо виконання тієї частини Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, які він надає ОКІ, та наявність КСЗІ з підтвердженою відповідністю.

7.2.5. Вимоги щодо забезпечення доступності та відмово стійкості компонентів та інформаційних ресурсів

Інформаційна інфраструктура ОКІ повинна будуватися на базі відмово стійкого підходу. Для цього в рамках ОКІІ повинні виконуватися, як мінімум, наступні заходи:

періодичне створення резервних копій інформаційних ресурсів ОКІІ та критичних бізнес/операційних процесів ОКІ, включаючи інформацію, яка зберігається на ОКІІ, технологічну інформацію компонентів об'єкта та образів серверів ОКІІ, а також їх відновлення у випадку втрати або пошкодження;

резервування критичних для функціонування ОКІІ та бізнес/операційних процесів ОКІ програмних та апаратних компонентів для забезпечення його сталого функціонування у випадку виходу з ладу одного з критичних компонентів. У разі використання на ОКІІ віртуальних серверів необхідно забезпечити їх резервування;

дублювання (кластеризація) критичних для функціонування ОКІІ та бізнес/операційних процесів ОКІ програмних та апаратних компонентів об'єкта для забезпечення його сталого функціонування, зниження навантаження та збільшення продуктивності;

використання засобів балансування навантаження;

використання джерел безперебійного живлення для критичних компонентів об'єкта;

зв'язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами

мережі передачі даних (провайдерами), - для об'єкта критичної інфраструктури, які надають свої послуги через Інтернет.

Під час розроблення, модернізації або оновлення компонентів системи управління технологічними процесами об'єкта критичної інфраструктури необхідно використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента його мережі для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення, перед тим як впровадити їх в промислову експлуатацію.

7.2.6. Вимоги щодо визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації

На об'єкті критичної інформаційної інфраструктури повинна проводитися перевірка всіх змінних (зовнішніх) пристроїв та носіїв інформації перед кожним їх використанням на ОКІІ засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

На об'єкті критичної інформаційної інфраструктури повинні забезпечуватися:

ідентифікація всіх змінних (зовнішніх) пристроїв та носіїв інформації за допомогою унікального ідентифікатора;

унеможливлення використання змінних (зовнішніх) пристроїв та носіїв інформації, які не зареєстровані на ОКІІ;

відключення автоматичного запуску програм із змінних (зовнішніх) пристроїв та носіїв інформації.

Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, мають бути заблоковані адміністраторами ОКІІ.

7.2.7. Вимоги щодо умов використання програмного та апаратного забезпечення

На об'єкті критичної інформаційної інфраструктури повинна проводитися перевірка на цілісність та автентичність

оновлень компонентів об'єкта. У разі порушення цілісності або не підтвердження автентичності оновлення воно повинно бути відхилене і не повинно застосовуватися, а цю подію необхідно запротоколювати в журналі подій.

У складі ОКІІ повинно використовуватися програмне та апаратне забезпечення, для якого не припинено підтримку виробника. Повинні використовуватися офіційні стабільні версії прикладного програмного забезпечення та драйверів.

На ОКІІ повинна надаватися перевага програмному забезпеченню, яке має більш вищий рівень гарантій відповідно до нормативного документа системи технічного захисту інформації 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", за результатами державної експертизи у сфері технічного захисту інформації.

На ОКІІ повинно блокуватися самостійне встановлення або видалення користувачами програмного забезпечення. Право на встановлення або видалення програмного забезпечення повинен мати тільки уповноважений адміністратор.

Засоби ОКІІ повинні забезпечувати неприйняття файла/повідомлення в обробку у разі отримання негативного результату перевірки електронного підпису файла/повідомлення, що надійшов/надійшло. Ця подія повинна відображатися в журналі реєстрації подій.

Програмні та апаратні засоби, які використовуються у складі ОКІІ, не повинні мати походження з іноземної держави, до якої застосовано санкції згідно із Законом України "Про санкції", чи бути розроблені/виготовлені юридичною особою - резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави.

7.2.8 Вимоги щодо умов розміщення компонентів ОКІІ

Компоненти та/або ОКІІ, крім систем управління технологічними процесами, можуть перебувати в сторонньому (не власному) центрі обробки даних тільки за умови, що центр обробки даних розташований на території України (за винятком тимчасово окупованої території України), а власником центру обробки даних є резидент України. При цьому у договорі із центром обробки даних повинні зазначатися його зобов'язання щодо виконання тієї частини Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, які він надає ОКІ.

Компоненти та інформація (дані) систем управління технологічними процесами ОКІ повинні бути розміщені тільки у власному центрі обробки даних.

З метою створення резервних копій своїх інформаційних ресурсів та їх оперативного відновлення у разі пошкодження або знищення державні органи використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

Компоненти ОКІІ повинні розміщуватися у приміщеннях, які унеможливлюють несанкціонований фізичний доступ до них сторонніх осіб.

Повинен бути забезпечений контрольований фізичний доступ до приміщень та/або комутаційних шаф, де розташовані робочі станції, сервери, мережеві компоненти та комутаційні вузли структурованої кабельної системи ОКІІ.

Забороняється підключати робочі місця адміністраторів та операторів ОКІІ до інших інформаційно-комунікаційних систем.

Схеми (креслення) розміщення обладнання структурованої кабельної системи та кабельних каналів ОКІІ, схеми підключення обладнання, таблиці маркування кабелів структурованої кабельної системи та кабельних з'єднань зберігаються в актуальному стані.

Висновки за розділом 7:

- На Держспецзв'язку покладене виконання функцій уповноваженого органу з питань захисту критичної інфраструктури України
- *Цикл управління кібербезпекою* складається з п'яти послідовних етапів кіберзахист у: 1) ідентифікація ризиків; 2) кіберзахист; 3)виявлення кіберінцидентів; 4) реагування; 5) відновлення поточного стану кібербезпеки.
- *Рівні впровадження заходів кіберзахисту* характеризують ступінь практичного впровадження організацією визначених заходів. Визначаються чотири рівні: 1) частковий; 2) ризик-орієнтований; 3) повторюваний; адаптивний. Кожний вищий рівень відображає більш досконалий характер впровадження заходів кіберзахисту.
- Набір обраних заходів відображається в *Профілі кіберзахисту*.
- *Поточний профіль кіберзахисту* зазначає заходи та результати ефективності їх впровадження на поточний час.
- *Цільовий профіль кіберзахисту* зазначає заходи та цільові показники забезпечення кібербезпеки, необхідні для досягнення бажаних цілей управління ризиками кібербезпеки.
- Кіберзахист об'єкту критичної інфраструктури (ОКІ) забезпечується шляхом впровадження на відповідному об'єкті критичної інформаційної інфраструктури (ОКІІ) або в рамках КСЗІ з підтвердженою відповідністю, або в рамках системи інформаційної безпеки (СІБ) з підтвердженою відповідністю.
- КСЗІ з підтвердженою відповідністю створюється у випадку, якщо на ОКІІ обробляються державні

інформаційні ресурси (ДІР) або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом.

- СІБ з підтвердженою відповідністю створюється у випадку, якщо на ОКІІ не обробляються ДІР або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом.
- Для надання доступу до служб (функцій) та інформації ОКІІ повинна використовуватися багатофакторна автентифікація користувачів та адміністраторів.
- Забороняється використовувати облікові записи та паролі за замовчуванням в програмному та апаратному забезпеченні.
- На ОКІІ повинні використовуватися засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів. Повинно бути забезпечене централізоване управління цими засобами захисту.
- Доступ адміністраторам до компонентів ОКІІ повинен надаватися виключно з IP-адрес (робочих станцій), які визначені для адміністрування.
- На ОКІ необхідно здійснити розподіл ОКІІ на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням між мережевих екранів або аналогічних за функціональністю засобів мережевого захисту.
- Архітектура ОКІІ повинна надавати можливість розподілу мережі щонайменше на такі частини/зони:
  - зовнішня зона (DMZ-zone): зона із зовнішніми діапазонами адресації мережі для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів ОКІІ;
  - зона прикладних застосувань ОКІІ (APP-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення серверів застосувань, доступна для виконання функціональних запитів користувачів інформаційних сервісів;

- зона сховищ даних ОКІІ (DB-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення баз даних, для доступу за запитами прикладних застосувань зони (APP-zone);
- зона прикладних застосувань системи безпеки (Security-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення сервісів та служб захисту інформації;
- тестова зона (Test-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення ОКІІ, перед тим як впровадити їх в промислову експлуатацію на ОКІІ.

- Власник/керівник ОКІ зобов'язаний проводити перевірку ефективності заходів щодо захисту ОКІІ від зовнішнього проникнення шляхом виконання періодичних (не рідше одного разу на рік) тестів на проникнення (Penetration test).
- До глобальних мереж передачі даних, зокрема Інтернету, ОКІІ повинні підключатися через тих постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними КСЗІ з підтвердженою відповідністю.

Контрольні питання та завдання

1. З яких функцій складається *цикл управління кібербезпекою*?
2. Шо відображає профіль кіберзахисту?
3. Яка ризниця між поточним та цільовим профілем кіберзахисту?
4. В яких випадках для впровадження заходів кіберзахисту на ОКІІ створюється КСЗІ з підтвердженою відповідністю?

5. В яких випадках для впровадження заходів кіберзахисту на ОКІІ створюється СІБ з підтвердженою відповідністю?
6. Розподіл на які зони повинна забезпечувати архітектура ОКІІ?
7. Призначення DMZ-zone?
8. Призначення APP-zone?
9. Призначення DB-zone?
10. Призначення Security-zone?
11. Призначення Test-zone?
12. Періодичність проведення тестування на проникнення ОКІІ?

8. ІНДУСТРІАЛЬНІ СИСТЕМИ КЕРУВАННЯ

- **принципи керування промисловими об'єктами за допомогою ICS.**
- **топологія системи керування на основі PLC**
- **топологія системи керування на основі DCS**
- **топологія системи керування на основі SCADA**
- **особливості об'єктів критичної інформаційної інфраструктури з ICS**

Індустріальні (промислові) системи керування ((Industrial Control System, ICS) — це інформаційні системи, які використовуються в індустріальних галузях для керування технологічними процесами різних промислових об'єктів [29]. В україномовному нормативному просторі замість терміну ICS часто також використовують наступні терміни: автоматизована система управління технологічними процесами (АСУ ТП); операційна технологія (ОТ).

Як правило, ICS збирають результати вимірювання датчиків (сенсорів) контролю поточного стану об'єкту керування, обробляють і відображають цю інформацію, а також передають команди керування локальному або віддаленому обладнанню виконавчих пристроїв (актуаторів). В електроенергетиці ICS можуть керувати генерацією, передачею та розподілом електроенергії, наприклад, розмикаючи та замикаючи автоматичні вимикачі та встановлюючи порогові значення для профілактичних відключень. Використовуючи інтегровані , підприємства нафтогазової промисловості можуть контролювати операції з переробки на заводі, віддалено контролювати тиск і потік у газопроводах, а також контролювати потік і шляхи транспортування газу. За допомогою ICS служби водопостачання можуть віддалено керувати рівнем водосховищ; контролювати швидкість різних потоків, рівні резервуарів або тиск у резервуарах для зберігання; контролювати характеристики якості води і

процедуру додавання хімікатів. ICS також використовуються у виробництві та хімічній переробці. Таки системи керування виконують функції, які варіюються від простих до складних; їх можна використовувати просто для моніторингу процесів — наприклад, умов навколишнього середовища в невеликій офісній будівлі — або для керування більшістю видів діяльності в муніципальній системі водопостачання чи навіть на атомній електростанції. У певних галузях промисловості, таких як хімічна промисловість і виробництво електроенергії, ICS впроваджуються, щоб забезпечити уникнення потенційно катастрофічних подій.

8.1. Класифікація індустріальних систем керування

Існує три основних типи (класи) систем керування [29]:

1) програмовані логічні контролери (Programmable Logic Controllers, PLC) — це комп'ютерні пристрої, які керують окремим промисловим обладнанням. PLC можуть використовуватися або окремо, або у якості компонент більш масштабних систем типу SCADA та DCS. Деякі приклади: керування окремими процесами конвеєру автоматизованої збірки автомобілів; керування комутаційними пристроями підстанцій системи передачі та розподілу електроенергії; керування центрифугами збагачення урану.

2) розподілені системи керування (Distributed Control Systems, DCS) використовуються для керування виробничими об'єктами одного географічного місця в таких галузях промисловості, як нафтопереробні заводи, очищення води та стічних вод, електростанції, хімічні заводи та фармацевтичні підприємства. DCS використовує централізований контур диспетчерського керування групою локалізованих контролерів, які спільно виконують загальні завдання щодо виконання всього виробничого процесу.

3) системи диспетчерського контролю та збору даних (Supervisory Control and Data Acquisition systems, SCADA)

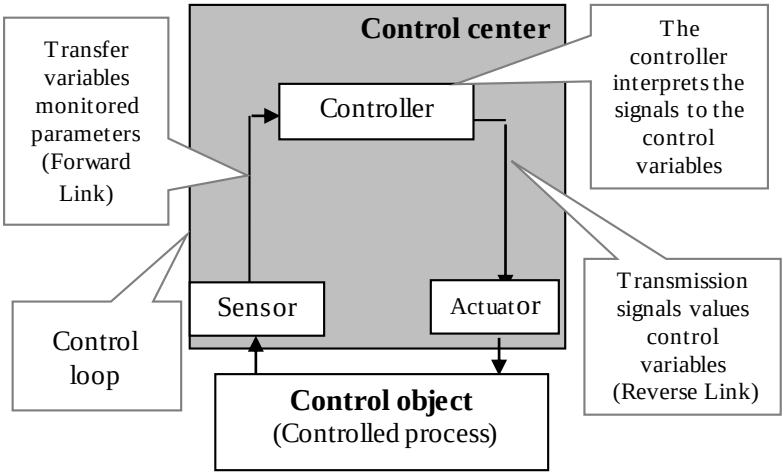
зазвичай використовуються для керування великими, територіально розподіленими промисловими об'єктами. Наприклад, комунальна компанія може використовувати DCS для виробництва електроенергії та систему SCADA для її розподілу. Інші приклади: системи розподілу води; системи збору каналізації; магістральні нафто- та газогони; системи передачі та розподілу електроенергії; системи залізничного та іншого громадського транспорту.

Системи керування на основі PLC можуть використовуватися окремо (керування окремими пристроями, процесами та інше), або у складі більш масштабних систем DCS та SCADA. В свою чергу, DCS також може бути складовою компонентною (частиною) SCADA. Різні комбінації менш масштабних систем дозволяють складати ієрархічні системи керування необхідної конфігурації. Наприклад, SCADA, що керує магістральним газогоном, має у своєму складі декілька DCS для керування окремими газонапірними станціями. В свою чергу, PLC можуть застосовуватися для керування окремими вентильними пристроями, що регулюють рівень тиску.

Далі більш детального розуміння роботи ICS розглянемо принципи керування та типові технічні структури цих систем.

8.2. Принципи керування промисловими об'єктами за допомогою ICS.

Процеси керування різного рівня складності, що застосовують різні види ICS, можуть бути реалізовані шляхом комбінування декількох циклічно повторюваних базових процесів. Сутність цих циклів представлена у вигляді структури кібернетичної (керованої) системи на малюнку 8.1.

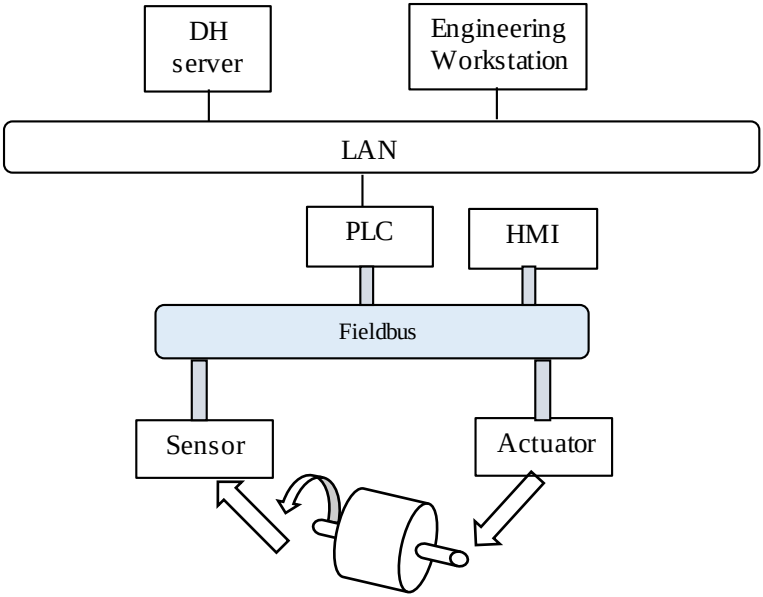


Мал.8.1. Модель базових процесів кібернетичної (керованої) системи

Кібернетична система складається з центру керування (control center, або - суб'єкт керування) та об'єкту керування (control object). Сенсор (sensor) суб'єкту керування формує сигнали, які передають значення контрольованих параметрів об'єкту керування лініями прямого зв'язку (Forward Link) до контролеру. Останній інтерпретує сигнали в керуючі команди, які передаються лініями зворотного зв'язку до актуаторів (виконуючих пристроїв). Останні впроваджують команди шляхом формування відповідних впливів на об'єкт керування. Ці впливи змінюють його стан. Зазначена послідовність дій в рамках кібернетичної системи має назву цикл керування (петля керування, control loop). Далі розглянемо особливості технічної реалізації різних класів ICS на основі застосування сучасних інформаційних технологій.

8.3. Топологія системи керування на основі PLC

Топологія системи керування на основі PLC представлена на малюнку 8.2.



Мал. 8.2. Система керування на основі PLC.

Основою системи є промислова мережа (промислова шина, Fieldbus), що поєднує PLC, диспетчерську машину (human-machine interface, HMI), датчики (сенсори), актуатори (виконавчі пристрої) для реалізації процесів циклу керування об'єктом (на малюнку – електродвигун). Інший порт PLC підключений до локальної мережі (LAN), що також поєднує архівний сервер (data history server, DH server) та інженерні комп'ютери (Engineering Workstation).

Fieldbus (польова шина, промислова мережа) — це цифрова, двонаправлена, багато точкова, послідовна комунікаційна мережа, що зв'язує територіально розподілені датчики, виконавчі механізми, контролери і використовується в промисловій автоматизації для побудови єдиного інформаційного і керуючого середовища, котре об'єднує інтелектуальні технологічні пристрої і контролери

цехового рівня. Описується стандартом IEC 61158. Fieldbus може бути реалізований різними протоколами обміну даними на основі різних середовищ передачі електромагнітного сигналу (електричного, радіо, оптичного).

Широке розповсюдження отримав Industrial Ethernet (промисловий Ethernet) - стандартизований варіант мережевого протоколу Ethernet, адаптованого з метою застосування у промислових умовах для автоматизації та керування технологічними процесами.

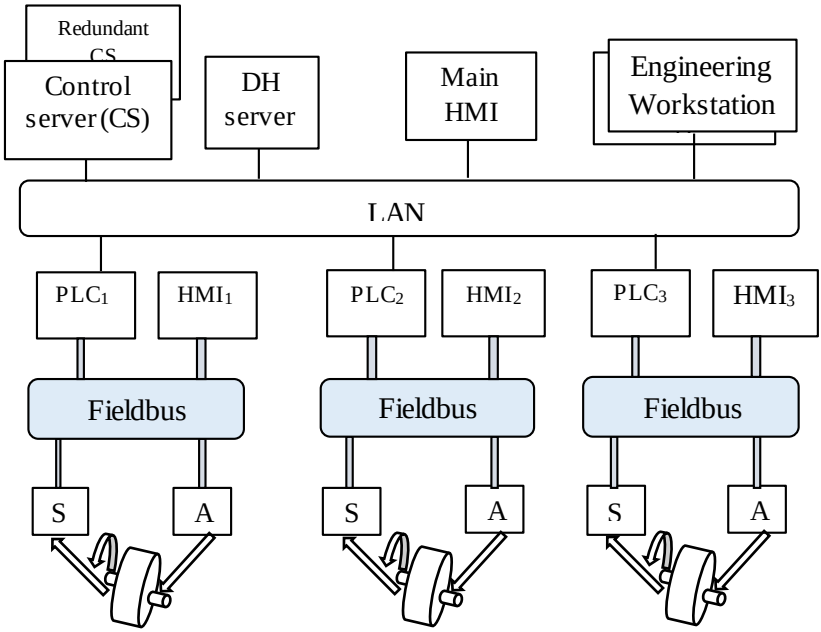
У залежності від вимог, що ставляться до мережі Industrial Ethernet, для передачі даних можуть використовуватися різні види каналів зв'язку:

a) канали зв'язку на основі витих пар. FC TP (Fast Connect twisted pair — вита пара для швидкого монтажу) — варіант організації каналів зв'язку для офісних застосувань, розширюваний на застосування в промислових умовах. Підключення до мережевих версій сайту може здійснюватися через роз'єм RJ45. Завдяки спеціальному виконання кабелю (FC) тривалість монтажу ліній зв'язку може бути істотно скорочено;
b) канали зв'язку на основі промислових витих пар. Промислові виті пари (ITP — Industrial Twisted Pair) дозволяють створювати електричні канали зв'язку з підключенням через з'єднувачі D-типу. Довжина лінії зв'язку може досягати 100 м;
c) оптичні канали зв'язку. Є оптимальним рішенням для побудови резервованих кільцевих топології мережі. Такі канали зв'язку виконуються оптоволоконним кабелем. Оптичні канали зв'язку не зазнають впливу електромагнітних полів і не вимагають використання додаткової ізоляції;
d) бездротові канали зв'язку. Використовуються для побудови локальних обчислювальних мереж, що працюють в частотному діапазоні 2.4 ГГц. Компоненти бездротових мереж відповідають вимогам стандарту IEEE 802.11b. Доступ через бездротові канали до локальної мережі Industrial Ethernet здійснюється через модулі RLM (Radio Link Module).

е) комбіновані системи. При необхідності в рамках однієї мережі Industrial Ethernet можуть використовуватися різні види каналів зв'язку. Узгодження різних видів каналів зв'язку між собою, що працюють з різними швидкостями передачі забезпечують Industrial Ethernet Switches та медіаконвертери.

8.4. Топологія системи керування на основі DCS

Топологія системи керування на основі DCS представлена на малюнку 8.3.



Мал. 8.3. Система керування на основі DCS

Всю DCS, що надана на малюнку, можливо представити двома рівнями керування:

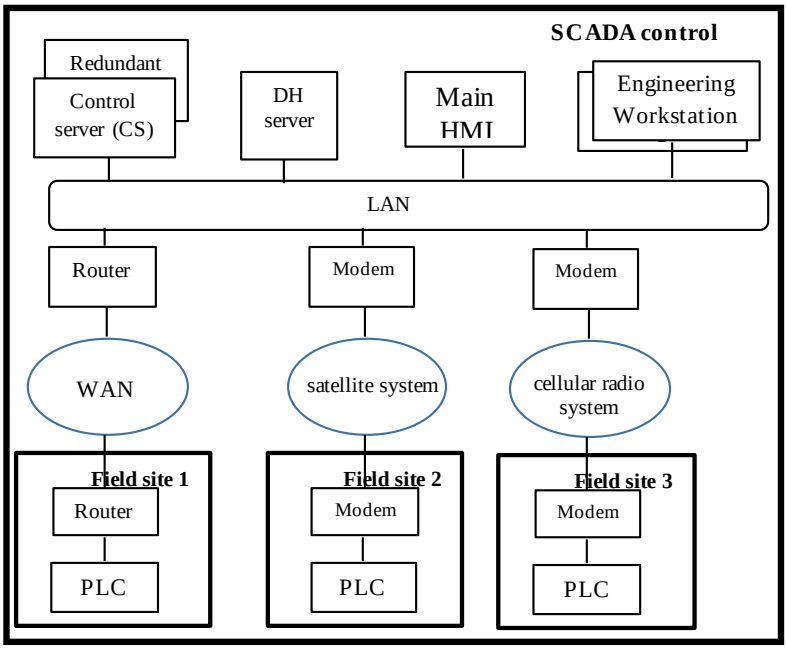
1) рівень супервізора. Поєднує за допомогою LAN головну диспетчерську машину (Main HMI), основний та резервний сервери керування (Control server, Redundant CS), архівний сервер (DH server) та інженерні комп'ютери (Engineering Workstation).

Цей рівень забезпечує комплексне керування всіма розподіленими промисловими об'єктами нижнього виробничого рівня;

2) рівень PLC (виробничий рівень). Складається з систем керування(на основі PLC. Забезпечує автоматичне або автоматизоване керування окремими промисловими об'єктами (компонентами виробничого процесу), прийом та виконання команд рівня супервізора.

8.5. Топологія системи керування на основі SCADA

Топологія системи керування на основі SCADA представлена на малюнку 8.4.



Мал. 8.4. Система керування на основі SCADA

Цю SCADA, що надана на малюнку, можливо представити двома рівнями керування:

1) рівень супервізора. Поєднує за допомогою LAN головну диспетчерську машину (Main HMI), основний та резервний сервери керування (Control server, Redundant CS), архівний

сервер (DH server) та інженерні комп'ютери (Engineering Workstation). За допомогою LAN також приєднуються маршрутизатори та модеми, що забезпечують обмін даними з польовими зонами (field site**)** через системи зв'язку. Цей рівень забезпечує комплексне керування всіма розподіленими промисловими об'єктами нижнього рівня польових зон;

2) рівень систем зв'язку. Забезпечує обмін даними між центром керування та пристроями керування промисловими об'єктами польових зон, що розташовані на великих відстанях. Для передачі сигналів керування використовуються різні технології корпоративного зв'язку або зв'язку загального користування (Internet, супутниковий зв'язок, мобільний стільниковий радіозв'язок та інші);
3) рівень польових зон. Складається з систем керування на основі PLC, DCS. Забезпечує автоматичне або автоматизоване керування віддаленими промисловими об'єктами (компонентами виробничого процесу), прийом та виконання команд рівня супервізора.

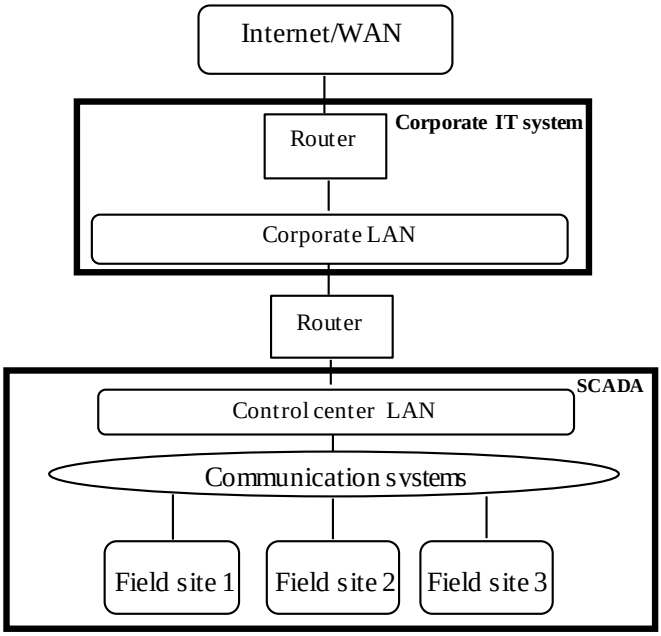
8.6. Особливості об'єктів критичної інформаційної інфраструктури з ICS

Як правило, більшість об'єктів критичної інформаційної інфраструктури промислової галузі можливо поділити на дві компоненти:

1) інформаційна система (система інформаційних технологій IT system, ITS);
2) індустріальна система керування (ICS).

Комп'ютерні засоби корпоративної інформаційної системи поєднуються за допомогою локальної мережі LAN та підтримують фінансове, кадрове, логістичне, юридичне, адміністративне та інше забезпечення підприємства. ICS призначено тільки для керування промисловими об'єктами. Між ICS та ITS існує фізичний зв'язок, який контролюється спеціальними

комп'ютерними засобами (фаєрволи, шлюзи). Типова структура ОКІІ, що має ICS на основі SCADA, представлена на малюнку 8.5. Комп'ютерні засоби корпоративної інформаційної системи (Corporate IT system), що об'єднані корпоративною LAN, за допомогою маршрутизатора периметру (Router) можуть мати доступ до зовнішніх інформаційних ресурсів Інтернет (глобальних мереж WAN). У разі необхідності корпоративна мережа має можливість обмінюватися даними з локальною мережею центру керування SCADA за допомогою іншого маршрутизатору.



Мал. 8.5. Інформаційна інфраструктура ОКІ з ICS на основі SCADA

Порядок забезпечення кіберзахисту таких інформаційних інфраструктур буде розглянуто далі.

Висновки за розділом 8:

- Індустріальні (промислові) системи керування ((Industrial Control System, ICS) — це інформаційні системи, які використовуються в індустріальних галузях керування технологічними процесами різних промислових об'єктів.
- В україномовному нормативному просторі замість терміну ICS часто використовують терміни: автоматизована система управління технологічними процесами (АСУ ТП); операційна технологія (ОТ).
- ICS збирають результати вимірювання датчиків (сенсорів) контролю поточного стану об'єкту керування, обробляють і відображають цю інформацію, а також передають команди керування локальному або віддаленому обладнанню виконавчих пристроїв (актуаторів).
- Існує три основних класи систем управління:
  - програмовані логічні контролери (Programmable Logic Controllers, PLC) - комп'ютерні пристрої для керування окремим промисловим обладнанням;
  - розподілені системи керування (Distributed Control Systems, DCS) - для керування виробничими об'єктами одного географічного місця;
  - системи диспетчерського контролю та збору даних (Supervisory Control and Data Acquisition systems, SCADA) - для керування територіально розподіленими промисловими об'єктами.
- Топологія ICS на PLC: основою системи - промислова мережа (промислова шина, Fieldbus), що поєднує PLC, диспетчерську машину (human-machine interface, HMI), датчики (сенсори), актуатори (виконавчі пристрої) для реалізації процесів циклу керування об'єктом.
- Fieldbus (польова шина, промислова мережа) — це цифрова, двонаправлена, багато точкова послідовна комунікаційна мережа, що зв'язує територіально розподілені датчики, виконавчі механізми, контролери і

використовується в промисловій автоматизації для побудови єдиного інформаційного і керуючого середовища, котре об'єднує інтелектуальні технологічні пристрої і контролери цехового рівня. Описується стандартом IEC 61158.

- Fieldbus може бути реалізований різними протоколами обміну даними на основі різних середовищ передачі електромагнітного сигналу (електричного, радіо, оптичного).
- Industrial Ethernet (промисловий Ethernet) - стандартизований варіант мережевого протоколу Ethernet, адаптованого з метою застосування у промислових умовах для автоматизації та керування технологічними процесами.
- Топологія ICS на основі DCS складається з двох рівнів:
  1) рівень супервізора: LAN поєднує головну диспетчерську машину (Main HMI), основний та резервний сервери керування (Control server, Redundant CS), архівний сервер (DH server) та інженерні комп'ютери (Engineering Workstation);
  2) рівень PLC (виробничий рівень).
- Топологія ICS на SCADA:

  1) рівень супервізора (LAN, Main HMI, Control server, Redundant CS, Engineering Workstations, архівний DH server);

  2) рівень систем зв'язку - обмін даними між центром керування та пристроями 3 рівня;

  3) рівень польових зон – сукупність систем керування на основі PLC, DCS. Забезпечує керування віддаленими промисловими об'єктами

Контрольні питання та завдання

1. Призначення ICS?
2. Класифікація ICS?
3. Призначення PLC?
4. Призначення DCS?

5. Призначення SCADA?
6. Різниця між DCS та SCADA?
7. Топологія ICS на основі DCS?
8. Топологія ICS на основі PLC?
9. Топологія ICS на основі SCADA?
10. Призначення DH сервера?
11. Призначення Redundant CS сервера?
12. Призначення Fieldbus?
13. Визначте послідовність циклу процесів, що складають *control loop* кібернетичної (керованої) системи.

9. КІБЕРЗАХИСТ ІНДУСТРІАЛЬНИХ СИСТЕМ КЕРУВАННЯ

- **інтеграція ICS та ITS**
- **особливості ICS та основні цілі захисту**
- **стратегія "захисту в глибину" ("Defense-in-Depth")**

В цьому розділі буде розглянуто базові підходи щодо організації кіберзахисту індустріальних систем керування (Industrial Control Systems, ICS).

9.1. Інтеграція ICS та ITS

Від початку появи ICS мало нагадували традиційні системи інформаційних технологій (ITS), оскільки ICS були ізольованими системами та застосовували власні протоколи керування з використанням спеціалізованого обладнання та програмного забезпечення. Поступове впровадження широкодоступних недорогих комп'ютерних технологій TCP/IP замість спеціалізованих рішень значно збільшує ймовірність кіберзагроз інформаційної інфраструктурі ICS. Таке рішення супроводжується впровадженням стандартних комп'ютерів, операційних систем і мережевих протоколів, що робить ICS подібними до ITS. Додатковим джерелом збільшення рівня кіберзагроз є рішення щодо підключення ICS до корпоративних інформаційних систем (ITS) для забезпечення віддаленого доступу. Ця інтеграція підтримує нові IT-можливості, але забезпечує значно меншу ізоляцію ICS від зовнішнього світу, створюючи більшу потребу в захисті. Хоча існує багато рішень щодо подолання проблем безпеки в типових ITS, необхідно вживати особливих запобіжних заходів під час впровадження цих самих рішень у середовища ICS. У деяких випадках потрібні особливі рішення безпеки, що адаптовані до середовища ICS.

9.2. Особливості ICS та основні цілі захисту

Хоча деякі характеристики між ITS та ICS подібні, останні також мають характеристики, які відрізняються від традиційних систем обробки інформації. Багато з цих відмінностей пов'язані з тим фактом, що виконання обчислювальних процесів в ICS безпосередньо впливає на фізичний світ. Деякі з цих характеристик пов'язані зі значним ризиком для здоров'я та безпеки життя людей, з серйозною шкодою навколишньому середовищу, а також серйозно впливають на фінансові проблеми, такі як втрати виробництва, негативний вплив на економіку країни та компрометацію конфіденційної інформації. ICS мають унікальні вимоги до продуктивності та надійності, і часто використовують операційні системи та програми, які можуть вважатися нетрадиційними для типового IT-персоналу. Крім того, цілі безпеки та ефективності іноді суперечать безпеці при проектуванні та експлуатації систем керування.

Спочатку реалізації ICS були сприйнятливі насамперед до локальних загроз, оскільки багато їхніх компонентів перебували у фізично захищених зонах і ці компоненти не були підключені до IT-мереж або систем. Однак тенденція до інтеграції з IT-мережами супроводжується зменшенням ізоляції ICS від зовнішнього світу. Це веде до зростання віддалених зовнішніх кіберзагроз. Крім того, збільшення обсягів використання бездротових мереж в інфраструктурі ICS значно збільшує ризики загроз з боку зловмисників, які знаходяться у фізичній близькості, але не мають прямого фізичного доступу до обладнання. Загрози системам управління можуть надходити з багатьох джерел, включаючи ворожі уряди, терористичні групи, незадоволених співробітників, зловмисників, складні ситуації, аварії, стихійні лиха, а також зловмисні або випадкові дії інсайдерів. Цілі безпеки ICS відповідають такому порядку пріоритетності в забезпеченні властивостей інформації:

доступність (Д), цілісність (Ц) та конфіденційність (К). Для ITS забезпечується інший порядок: К, Ц, Д.

Найбільш критичні події (інциденти) ICS, що впливають на безпеку промислового ОКІ, включають наступні:

- заблокований або затриманий потік інформації через мережі, що може порушити роботу ICS (порушення доступності інформації обміну);
- несанкціоновані зміни інструкцій, команд або порогових значень технологічних процесів, які можуть пошкодити, вивести з ладу або вимкнути обладнання, створити вплив на навколишнє середовище та/або поставити під загрозу життя людини (порушення цілісності інформації від сенсорів та/або інформації від центру керування до актуаторів);
- неточна інформація, надіслана системним операторам, щоб приховати несанкціоновані зміни або змусити операторів ініціювати неналежні дії, які можуть мати різні негативні наслідки (порушення цілісності інформації від сенсорів до контролерів/операторів);
- програмне забезпечення ICS чи параметри конфігурації несанкціоновано змінені, або програмне забезпечення ICS заражене шкідливим програмним забезпеченням. Це веде до різних негативних наслідків (порушення цілісності програмного забезпечення контролерів/центрів керування);
- втручання в роботу систем безпеки, що може загрожувати життю людини (порушення доступності та цілісності системи керування).

Основні цілі безпеки для ICS та заходи захисту:

1) обмеження логічного доступу до мережі ІКС та мережевої активності.

Забезпечується шляхом використання:

- односпрямованих шлюзів;
- мережевої архітектури демілітаризованої зони (DMZ) із фаєрволами (FW) для запобігання прямого проходження

мережевого трафіка між корпоративною мережею ITS та мережами ICS;

- окремих механізмів автентифікації та облікових даних для користувачів корпоративної мережі ITS та мереж ICS;
- мережевої топології, яка має кілька рівнів, при цьому найважливіші комунікації відбуваються на найбільш безпечному та надійному рівні;
- заходів та засобів сегментації мережевого простору

2) обмеження фізичного доступу до мережі та пристроїв ІКС.

Забезпечується заходами та засобами захисту від несанкціонованого доступу до фізичного середовища та компонентів ICS:

- механічні та електронно-механічні замки;
- системи охорони (охоронці, огородження, охоронна сигналізація);
- системи автентифікації персоналу по електронним/біометричним параметрам.

3) захист комп'ютерних засобів від інформаційного несанкціонованого доступу.

Забезпечується наступними заходами:

- своєчасне оновлення програмного забезпечення патчами безпеки після їх тестування в польових умовах;
- відключення всіх портів і служб, які не використовуються, гарантоване забезпечення їх відключеного стану;
- обмеження привілеїв користувачів ICS лише тими, які необхідні для ролі кожної особи;
- відстеження та моніторинг журналів аудиту на наявність інцидентів безпеки;
- використання засобів контролю безпеки, таких як антивірусне програмне забезпечення та програмне забезпечення для перевірки цілісності даних та комп'ютерного обладнання, запобігання, виявлення та пом'якшення зловмисного програмного забезпечення;

4) обмеження дій щодо несанкціонованої зміни даних.

Заходи та засоби захисту:

- використання механізмів криптозахисту для автентифікації повідомлень, відправників та отримувачів повідомлень;
- використання механізмів криптозахисту для забезпечення цілісності файлів, що зберігаються.

5) виявлення подій безпеки та формування своєчасної відповіді, що розриває ланцюг атак до того, як зловмисники досягнуть своїх цілей.

Забезпечується використанням інфраструктури кіберзахисту (IDS/IPS, SOC, SIEM, CTI), що забезпечує реалізацію процесів циклу керування кібербезпекою;

6) збереження працездатності ICS в несприятливих умовах. Передбачає проектування ICS таким чином, щоб кожен критичний компонент мав надлишковий аналог (резервування). Крім того, якщо компонент виходить з ладу, він повинен виходити з ладу таким чином, щоб не генерувати непотрібний трафік у ICS чи інших мережах або не викликати іншу проблему деінде, наприклад каскадну подію. ICS також має дозволити плавну деградацію, наприклад перехід від «нормальної роботи» з повною автоматизацією до «аварійної» з більшою залученістю операторів і меншою автоматизацією до «ручної роботи» без автоматизації.

7) відновлення системи після інциденту.

Інциденти безпеки неминучі, план реагування на них важливий. Основною характеристикою хорошої програми безпеки є те, наскільки швидко можна відновити систему після інциденту.

9.3. Стратегія “захисту в глибину” (“Defense-in-Depth”).

Для досягнення цілей захисту ICS часто використовується стратегія “захисту в глибину” (англ. - “Defense-in-Depth”, далі

– Стратегія DD). Стратегія DD [29] представляє процес захисту як сукупність заходів захисту, що узгоджені між собою за:

- просторами функціонування ICS;
- рівнями кібератаки (етапами дій зловмисника в комп'ютерної системи ICS);
- рівнями захисту (етапами дій захисників).

Ціллю узгодження заходів захисту за просторами та рівнями ICS, як правило, є встановлення такого набору заходів, що формують декілька бар'єрів протидії зловмиснику в рамках одного вектору кібератаки, або набору векторів кібератаки. Під "вектором кібератаки" будемо розуміти сукупність дій зловмисника по досягненню визначеної мети кібератаки. Наприклад, якщо ціллю атаки є отримання зловмисником дистанційного керування диспетчерською машиною ICS, то для цього може бути обрано декілька векторів атаки (послідовностей дій). В цьому випадку заходи захисту будуть узгодженими відносно мети атаки, якщо вони будуть протидіяти реалізації дій зловмисника в рамках вектору (набору векторів) атаки.

Для розуміння сутності Стратегії DD важливо відрізняти поняття "простір" та "рівень" ICS . Простір (середовище) пов'язують з діяльністю в рамках одної складової ICS. Так як ICS, є різновидом інформаційної системи, то найбільш часто розглядають наступні види просторів:

- організаційний (адміністративний) простір, де функціонує персонал ІС для забезпечення технології обробки інформації;
- комп'ютерний (технологічний) простір, де за допомогою комп'ютерних засобів реалізується технологія обробки цифрової інформації (даних);
- фізичний простір – це споруди, приміщення, окремі зони, де знаходяться персонал та засоби комп'ютерної системи, що забезпечують реалізацію технології обробки інформації.

Поняття "рівень" ICS, як правило, пов'язують з етапами кібератаки та етапами захисту від ней. Для формалізації

(уточнення деталей) кібератаки часто використовують модель "Cyber Kill Chain" (Ланцюжок кіберзнищення), який представляє набір дій з підготовки та реалізації атаки на конкретний ресурс інформаційної системи у вигляді послідовності етапів (тактик). Кожний етап характеризується проміжною (тактичною) ціллю в рамках атаки та описом відповідних заходів і засобів її реалізації (технік і процедур). Більш детально ця модель буде розглянута в розділі 13.

Для формалізації рівній захисту останнім часом часто застосовується модель, яка розглядає систему заходів кіберзахисту у вигляді послідовності етапів циклу керування кібербезпекою (мал. 7.1.). В свою чергу, опис заходів захисту деталізується за допомогою ієрархічної структури рівній заходів: класи, категорії та підкатегорії (мал. 7.2.).

Застосування Стратегії DD дозволяє поєднувати різні складні аспекти організації та удосконалення захисту ICS шляхом застосування набору інструментів формалізації (подолання невизначеностей) опису ситуації. Принципи застосування Стратегії DD можуть бути пояснені наступним прикладом:

1) **організаційний простір**:

- в рамках сформованої політики безпеки ICS диспетчерська машина (ДМ) визначається критичним ресурсом, для захисту якого потрібно впровадити заходи захисту від несанкціонованого доступу (НСД);
- в рамках цієї же політики уточняються сутності необхідних заходів захисту від НСД шляхом визначення та загального опису відповідних процедур:

a) процедура ідентифікації, автентифікації та авторизації. Доступ до ДМ службової інформації надається тільки ідентифікованим та автентифікованим користувачам на основі визначених правил розподілу доступом;

b) процедура блокування НСД доступу. Спроби доступу до ДМ користувачами, які не мають на це повноважень,

неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися;

c) процедура реєстрації подій безпеки. Під час забезпечення доступу до ДМ у системі повинна здійснюватися обов'язкова реєстрація:

результатів ідентифікації та автентифікації користувачів;

результатів виконання користувачем операцій з обробки інформації;

спроб несанкціонованих дій;

фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

результатів перевірки цілісності засобів захисту інформації.

d) процедура сегментації ICS. З метою ускладнення НСД доступу до ДМ забезпечується сегментація комп'ютерного та фізичного простору.

2) **комп'ютерний простір**. Відповідно до правил та процедур Політики безпеки впроваджуються наступні технічні механізми:

- сервіс електронного каталогу Active Directory для сегментації мережі та керування доступом до ДМ;
- фаєрволи (FW), VLAN та демілітаризовані зони (DMZ) для сегментації мережі та керування доступом до ДМ;
- впроваджується система управління доступом між сегментами на основі ролевих політик;
- засоби IDS та SIEM для реєстрації та аналізу подій НСД до ДМ;

3) **фізичний простір**. Відповідно до правил та процедур Політики безпеки впроваджуються наступні механізми захисту від НСД фізичного доступу до ДМ:

- всі приміщення центру керування представляють окремі сегменти, доступ до яких має персонал відповідно до розподілу функціональних обов'язків;

- доступ до кожного сегменту тільки на основі персональних електронних карток;
- в приміщення кожного сегменту впроваджується система охоронної сигналізації;
- для протидії атакам спеціального впливу сегменти з серверним обладнанням додатково забезпечуються системою об'єктового екранування;

4) **рівень кіберзагроз (атак).** Для визначення загроз структурі інтегрованої системі ITS+ICS з заходами захисту в трьох просторах (вищезазначені пункти 1, 2, 3) застосовується модель "Cyber Kill Chain" для опису атаки. В рамках кожної тактики (етапу) цієї моделі визначається перелік можливих загроз;

5) **рівень заходів кіберзахисту.** Після оцінювання ризиків загроз з раніше визначеного переліку необхідний набір заходів кіберзахисту. Ці заходи можливо визначити зі спеціалізованого документу "Методичні рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами" [28]. Цей документ по аналогії з [15] (розглядалось у розділі 7) надає класифікацію (таксономію) заходів кіберзахисту для ICS. Конкретні заходи захисту визначаються відповідності до пріоритетності кіберзагроз та формується поточний профіль кіберзахисту.

В рамках Стратегії DD можуть використовуватися люби інші моделі атак та кіберзахисту.

Висновки за розділом 9:

- Поступове впровадження широкодоступних недорогих комп'ютерних технологій TCP/IP замість спеціалізованих рішень значно збільшує ймовірність кіберзагроз інформаційної інфраструктурі ICS.
- Додатковим джерелом збільшення рівня кіберзагроз є підключення ICS до корпоративних інформаційних систем (ITS).

- У деяких випадках потрібні особливі рішення безпеки, що адаптовані до середовища ICS та відрізняються від рішень для ITS.
- Особливість ICS - обчислювальні процесів безпосередньо впливають на фізичний світ. Це пов'язано зі значним ризиком для здоров'я та безпеки життя людей, з серйозною шкодою навколишньому середовищу, а також серйозно впливають на фінансові проблеми,
- ICS мають унікальні вимоги до продуктивності та надійності, і часто використовують операційні системи та програми, які можуть вважатися нетрадиційними для типового IT-персоналу.
- Тенденція до інтеграції ICS зі звичайними IT-мережами супроводжується зменшенням ізоляції ICS від зовнішнього світу. Це веде до зростання віддалених зовнішніх кіберзагроз.
- Цілі безпеки ICS визнають наступну пріоритетність в забезпеченні властивостей інформації: Д, Ц та К. Для звичайних ITS - інший порядок: К, Ц, Д.
- Основні цілі безпеки ICS та заходи захисту:

1) обмеження логічного доступу до мережі ICS.

Заходи та засоби захисту:

- односпрямовані шлюзи;
- DMZ із фаєрволами для запобігання прямому трафіку між корпоративною ITS та ICS;
- окремі механізми автентифікації для ITS та ICS;
- багаторівнева ієрархічна топологія - найважливіші комунікації на найбільш безпечному та надійному рівні;
- заходи та засоби сегментації мережевого простору;

2) обмеження фізичного доступу до мережі та пристроїв ІКС.

Заходи та засоби захисту:

- механічні та електронно-механічні замки;

- системи охорони (охоронці, огородження, охоронна сигналізація);
- системи автентифікації персоналу по електронним/біометричним параметрам.

3) захист комп'ютерних засобів від інформаційного НСД.

Заходи та засоби захисту:

- своєчасне оновлення ПЗ після тестування в польових умовах;
- відключення всіх портів і служб, які не використовуються, гарантоване забезпечення їх відключеного стану;
- обмеження привілеїв користувачів ICS лише тими, які необхідні для ролі кожної особи;
- відстеження та моніторинг журналів аудиту на наявність інцидентів безпеки;
- використання засобів контролю безпеки: антивірусне ПЗ та ПЗ для цілісності даних та комп'ютерного обладнання; обмеження дій несанкціонованої зміни даних.

4) обмеження дій щодо несанкціонованої зміни даних.

Заходи та засоби захисту:

- криптозахист автентифікації повідомлень, відправників та отримувачів повідомлень;
- криптозахист даних від сенсорів.

5) виявлення подій безпеки та формування своєчасної відповіді на розрив ланцюга атаки.

Заходи та засоби захисту:

- інфраструктура кіберзахисту (IDS/IPS, SOC, SIEM, CTI), що забезпечує реалізацію процесів циклу керування кібербезпекою;

6) збереження роботоздатності ICS в несприятливих умовах.

Заходи та засоби захисту:

- ефективне проектування заходів резервування;
- можливість переходу до ручного керування;
- обмеження генерації надлишкового трафіку;
- план реагування критичні події.

- Стратегія “захисту в глибину” (від англ. - “Defense-in-Depth”) - сукупність заходів захисту, що узгоджені між собою за:
- просторами функціонування ICS;
- рівнями кібератаки (етапами дій зловмисника);
- рівнями захисту (етапами дій захисників).
- “Методичні рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами” – документ, що надає класифікацію (таксономію) заходів кіберзахисту для ICS.

Контрольні питання та завдання

1. Особливості ICS відносно ITS?
2. Пріоритетність в забезпеченні властивостей інформації ICS?
3. Основні цілі безпеки ICS?
4. Заходи та засоби захисту для обмеження логічного доступу до ресурсів ICS?
5. Заходи та засоби захисту для обмеження фізичного доступу до мережі та пристроїв ІКС?
6. Заходи та засоби захисту від інформаційного НСД?
7. Заходи та засоби захисту від НСД щодо цілісності даних автентифікації?
8. Заходи та засоби спостереження за подіями безпеки та своєчасного реагування?
9. Заходи та засоби забезпечення роботоздатності ICS в несприятливих умовах?
10. Визначте додаткові моделі для застосування в рамках стратегія “Defense-in-Depth”.
11. Визначте конкретні комп’ютерні засоби для розмежування доступу до ICS з мережі корпоративної ITS.

10. НАЦІОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ

- **правові та організаційні основи**
- **об'єкти та суб'єкти кіберзахисту**
- **визначення НСКБ та основні складові**
- **модель НСКБ**

В цьому розділі розглядаються призначення, основні компоненти та принципи організації національної системи кібербезпеки України. Ця система дозволяє скоординувати діяльність всіх суб'єктів захисту національного сегменту кіберпростору.

10.1. Правові та організаційні основи забезпечення кібербезпеки.

Правову основу створення та функціонування національної системи кібербезпеки України (далі – НСКБ) становлять:

- Конституція України,
- закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом;
- закон України "Про основні засади забезпечення кібербезпеки України";
- міжнародна Конвенція про кіберзлочинність інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України,
- укази Президента України,
- акти Кабінету Міністрів України,
- інші нормативно-правові акти, що приймаються на виконання законів України.

Закон України «Про основні засади забезпечення кібербезпеки України» (далі – Закон) визначає:

- правові та організаційні основи забезпечення захисту життєва 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 їх діяльності із забезпечення кібербезпеки.

10.2. Об'єкти та суб'єкти кіберзахисту

Закон визначає, що *об'єктами кіберзахисту* є:

1) комунікаційні системи (інформаційні, комунікаційні, інформаційно-комунікаційні системи) всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури (ОКІІ);

3) комунікаційні системи (інформаційні, комунікаційні, інформаційно-комунікаційні системи), які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах:

- електронного урядування,
- електронних державних послуг,
- електронної комерції,
- електронного документообігу.

Також Закон визначає суб'єкти кіберзахисту та порядок їх координації:

а) координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється *Президентом України* через очолювану ним *Раду національної безпеки і оборони України.*

б) *Національний координаційний центр кібербезпеки* (НКЦКБ) як робочий орган Ради національної безпеки і оборони України:

- здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку,

- вносить Президентові України пропозиції щодо формування та уточнення *Стратегії кібербезпеки України.*

в) *Кабінет Міністрів України* забезпечує:

- формування та реалізацію державної політики у сфері кібербезпеки,

- захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі,

- боротьбу з кіберзлочинністю;

-організовує та забезпечує необхідними силами, засобами і ресурсами функціонування *національної системи кібербезпеки*;

- формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на *об'єктах критичної інфраструктур*и (крім об'єктів критичної інфраструктури у банківській системі України).

Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними

інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

10.3. Визначення національної системи кібербезпеки та її основні складові.

Національна система кібербезпеки (НСКБ) 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 (ДССЗЗІ),
- Національна поліція України,
- Служба безпеки України,
- Міністерство оборони України та Генеральний штаб Збройних Сил України,
- розвідувальні органи,
- Національний банк України.

Закон визначає основні завдання Державної служби 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, активної протидії агресії у кіберпросторі, 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;

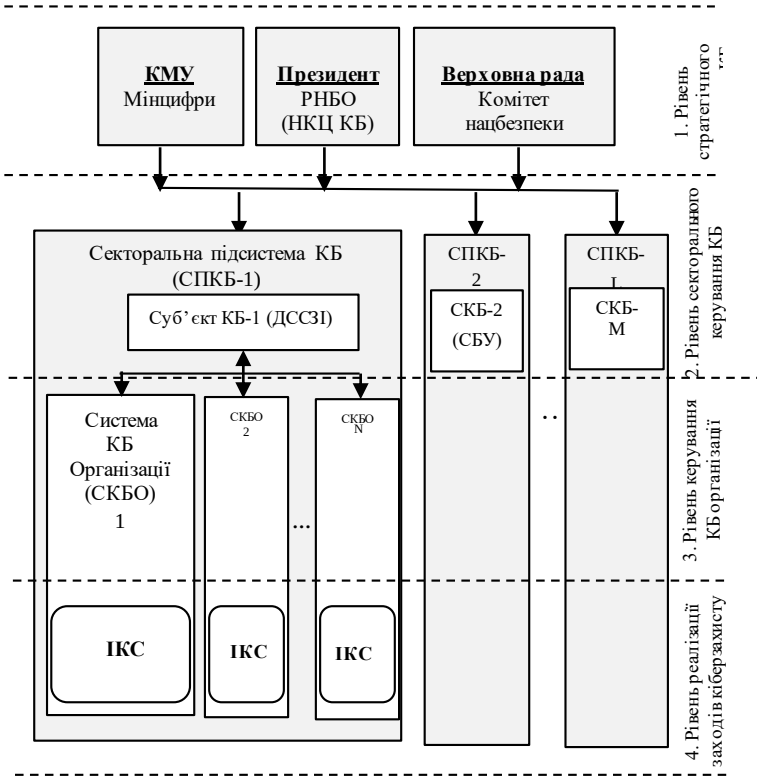
- забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

- забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Закон також впроваджує поняття *Національний центр резервування державних інформаційних ресурсів*, що представляє собою організовану сукупність об'єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій.

10.4. Модель національної система кібербезпеки

З точку зору системного підходу НСКБ представляє собою складну організаційно-технічну систему, властивості якої слабоформалізовані. За допомогою засобів графічної формалізації можливо сформувати відповідну ієрархічну модель (мал. 10.1), що уточнює склад системи та характер зв'язків між її компонентами. В рамках цієї моделі НСКБ



Мал. 10.1. Ієрархічна модель національної системи кібербезпеки (НСКБ)

представлена в вигляді кібернетичної системи, процеси керування якої забезпечують стан безпеки національного кіберсегменту. Цей сегмент представляє собою сукупність всіх національних інформаційно-комунікаційних систем (тобто, національний кіберсегмент, представлений на рівні 4) та є об'єктом керування в рамках НСКБ.

Кожна ІКС національного кіберсегменту є об'єктом кіберзахисту. Всі процеси керування станом кібербезпеки ІКС формуються та реалізуються суб'єктами кіберзахисту, що організовані в рамках трирівневої ієрархії. Особливість організації ієрархії в тому, що функції збору інформації про стан кібербезпеки та формування команд щодо впровадження необхідних заходів кіберзахисту кожний рівень НСКБ реалізує за допомогою функцій нижнього рівня. Наприклад, збір інформації про поточний стан безпеки національного кіберсегменту формується на 3 рівні, потім секторально агрегується і аналізується на 2 рівні та остаточно агрегується і аналізується на 1 рівні. Основні характеристики рівнів керування кібербезпекою:

1) *рівень стратегічного керування кібербезпекою* (рівень 1) відповідає за формування та реалізацію державної політики в сфері кібербезпеки. Ця політика декларується в Законах України та Указах Президента України. Порядок реалізації політики визначається в Постановах Кабінету Міністрів України. Координацію діяльності всіх суб'єктів в сфері кіберзахисту на цьому рівні здійснює Президент України через очолювану ним Раду національної безпеки і оборони України (РНБО України). Всю поточну координацію та контроль діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, реалізує Національний координаційний центр кібербезпеки (НКЦ КБ) як робочий орган РНБО України;

2) рівень секторального керування кібербезпекою (рівень 1) через відповідні суб'єкти секторального кіберзахисту

уточнює особливості діяльності, реалізує та контролює виконання державної політики в сфері кібербезпеки. Наприклад, ДССЗЗІ має декілька секторів відповідальності в національному кіберсегменті;

- всі ІКС, де оброблюються державні інформаційні ресурси та інформація, вимога щодо захисту якої встановлена законом;

- всі ІКС, що відносяться до об'єктів критичної інформаційної інфраструктури;

3) рівень керування кібербезпекою організації (рівень 3) через відповідні службу захисту інформації конкретної ІКС уточнює особливості діяльності організації, реалізує та контролює виконання державної політики в сфері кібербезпеки;

4) рівень реалізації заходів кіберзахисту (рівень 4) за допомогою засобів інфраструктури кіберзахисту конкретної ІКС збирається та аналізується інформація про поточні події в комп'ютерному середовищі. В разі виявлення події безпеки за допомогою розробленої політики безпеки інформації для цієї ІКС приймаються та впроваджуються відповідні дії щодо відновлення стану кібербезпеки.

Висновки за розділом 10

- ***Національна система кібербезпеки*** *(НСКБ)* – 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.
- НСКБ відноситься класу складних організаційно-технічних систем, які функціонують за принципами кібернетичних (керованих) систем.

- ***Об'єктом керування*** (об'єктом кіберзахисту) в рамках НСКБ є національний кіберсегменту, що представляє собою сукупність національних інформаційно-комунікаційних систем.
- Закон України "Про основні засади забезпечення кібербезпеки України" визначає наступні ***категорії об'єктів кіберзахисту:***

  1) ІКС (інформаційні, комунікаційні, інформаційно-комунікаційні системи) всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

  2) об'єкти критичної інформаційної інфраструктури;

  3) ІКС, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах:

  - електронного урядування,
  - електронних державних послуг,
  - електронної комерції,
  - електронного документообігу.

15. ***Суб'єктом керування НСКБ*** є ієрархічна сукупність суб'єктів кіберзахисту, що виконує функції підсистеми керування.

16. ***Суб'єктами кіберзахисту стратегічного рівня*** є Верховна Рада України, Президент України та Кабінет Міністрів України.

17. Президент України через РНБО України та Національний координаційний центр кібербезпеки (НКЦ КБ), що є робочим органом в складі РНБО, здійснює ***координацію діяльності всіх суб'єктів кіберзахисту***.

18. ***Суб'єктами кіберзахисту у межах своїх компетенції*** є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;
4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;
5) Збройні Сили України, інші військові формування, утворені відповідно до закону;
6) Національний банк України;
7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;
8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

19. ***Основними суб'єктами*** *національної системи кібербезпеки* є:
- Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ),
- Національна поліція України,
- Служба безпеки України,
- Міністерство оборони України та Генеральний штаб Збройних Сил України,
- розвідувальні органи,
- Національний банк України.

20. ***Державна служба спеціального зв'язку та захисту інформації України***, як основний суб'єкт національної системи кібербезпеки:
- забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, 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 вразливість;
- забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.
21. ***Національний центр резервування державних інформаційних ресурсів*** - сукупність об'єктів для:
- забезпечення надійності та безперебійності роботи державних інформаційних ресурсів;
- кіберзахисту, зберігання національних електронних інформаційних ресурсів;
- резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій.

22. Безпосередні заходи кіберзахисту ІКС впроваджуються за допомогою заходів та засобів ***інфраструктури кіберзахисту***, що дозволяють збирати та аналізувати інформація про поточні події в комп'ютерному середовищі. В разі виявлення події безпеки (інциденту кібербезпеки) за допомогою розробленої політики безпеки інформації для цієї ІКС приймаються та впроваджуються відповідні дії щодо відновлення стану кібербезпеки.

Контрольні питання та завдання

1. Які основні складові Національної системи кібербезпеки (НСКБ)?
2. До якого класу систем відноситься НСКБ?
3. Що є об'єктом керування НСКБ?
4. Категорії об'єктів кіберзахисту?
5. Які державні органи формують державну політику у сфері кібербезпеки?
6. Суб'єкти кіберзахисту в рамках своїх компетенцій?
7. Основні суб'єкти НСКБ?
8. Визначте основні завдання Держспецзв'язку в рамках основного суб'єкту НСКБ.
9. Визначте рівні ієрархії керування в рамках НСКБ.
10. Яким чином забезпечується координація суб'єктів кіберзахисту?
11. Яким чином забезпечується кіберзахист конкретної ІКС?

11. КІБЕРАТАКИ

- **поняття кібератаки**
- **класифікація кібератак**
- **APT атака та проактивна стратегія кіберзахисту**
- **кібернетична модель APT атаки**

Процеси нападу та захисту в кіберпросторі носять скритний, складний та багатоплановий характер, що робить їх слабоформалізованими та важкими до системного розуміння. Для організації ефективної колективної роботи в підрозділах кіберзахисту необхідною умовою стає питання використання фахових понять, що дозволяють подолати можливі семантичні невизначеності на основі послідовної узгодженості між собою базових професійних термінів. Таку узгодженість можливо сформувати на основі використання аксіоматичного підходу, який дуже добре зарекомендував себе в математичної сфері. Його сутність:

- є базові поняття, що сформовані на твердженнях (аксіомах, постулатах);
- всі інші поняття формуються на основі базових;
- забороняється формувати нове поняття на основі використання термінів, що ще не визначені.

Такий підхід дозволяє подолати багато невизначеностей за рахунок того, що не будуть використовуватися таки описи об'єктів в яких термін через ланцюжок інших термінів пояснюється сам через себе ("термінологічне замкнуте коло").

Приклад застосування такого аксіоматичного підходу до визначення термінів "кіберпростір" та "кібербезпека" був наведений в розділі 5. В цьому розділі з цих позицій буде розглянута сутність та зв'язок базових понять "кібервразливість", "кіберзагроза", "кібератака" та "кіберінцидент".

11.1. Поняття кібератаки

Законодавство України [1] застосовує два поняття для позначення дій, які впливають на стан кібербезпеки інформаційно-комунікаційної системи:

1) *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.

2) *інцидент кібербезпеки* (далі - *кіберінцидент*) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) 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;

Якщо проаналізувати визначення цих понять з позицій системного підходу та на основі знань про склад і співвідношення інформаційно-комунікаційних, інформаційних,

електронно-комунікаційних та комп'ютерних систем (розділ 3), сутність комп'ютерних технологій обробки інформації та формалізоване поняття "кібербезпека" (розділи 4, 5), та можливо зробити наступні висновки:

- визначення дуже складні через наявність надлишкових уточнень ("кібератака": зрозуміло, що дії в кіберпросторі можливо тільки за допомогою тільки апаратних та програмних комп'ютерних засобів; порушення любих важливих властивостей інформації – це вже порушення кібербезпеки; "кіберінцидент": якщо це подія в складі кібератаки, те не має сенсу додатково уточнювати можливі наслідки від порушення кібербезпеки);
- поняття мають ряд семантичних невизначеностей ("кібератака": пояснюється через кібератаку (… використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак …); "інформаційно-комунікаційні технології" – що це? "Кіберінцидент" - можливо лі помилкові дії людини, що спровоковані зловмисником, відносити до ненавмисного характеру?).

За результатами семантичного аналізу двох понять можливо зробити наступний висновок - ці поняття дуже складно використовувати для практичного застосування в підрозділах кіберзахисту. Для технічних фахівців в галузі комп'ютерних технологій рекомендуємо використовувати наступну групу понять, що за сенсом послідовно узгоджені між собою:

вразливість інформаційної системи (кібервразливість) – це така властивість інформаційної системи, що дозволяє зловмиснику порушити стан кібербезпеки;

загроза інформаційній системі (кіберзагроза) – це сукупність можливих дій зловмисника, що дозволяють використати вразливість для порушення стану кібербезпеки;

кібератака – це реалізована загроза, або загроза в стадії реалізації;

кіберінцидент – це зареєстрована подія в комп'ютерному середовищі (кіберсегменті), що може бути частиною кібератаки.

Приклади:

1) інформаційна система в рамках технології забезпечення цілісності свого програмного забезпечення використовує алгоритм хешування MD5 (Message Digest 5) , який з 2011 року вважається ненадійним (дозволяє за невеликий час знайти колізію хеш-образу). Знаючі про цю *кібервразливість* в зловмисник може підготувати *кібератаку* по впровадженню шкідливого програмного коду в рамках штатного оновлення програмного забезпечення;

2) інформаційна система в рамках використання корпоративної електронної пошти не застосовує засоби захисту поштових повідомлень на предмет визначення шкідливих вкладень або посилань. Ця *вразливість* значно спрощує зловмиснику завдання по організації *атаки* категорії "фішінг" ("Phishing", методи соціальної інженерії для провокування користувачів ІС на потрібні дії) з метою впровадження в кіберсегмент шкідливої програми-агента, наприклад, на основі використання завантажувача шкідливого ПО Cobalt Strike's Beacon.

11.2. Класифікація кібератак

Результативність проведення атак залежить від знань зловмисника про: структуру системи-жертви; набор сервісів, що використовуються в технологіях обробки інформації; вразливості технологій та складності їх використання. Чим менший обсяг цих знань, тим більше витрати часу, фінансів та фахових людських ресурсів на підготовку та проведення атаки. Малозатратні атаки можливо віднести до *простих атак*, що можуть застосовуватися відносно конкретних інформаційних систем з гарантованим результатом, або до великої кількості

систем з випадковим результатом відносно тільки деяких з них. Наприклад:

1) відомо що веб-сайти можуть використовувати протокол http для обміну гіпертекстом. Він має вразливість відносно неможливості самостійно переривати незакінчені процедури встановлення логічного з'єднання між клієнтом та сервером. Ці знання дозволяють швидко організувати нескладні, малозатратні та результативні атаки на відмову в обслуговувані ((distributed) denial-of-service attack, DOS та DDOS);

2) на основі вразливості процедури оновлення електронного сервісу податкової звітності масштабно застосовується шкідливе ПЗ, що самостійно розповсюджується (програма "хробак") в Інтернет. Ця малозатратна атака буде результативної тільки відносно тих ІС, де застосовується цей електронний сервіс. Всі інші, куди попав цей "хробак", продовжують працювати в штатному режимі. У випадку коректної роботи їх інфраструктури кіберзахисту факт наявності "хробака" буде оцінений як кіберінцидент.

До складних атак відносяться ті, що потребують великих витрат. Таки атаки проводяться відносно конкретних складних систем з дуже критичним інформаційним ресурсом. Вони готуються та реалізуються тривалий час (від декілька місяців до 1,5 року та більше), потребують великі фінансові (від ста тисяч до 100 мільйонів доларів) та людські (до сотень висококваліфікованих фахівців) ресурсів. Як правило, підготовку таких атак можуть собі дозволити крупні корпорації або державні спецслужби. Таки атаки прийнять називати цільовими, таргетованими (від англ. *target* – мішень, об'єкт, ціль) або APT атаками (від англ. *Advanced Persisten Threat* - вдосконалена стійка (довготривала) загроза).

Приклади APT атак:

1) атака на промисловий комплекс зі збагачення урану в місті Натанзі (Іран) за допомогою комп'ютерного вірусу win32/Stuxnet. Це перший відомий комп'ютерний хробак, що

перехоплює і модифікує інформаційний потік між програмованими логічними контролерами (PLC) марки SIMATIC S7 і робочими станціями SCADA-системи SIMATIC WinCC фірми Siemens. За деякими джерелами підготовка атаки почалась з 2007 року. За результатами виведено з ладу більше 1000 центрифуг шляхом підвищення швидкості обертів двигунів. Це перший зареєстрований випадок руйнування фізичної інфраструктури комп'ютерним вірусом;

2) APT атака на ПАТ "Прикарпаттяобленерго" 23 грудня 2015 року (міжнародна назва атаки – BlackOut). За результатами атаки було відключено біля 225 000 користувачів системи електрозабезпечення. Перший зареєстрований випадок результативної кібератаки на енергетичну структуру. Проведена за допомогою комп'ютерного вірусу Black Energy 3, який був впроваджений в систему за допомогою фішінгу на електрону пошту організації. Атака почалась в березні 2014 року та складалась з послідовності декількох етапів.

У вітчизняному нормативному просторі застосовується наступний Перелік категорій кіберінцидентів (далі – Перелік, табл. 11.1) розроблений на основі Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021)). Перелік призначений для впровадження таксономії як інструменту для обміну інформацією щодо кіберінцидентів. Цей Перелік має регулярно переглядатися з урахуванням практики його застосування, появи нових категорій і типів кіберінцидентів, а також інформації, отриманої від суб'єктів забезпечення кібербезпеки.

Табл.11.1. Перелік категорій кіберінцидентів

Код xx	**Категорія інциденту**	**Код xx**	**Тип інциденту**	**Тип інциденту (англ.).**	**Опис типу інциденту**
01.	Шкідливий (образливий) вміст (Abusive content)	01	Спам	Spam	Надсилання небажаних повідомлень або великої кількості повідомлень (флуд)
02.	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (далі – ШПЗ)	Malware infection	У системі виявлено ШПЗ.
		02	Розповсюдження ШПЗ	Malware distribution	Розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містять вкладення з шпз або посилання на його завантаження.
		03	Командно-контрольний центр (C2)	Command & Control (C2)	Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами.
		04	Шкідливе підключення	Malicious connection	Спроби з'єднання від/до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов'язаних із активністю певної бот-мережі.
03.	Збір інформації зловмисником (Information Gathering)	01	Сканування	Scanning	Збір інформації про системи або мережі.
		02	Сніфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та

					зчитування мережевого трафіку.
		03	Фішинг	Phishing	Спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою спрямована на збір даних, може містити посилання на фішингові сайти)
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnerability exploitation attempt	Спроба вторгнення з використанням вразливості у системі, компоненті чи мережі
		02	Спроби авторизації/ входу в систему	Login attempts	Спроба входу до служб або механізмів автентифікації / доступу. Невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних.
05.	Втручання (Intrusion)	01	Компрометація облікового запису	Account compromise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
		02	Компрометація системи	System compromie	Фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід системи контролю доступу.
06.		01	Атака на відмову в	DoS/DDoS	Вплив на нормальне функціонування

	Порушення доступності (Availability)		обслуговуванні		системи чи сервісу що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів.
		02	Саботаж / шкідливі дії	Sabotage	Дії (навмисні або ненавмисні), спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо.
		03	Збій	Outage, no malice	Збій в роботі системи чи її компоненту без зловмисного втручання.
07.	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації	Unauthorised access to information	Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації.
		02	Несанкціонована модифікація	Unauthorised modification ofinformation	Несанкціонована зміна або видалення певного набору інформації.
08.	Шахрайство (Fraud)	01	Шахрайський сайт	Fraudulent site	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Використання ресурсів установи для цілей, відмінних від передбачуваних.
09.	Відома вразливість (Vulnerable)	01	Вразливість	Vulnerability	Наявність в системі чи її компонентах відомих вразливостей, відкритих для експлуатації
		02	Некоректна конфігурація	Misconfigur-ation	Недоліки в налаштуваннях, що можуть бути використані зловмисником

					(налаштування за замовчуванням тощо)
10.	Інше (Other)	01	Невизначений інцидент	Undetermined incident	Недостатньо даних для обробки інциденту

ПРИКЛАД 1:
Код інциденту: 01.01; Тип інциденту: Spam (Спам).

ПРИКЛАД 2: Код інциденту: 02.04; Тип інциденту: Malicious connection (Шкідливе підключення).

Якщо інцидент віднесено до певної категорії, проте не визначено його тип, використовується код 00.
ПРИКЛАД 3: Код інциденту: 01.00; Тип інциденту: не визначено. Категорія: Abusive content.

11.3. APT атака та проактивна стратегія кіберзахисту

Аналіз практик захисту корпоративних інформаційно-комунікаційних систем (ІТС) дозволяє виділити дві стратегії протидії кібератакам:

- реактивний захист;
- проактивний (превентивна) захист.

Загальною основою для цих стратегій є такі процеси:

1) спостереження в реальному часі (in real time) за подіями в позначеному сегменті кіберпростору;

2) формування за допомогою сенсорів, збір і нормування інформації про події безпеки в єдиному центрі оперативної обробки;

3) аналіз подій і прийняття рішення про наявність кібератаки;

4) прийняття рішення про протидію атаці і реалізація цього рішення за допомогою актуаторів безпеки (виконавчих пристроїв безпеки).

Для *реактивної стратегії* прийняття рішення про виявлення атаки завершується після її закінчення. Заходи протидії можуть запобігти тільки такий же наступній атаці. Для *проактивного (превентивного) захисту* виявлення атаки має відбутися ще до її завершення. В такому випадку залишається час на реалізацію заходів переривання цієї атаки.

Ряд особливостей APT атак представляють інтерес з позицій проактивного захисту:

- атака представляє складний набір взаємозв'язаних за часом і простором дій зловмисника. Окремо ці дії можуть не викликати підозр;

- цільова (заключна) акція атаки в кіберсегменті об'єкта готується тривалий час (від декількох місяців до року і більше);

- сукупність дій зловмисника - це ланцюжок тактик, виконання яких дозволяє досягти мети атаки. Незважаючи на різноманітність засобів, що використовуються в APTs з різними цілями, набір більшості тактик і їх сутність залишаються постійними.

Повторення послідовності дій зловмисника в різних нападах на різні об’єкти сприяє розвитку конструктивних методів проактивного захисту від APT атак, що робить актуальними дослідження в цієї області. Представлена далі деталізація дозволяє уточнити суть дій зловмисника.

Після визначення цільової ІКС і її ресурсу, який критичний для зловмисника (наприклад: база даних, диспетчерський комп’ютер SCADA, веб-сайт або інше. Далі - об'єкт атаки) він діє в рамках наступної послідовності тактик.

Етап 1. Зовнішня розвідка. Здійснюється збір інформації про характеристики ІКС з різноманітних джерел поза нею.

Етап 2. Підготовка атаки. На основі інформації зовнішньої розвідки приймається рішення про засоби і способи запуску несанкціонованих процесів в одному з вузлів мережі ІКС. Розробляються (підбираються) та перевіряються необхідні засоби нападу.

Етап 3. Проникнення в кіберсегмент ІКС. За допомогою комп'ютера зловмисника здійснюється реалізація рішення шляхом направлення через Інтернет (або іншим шляхом) необхідних засобів атаки в комп'ютерне середовище жертви. На основі активації доставлених засобів нападу повідомлень запускаються процеси, які встановлюють прихований канал віддаленого керування комп'ютером .

Етап 4. Доставка засобів впливу. Отримана зловмисником інформація про встановлений прихований канал управління запускає процес доставки набору несанкціонованих програмних засобів, що дозволяють здійснити внутрішню розвідку в межах комп'ютерної мережі жертви.

Етап 5. Внутрішня розвідка. Шляхом запуску несанкціонованих і штатних обчислювальних процесів здійснюється збір даних про компоненти мережі. Зібрана інформація надсилається по прихованому каналу зловмиснику. Після її оцінки приймається і реалізується рішення про просування вузлами мережі до моменту виявлення критичного ресурсу.

Етап 6. Цільовий вплив (цільова акція атаки). На основі отриманих даних про знаходження критичного ресурсу приймається рішення про засоби і заходи реалізації цільового впливу. За допомогою прихованого каналу управління критичним кінцевим вузлом доставляються необхідні програмні засоби. Запускаються несанкціоновані процеси, які

реалізують компрометацію цільового ресурсу (отримання доступу до критичної інформації і передача її зловмиснику, отримання доступу до управління технологічним процесом та переведення його в потрібний стан, порушення процесів обробки інформації та ін.).

Етап 7. Приховування слідів атаки. За допомогою несанкціонованих процесів на всіх кінцевих вузлах стираються дані, які були пов'язані з атакою.

В рамках цих етапів сукупність дій різних атака може суттєво відрізнятися. Це залежить від апріорних знань зловмисника про об'єкт. Незалежно від цього загальна логіка атаки остається однаковою. Це дозволяє розробляти ріні моделі APT атак для застосування в стратегії превентивного захисту.

11.4. Кібернетична модель APT атаки

Більшість відомих моделей APT атак представлені у вигляді вербального опису етапів атаки і їх смислового змісту. Приклад такого опису у вигляді послідовності етапів був представлений в попередньому пункті. Переваги таких моделей - вони виділяють загальні закономірності для різних атак:

- всі APT атаки спрямовані на конкретний ресурс ІКС (цільовий ресурс);
- незалежно від відмінності в цілях і засобах всі APT атаки проходять однакові етапи: зовнішня розвідка; проникнення в систему; доставка засобів впливу; внутрішня розвідка; цільова акція атаки; приховування слідів атаки.

Недолік таких моделей - неможливість прямого їх в рамках інфраструктури кіберзахисту через відсутність загальної основи для алгоритмізації дій зловмисника в рамках етапів. Це не дозволяє розробляти відповідні комп'ютерні заходи захисту.

В основі іншої групи моделей лежать різні математичні конструкції, що дозволяють уявити масштабні дії зловмисника у вигляді одного складного процесу. Одні такі моделі засновані на представленні у вигляді дерева атаки (графа), в якому елементи (гілки, листя) об'єднуються за допомогою логічних елементів AND або OR. При використанні таких моделей на рівні оцінки в комп'ютерних засобах захисту може використовуватися мурашиний алгоритм оптимізації (AntColony Optimization, ACO). Такі моделі не вважаються найкращими, тому що вони складно зв'язуються з технологічними процесами в кіберсегменті. Інша концептуальна модель, *піраміда атаки*, дозволяє відобразити траєкторію нападу в різних складових середовищах ІКС. Також можливо виділити моделі, які ідентифікують атаку на ранніх етапах і прогнозують її розвиток за допомогою прихованої марківської моделі (Hidden Markov Model, HMM). Практичне застування всіх цих моделей обмежене невизначеністю сутності прихованих станів і складністю реалізації алгоритму Вітербі (Viterby algorithm) для прийняття рішення по значенню стана (тобто, про наявність атаки).

Далі буде розглянута кібернетична модель APT атаки [26], яка дозволяє позбутися перелічених вище недоліків.

В основі моделі лежить загальна для всіх різновидів APT атак наступна послідовність дій, яка регулярно повторюється на всіх етапах:

- отримання зловмисником інформації про стан компонентів ІКС;
- прийняття на основі отриманої інформації рішення про подальші дії;
- реалізація зловмисником прийнятого рішення в ІКС шляхом застосування доставленими або штатними засобами;

- отримання інформації про результати нових дій (несанкціонованого впливу).

Такий регулярний порядок дій дозволяє уявити APT атаку у вигляді траєкторії поведінки керованої (кібернетичної) системи. У такій системі, назвемо її кібернетичної системою APT атаки (CyberSystem of APT, CSoA), можна виділити наступні компоненти:

- об'єкт управління (*Management Object, MO*) - це може бути комп'ютер, комутаційне обладнання мережі, обчислювальні процеси в цих пристроях, або будь-які інформаційні ресурси (файли, бази даних та ін.);
- підсистема управління (*Control SubSystem, CSS*), яка складається з:
- центру управління (*Control Center, CC*) - зловмисник і його комп'ютер;
- сенсора (*sensor, S*) і актуатора (*actuator, A*) - це процеси комп'ютерів, які відповідають за передачу інформації про стан об'єкта управління і прийому інформації про керуючий вплив;
- прямого і зворотного каналу зв'язку (*Forward Link, FL; Return Link, RL*) - це комп'ютерна мережа Internet, що забезпечує обмін інформацією між центром управління CC і об'єктом управління MO.

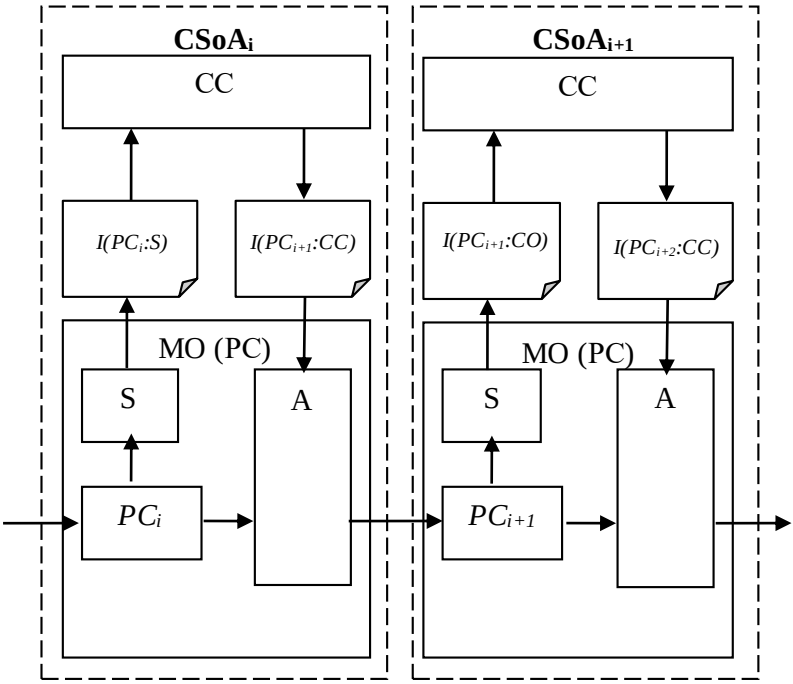
При подальшому уточнені моделі CSoA використовувалося ряд тверджень, які дозволили спростити графічний і математичний опис ситуації:

- будь-які характеристики та стан кінцевого вузла комп'ютерної мережі можна представити у вигляді кінцевої множини двійкових одиниць (бітів);
- інформація про будь-який стан будь-якого кінцевого вузла, яка передається через мережу до будь-якого іншого вузлу, може бути представлена такою же двійкового множиною, як і сам стан;

- роль сенсора кібернетичної системи в комп'ютері виконує обчислювальний процес, який передає інформацію про стан комп'ютера через мережу за вказаною адресою;
- роль актуатора кібернетичної системи в комп'ютері виконує процес, який на основі прийнятих команд запускає нові процеси, що виконують необхідні дії.

Дані твердження дозволяють представити графічно дві суміжні фази CSoA у вигляді наступної структури на малюнку 11.1.

В рамках моделі персональний комп'ютер (PC), що входить до складу корпоративної елемент мережі, виступає в ролі об'єкта управління (MO). Зловмисник і його комп'ютер представлені як центр управління (CC). $I(PC_i:S)$ - це інформація про стан PC_i персонального комп'ютера в рамках актуальної (поточної) фази $CSoA_i$. Дана інформація сформована і направлена до CC сенсором S. На основі прийнятої інформації центр управління CC приймає рішення про переведення об'єкта управління MO в наступний стан PC_{i+1} і оформлює це рішення в вигляді інформації $I(PC_{i+1}:CO)$. Далі ця інформація пересилається до CO, де прийняте рішення реалізується за допомогою актуатора A: об'єкт управління переходить в наступний стан PC_{i+1}.



Мал. 11.1. Графічна модель кібернетичної системи APT атаки

Процес управління в рамках CSoA і поведінку самої CSoA (перехід з однієї фази в іншу) може бути описаний наступною системою рівнянь (11.1):

$$\begin{cases} I(PC_{i+1}:CC) = F_{cc}[I(PC_i:S)]; \\ PC_{i+1} = F_A[PC_i, I(PC_{i+1}:CC)]. \end{cases} \quad (11.1)$$

У даній системі рівнянь:

- PC_{i+1}, $I(PC_i:S)$, $I(PC_{i+1}:CC)$, PC_i - це кінцеві бітові множини;
- F_{cc} [.] - це оператор відображення, який на основі прийнятої інформації і по заданому правилу прийняття рішення формує команду про перехід в інший стан;
- F_A [.] - це оператор відображення, який на підставі прийнятої команди переводить об'єкт управління з одного стану в інший.

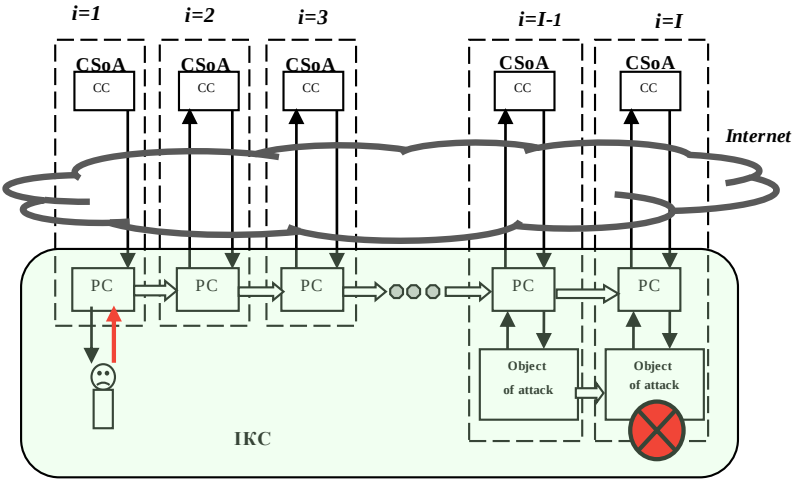
Отримані результати графічної і математичної формалізації CSA дозволяють математично представити всю APT атаку у вигляді наступної множини:

$$\boldsymbol{APT}=\{\boldsymbol{CSoA}_i\},\ i=1,\ldots,I. \qquad (11.2)$$

де:

- ***APT*** - це кінцева множина, що складається з кінцевих підмножин $CSoA_i$ (відповідних фаз кібернетичної системи атаки);
- $\boldsymbol{CSoA_i} = \{PC_i, I(PC_i:S), I(PC_{i+1}:CC)\}$ - підмножина, що складається з кінцевих бітових наборів (множин). Ці набори двох суміжних фаз ***CSoA*** пов'язані між собою системою рівнянь (1);
- $i = 1,\ldots,I$ - номер поточної фази CSA, I - кількість фаз APT атаки.

За допомогою такої формалізації вдалося представити APT атаку у вигляді послідовності фаз кібернетичної системи атаки. Кожна фаза - це послідовність регулярно повторюваних дій, які можна назвати *процедурами атаки*. Часові межі кожної фази визначаються моментами встановлення нового стану об'єкта управління. Під новим станом слід розуміти або зміни в керованому комп'ютері, або перехід до іншого комп'ютера в мережі. Візуальним поясненням запропонованої моделі може бути структура на малюнку 11.2.



Мал. 11.2. Кібернетична модель APT атаки

Пояснення: на малюнку 11.2 в рамках фази 1 ($CSoA_1$) відображено застосування зловмисником прийому "Фішинг". Тобто, провокування користувача системи на дії, що порушують вимоги політики безпеки.

За допомогою запропонованої моделі можливо:

- кожен етап вербальної моделі представити у вигляді однієї або декількох фаз кібернетичної системи;
- кожну фазу представити у вигляді конкретних подій (процедур атаки), що можуть бути зафіксовані на конкретних пристроях корпоративної ІКС;
- кожну процедуру атаки пов'язати із елементарними подіями або набором елементарних подій в ІКС.

Можливо розглядати три види елементарної події:

1) обчислювальний процес вузла мережі;

2) послідовність даних, якими обмінюються обчислювальні процеси вузлів мережі (трафік між процесами вузлів мережі);

3) набір даних (файл) у заданому форматі, які зберігаються на компонентах комп'ютера.

З одного боку кожна елементарна подія пов'язана із набором індивідуальних характеристик конкретного вузла (вузлів) комп'ютерної мережі. Наприклад: кожний трафік пов'язаний із просторовими характеристиками мережі: IP-адреса, MAC-адреса, *domen name* та інші. Також трафік пов'язаний із видом транспортного протоколу (TCP або UDP) і із конкретним обчислювальним процесом (через номер IP-порта). Кожний обчислювальний процес також пов'язаний із рядом характеристик: образ виконуваного машинного коду; пам'ять (зазвичай деяка область віртуальної пам'яті) і її стан; стан стеку викликів; дескриптори ресурсів операційної системи; файлові дескриптори; набір повноважень процесу (допустимі операції); стан процесору (контекст процесору) та інші. Операційна система зберігає більшу частину інформації про процеси в таблиці процесів.

З іншого боку кожна елементарна подія може бути процедурою інформаційного процесу управління кібернетичної системи зловмисника. Відповідно до запропонованої моделі це дозволяє представити дії зловмисника не тільки у вигляді вербального опису в рамках етапів APT, а й у вигляді послідовності фаз кібернетичної системи. У свою чергу кожна послідовність фаз може бути представлена у вигляді послідовності елементарних подій із конкретними характеристиками.

Таким чином за допомогою розглянутої моделі кожну APT атаку можливо представити у вигляді набору взаємопов'язаних характеристик елементарних подій на вузлах мережі ІКС. Такий набор є шаблоном APT атаки, що може бути застосований в рамках автоматизованого її детектування засобами інфраструктури кіберзахисту.

Висновки за розділом 11

- *Вразливість інформаційної системи (кібервразливість)* – це така властивість інформаційної системи, що дозволяє зловмиснику порушити стан кібербезпеки.
- *Загроза інформаційній системі (кіберзагроза)* – це сукупність можливих дій зловмисника, що дозволяють використати вразливість для порушення стану кібербезпеки.
- *Кібератака* – це реалізована загроза, або загроза в стадії реалізації.
- *Реактивної стратегія кіберзахисту* - прийняття рішення про наявність атаки завершується після її закінчення. Відсутній час для переривання атаки.
- *Проактивна (превентивна) стратегія захисту* - виявлення атаки має відбутися ще до її завершення. В такому випадку залишається час на реалізацію заходів переривання цієї атаки.
- Кожна атака залежить від обсягу ресурсів зловмисника: знання про структуру системи-жертви; витрати часу, фінансів та фахових людських ресурсів на підготовку та проведення атаки.
- *Прості атаки* – це малозатратні атаки. *Складні атаки* – це багатозатратні атаки.
- До складних атак відноситься і (від англ. *Advanced Persisten Threat* - вдосконалена стійка (довготривала) загроза). Інша назва – цільова (таргетована, від англ. *target* – мішень, об'єкт, ціль) атака.
- Особливості APT атак, що представляють інтерес з позицій проактивного (превентивного) захисту:

- атака представляє складний набір взаємозв'язаних за часом і простором дій зловмисника. Окремо ці дії можуть не викликати підозр;
- цільова (заключна) акція атаки в кіберсегменті об'єкта готується тривалий час (від декількох місяців до року і більше);
- сукупність дій зловмисника - це ланцюжок тактик, виконання яких дозволяє досягти мети атаки. Незважаючи на різноманітність засобів тактик їх сутності залишаються постійними.

- Основні тактики APT атак:
  Зовнішня розвідка об'єкту атаки.
  Підготовка атаки.
  Проникнення в кіберсегмент об'єкта.
  Доставка засобів впливу.
  Внутрішня розвідка.
  Цільовий вплив (цільова акція атаки).
- Для створення ефективних заходів захисту від APT потрібні таки моделі атак, що дозволяють пряме їх застосування в рамках інфраструктури кіберзахисту через можливість алгоритмізації відповідних обчислювальних процесів.
- Кібернетична модель APT атаки представляє її у вигляді циклічної поведінки керованої системи. Зловмисник – суб'єкт керування такою системою, а комп'ютер-жертва інформаційної системи – об'єкт керування.
- Модель дозволяє кожний цикл керування атакою пов'язати з набором елементарними подій в ІС, що можуть бути зафіксовані на конкретних пристроях.

Контрольні питання та завдання

1. Співвідношення кібервразливості та кіберзагрози?
2. Кібератака, класифікація?
3. APT атака та її особливості?
4. Реактивна стратегія кіберзахисту? Приклади.
5. Проактивна стратегія кіберзахисту? Приклади.
6. Особливості APT атак, що дозволяють проводити проективну стратегію кіберзахисту?
7. Сутність основних тактик APT атаки?
8. Визначте перелік інформації про ІС-жертву, що може бути визначена в рамках тактики "*зовнішня розвідка"*?
9. Визначте можливі цілі APT атаки на систему SCADA для керування залізничним транспортом.
10. Визначте можливі цілі APT атаки на інформаційну систему державної установи.

12. ІНФРАСТРУКТУРА КІБЕРЗАХИСТУ

- **поняття та компоненти інфраструктури кіберзахисту**
- **характеристики засобів кіберзахисту**
- **зв'язок циклу керування кібербезпекою з компонентами інфраструктури**
- **графічна модель та інформаційні процеси інфраструктури**

В розділі 7 було розглянуто сучасні системні засади організації кіберзахисту інформаційно-комунікаційних систем [15, 17, 18]. Теоретичну основу всього процесу кіберзахисту складають наступні підходи:

- всі заходи кіберзахисту поділяються на 5 етапів;
- послідовне виконання функції цих етапів складає цикл кіберзахисту;
- безперервність кіберзахисту забезпечується послідовним повторюванням циклів (циклічний процес);
- в основі кожного циклу застосовується концепція управління ризиками загроз (ідентифікація та оцінювання ризиків загроз, визначення фактів реалізації загроз, обробка ризиків загроз до прийнятного рівня);
- для опису комплексу заходів кіберзахисту кожного етапу застосовується принцип ієрархічної декомпозиції:

1) всі заходи поділяються на окремі блоки:

2) всі блоки розміщуються на різних рівнях ієрархії;

3) кожний блок заходів вищого рівня реалізується послідовністю (набором) блоків нижнього рівня;

4) більш загальний опис заходу вищого рівня деталізується в описах блоків нижнього рівня.

Всі ці теоретичні конструкції потрібно реалізовувати сукупністю конкретних засобів та заходів, які складають інфраструктуру (систему) кіберзахисту конкретної ІКС. В цьому розділі буде розглянуто основні компоненти

інфраструктури, їх загальні характеристики та принципи застосування.

12.1. Поняття та компоненти інфраструктури кіберзахисту

Діяльність із забезпечення кібербезпеки спрямована на зниження відповідних ризиків та має безперервний циклічний характер. Кожний цикл керування кібербезпекою складається з п'яти етапів (мал. 7.1). Заходи кіберзахисту кожного етапу повинні виконувати окрему функцію. Кожна функція має назву та загальний опис її змісту:

1) «Ідентифікація ризиків кібербезпеки» (Identify, ID).
   Формування розуміння складу інформаційної системи, умов її функціонування, переліку інформаційних ресурсів, що підтримують надання життєва важливих послуг та функцій. Визначення ризиків кібербезпеки, що пов'язані з цими послугами та функціями. Обґрунтований вибір пріоритетів захисту та конкретних заходів для впровадження;
2) «Кіберзахист» (Protect, PR).
   Визначення (розробка) відповідних методів, засобів, процедур кіберзахисту. Впровадження в інформаційну систему прийнятих рішень за допомогою інфраструктури кіберзахисту;
3) «Виявлення кіберінцидентів» (Detect, DE);
   Реалізація заходів своєчасного виявлення кіберінцидентів.
4) «Реагування на кіберінциденти» (Respond, RS)
   Прийняття рішення щодо заходів зниження негативного впливу визначеного кіберінциденту.
5) «Відновлення стану кібербезпеки» (Recover, RC).
   Реалізація заходів зниження негативного впливу кіберінциденту та відновлення поточного стану кібербезпеки.

Для впровадження циклу керування кібербезпекою потрібна інфраструктура кіберзахисту (ІК), яка впроваджується в середовище інформаційної системи. Основою такої ІК є сукупність апаратних та програмних комп'ютерних засобів, які відносяться до таких функціональних компонентів:

1) засоби системи виявлення вторгнень (Intrusion Detection System, IDS);
2) засоби системи запобігання вторгненням (Intrusion Prevention System, IPS);
3) засоби центру операцій кібербезпеки (the Cyber Security Operations Center, CSOC, або просто SOC);
4) засоби системи управління подіями та інформацією безпеки SIEM (Security Information and Event Management);
5) засоби та заходи розвідки кіберзагроз (Cyber Threat Intelligence, CTI).

Розглянутий вище матеріал дозволяє у подальшому використовувати наступне поняття:

Інфраструктура кіберзахисту (ІК) – це організаційно-технічна система, що забезпечує реалізацію комплексу процесів кіберзахисту та об'єднує:

- сукупність апаратних та програмних комп'ютерних засобів кіберзахисту;
- фахівців із кіберзахисту;
- заходи організації процесів кіберзахисту.

12.2. Характеристики засобів кіберзахисту

В якості засобів IDS/IPS можуть застосовуватися люби комп'ютерні засоби, що дозволяють відслідковувати та реєструвати події комп'ютерного середовища (операційні системи, антивірусні засоби, фаєрволи та багато інших). Засоби IDS/IPS можливо класифікувати наступним чином:

- мережеві IDS/IPS (Network-based IDS/IPS, NIDS/NIPS): відстежують трафік в комп'ютерній мережі і блокують підозрілі потоки даних;
- хостові IDS/IPS (Host-based IDS/IPS, HIDS/HIPS): відстежують події безпеки окремих комп'ютерів;
- IDS/IPS для бездротових мереж (Wireless HIDS/HIPS, WIDS/WIPS): перевіряють активність в бездротових мережах. Зокрема, виявляють невірно сконфігуровані точки бездротового доступу до мережі, атаки "людина посередині", спуфинг MAC-адрес;
- IDS/IPS окремих застосувань (Application Protocol-based IDS/IPS, APIDS/APIPS): для захисту окремих застосувань (E-mail, веб-серверів, баз даних та інше).

Відомі безкоштовні IDS/IPS: Snort; Suricata; *mod_security* (для веб-сервера Apache).

Засоби SIEM призначені для виконання наступних функцій:

- *Агрегація даних:* данні (журнали подій) збираються з різних IDS інформаційної системи, потім нормалізуються до необхідного формату, поєднуються та візуалізуються для подальшого аналізу з метою пошуку критичних подій.
- Аналіз даних: пошук в агрегованих даних ознак, що дозволяють прийняти рішення про наявність подій безпеки.
- *Підтримка прийняття рішень про відповідь на подію безпеки*;
- *Зберігання даних:* довготривале зберігання даних в історичному порядку для кореляції даних за часом та іншими ознаками. Таке зберігання важливо для проведення комп'ютерно-технічних експертиз, оскільки розслідування складних інцидентів, зазвичай, відбувається з часовою затримкою від моменту порушення.
- *Експертний аналіз:* визначення подій безпеки по агрегованої інформації безлічі журналів від IDS різних вузлів мережи;

- *Організація ефективної колективної роботи фахівців безпеки.*

Відомі доступні засоби SIEM: платформа ELK Stack (Elasticsearch, Logstash, Kibana); Splunk; IBM QRadar.
Наприклад, в рамках платформи *ELK Stack* засіб *Logstash* забезпечую збір та первинний аналіз журналів подій, *Elasticsearch* забезпечую процедури індексацію та швидкий пошук подій, а засіб *Kibana* надає можливість візуалізації та забезпечує засобами поглибленого аналізу комплексу подій.

12.3. Зв'язок циклу керування кібербезпекою з компонентами інфраструктури кіберзахисту

Функціональні компоненти інфраструктури кіберзахисту поєднується з *циклом керування кібербезпекою* наступним чином (табл. 12.1.):

Таблиця 12.1.

Співвідношення функцій керування кібербезпекою з процесами інфраструктури кіберзахисту

Функція циклу	Процеси інфраструктури кіберзахисту
1. Ідентифікація ризиків (ID)	CTI на основі аналізу ресурсів та сервісів (послуг) інформаційної системи визначає перелік загроз. Для кожної загрози визначаються технічні ознаки (*індикатори компрометації*, *indicators of compromise*, *IOC*), які можуть поєднуватися в *шаблони ознак подій безпеки* (*security event attributes pattern*, *SEAP*). Визначаються перелік необхідних комп'ютерних засобів для інфраструктури кіберберзахисту та необхідні заходи їх використання.
2. Кіберзахист (PR)	Всі засоби та заходи захисту впроваджуються в середовище інформаційної системи. Створюється SOC (це організаційно-технічна система,

	компонентами якої є офіцери безпеки, засоби SIEM та CTI). Режими роботи засобів IDS конфігуруються на основі IOC або SEAP. Перевіряється роботоздатність всіх засобів. Інфраструктура впроваджується в експлуатацію.
3. Виявлення кіберінцидентів (DE)	Засоби IDS порівнюють поточні елементарні події (трафіки, файли, обчислювальні процеси) в комп'ютерному середовищі з відомими IOC та SEAP. У разі збігу індикаторів (шаблонів) з подією (подіями) комп'ютерного середовища формується інформація про подію безпеки (security information) та передається для аналізу на засоби SIEM. За результатами збору, нормалізації та аналізу такої інформації з всієї інформаційної системи офіцери безпеки (або автоматизовані процеси) приймають рішення про наявність інциденту кібербезпеки (кібератаки).
4. Реагування на кіберінциденти (RS)	На основі попереднього досвіду та актуальних знань офіцери безпеки приймають рішення про відповідь на інцидент. За допомогою засобів SIEM формуються та направляються до засобів IPS відповідні команди.
5. Відновлення стану кібербезпеки (RC)	Засобі IPS на основі отриманих команд реалізують прийняте рішення щодо відновлення стану кібербезпеки.

12.3. Графічна модель та інформаційні процеси інфраструктури кіберзахисту

Циклічність процесів кіберзахисту дозволяє представити функціонування інфраструктури кіберзахисту у вигляді процесів кібернетичної системи. По аналогії з моделлю (мал. 8.1.) інфраструктура кіберзахисту може бути представлена сукупністю наступних частин:

1) інформаційна система (ІС) - буде розглядатися як об'єкт керування (Control object, CO);
2) підсистема керування (Control center, CC) кібербезпекою ІС буде складатися з:
   - IDS, що виконують функції сенсорів безпеки (відслідковують події безпеки в ІС та формують відповідну інформацію);
   - SOC, що виконує функції контролера (збирає інформацію про події в ІС, приймає рішення про наявність кіберінцидентів та відповіді для відновлення стану кібербезпеки);
   - IPS, що виконують функції актуаторів безпеки (реалізують впливи на ІС відповідно до рішень SOC);
3) у свою чергу до складу SOC відносяться засоби SIEM, CTI та фахівці (офіцери, оператори) безпеки.

За допомогою засобів графічної формалізації процеси керування кібербезпекою можуть бути представлені у вигляді наступної схеми (малюнок 12.1.). Всі процеси інфраструктури кіберзахисту можливо поділити на дві групи:

I. Процеси розвідки кіберзагроз (далі – процеси CTI).

II. Процеси кіберзахисту (далі – процеси CD, від англ. *cyber defense*).

Процеси I групи є попередніми відносно процесів CD (II групи). Вони забезпечують IDS ознаками можливих подій безпеки *(IOCs)*, без яких не можливе детектування кіберінцидентів та формування відповіді на атаку.

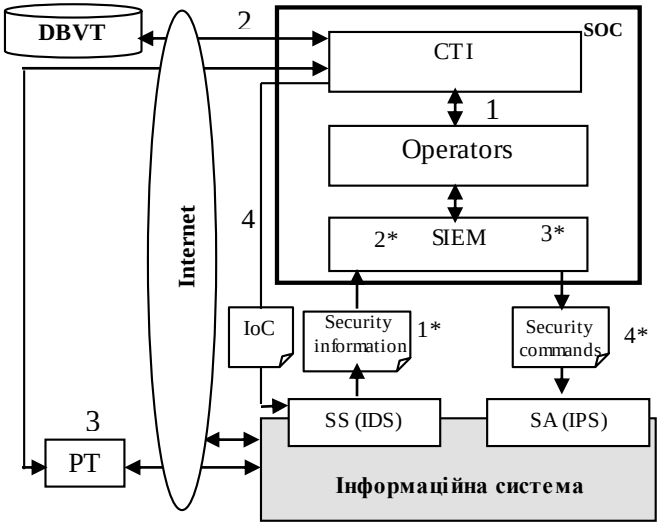
Сутність процесів CTI наступна:

- визначається перелік ресурсів ІС, що потрібно захищати, та відповідних інформаційних технологій;

- на основі переліку ресурсів з різних джерел збирається інформація про відповідні вразливості, загрози та ознаки подій безпеки;

- всі джерела можливо поділити на три групи:

- ✓ загальнодоступні безкоштовні бази даних про вразливості та загрози (наприклад, NVD, MITRE ATT&CK, CAPEC, OWASP, CERT/CC);
- ✓ бази даних спеціалізованих фірм, що надають



I. Процеси розвідки кіберзагроз (CTI):
1 - визначення характеристик ІС;
2 - визначення всіх актуальних загроз;
3 - визначення актуальних вразливостей за допомогою PT
4 - формування набору індикаторів компрометації для сенсорів ІС

II. Процеси кіберзахисту (CD):
1* - спостереження за подіями безпеки ІС;
2* – збір і нормування інформації з сенсорів безпеки про стан ІС;
3* – аналіз подій і прийняття рішень про наявність атаки.
4* - прийняття рішення про протидію та його реалізація актуаторами безпеки.

DBVT – бази даних вразливостей
PT - тестування на проникнення
SS – сенсор безпеки
SA – актуатор безпеки

Мал. 12.1. Модель інфраструктури кіберзахисту та процесів керування кібербезпекою

інформацію за гроші;

- ✓ власні підрозділи CTI, що визначають актуальні вразливості ІС шляхом тестування на проникнення (*penetration testing, PT*);
- формування набору індикаторів компрометації для сенсорів безпеки ІС.

Сутність процесів CD наступна:

- IDS різних компонентів ІС на основі індикаторів компрометації визначають (детектують) події безпеки та формують відповідну інформацію у вигляді файлів журналів подій (*logs*);
- офіцери безпеки засобами SIEM збирають логі зі всіх компонентів ІС, після нормалізації та аналізу інформації приймається рішення про наявність кіберінциденту;
- після комплексного аналізу кіберінциденту приймається рішення про необхідні дії по реагуванню на подію безпеки;
- на основі прийнятого рішення формуються відповідні команди, що реалізуються засобами IPS.

Запропонована модель дозволяє проводити структурний аналіз інфраструктури кіберзахисту для уточнення сутності процесів автоматизації.

Висновки за розділом 12

- цикл керування кібербезпекою складається з п'яти етапів (мал. 7.1). Заходи кіберзахисту кожного етапу повинні виконувати окрему функцію. Кожна функція має назву та загальний опис її змісту.
- Функція 1. **«Ідентифікація ризиків кібербезпеки»** (Identify, ID). Визначення складу ІС, важливих ресурсів, ризиків кібербезпеки, пріоритетів захисту та відповідних заходів.
- Функція 2. **«Кіберзахист»** (Protect, PR). Визначення (розробка) відповідних методів, засобів, процедур кіберзахисту. Впровадження за допомогою інфраструктури кіберзахисту.
- Функція 3. **«Виявлення кіберінцидентів»** (Detect, DE); Реалізація заходів своєчасного виявлення кіберінцидентів.
- Функція 4. **«Реагування на кіберінциденти»** (Respond, RS). Прийняття рішення щодо заходів зниження негативного впливу визначеного кіберінциденту.

- Функція 5. **«Відновлення стану кібербезпеки»** (Recover, RC). Реалізація заходів зниження негативного впливу кіберінциденту та відновлення стану кібербезпеки.
- Функції циклу керування кібербезпекою впроваджуються в ІС інфраструктурою кіберзахисту (ІК).
- Основні функціональні компоненти ІК:
  1) засоби системи виявлення вторгнень (**Intrusion Detection System, IDS**);
  2) засоби системи запобігання вторгненням (**Intrusion Prevention System, IPS**);
  3) засоби та заходи центру операцій кібербезпеки (the **Cyber Security Operations Center, CSOC**, або просто **SOC**);
  4) засоби системи управління подіями та інформацією безпеки **SIEM (Security Information and Event Management**);
  5) засоби та заходи розвідки кіберзагроз (Cyber Threat Intelligence, CTI).
- **Інфраструктура кіберзахисту (ІК)** – це організаційно-технічна система, що забезпечує реалізацію комплексу процесів кіберзахисту та об'єднує:
  - сукупність апаратних та програмних комп'ютерних засобів кіберзахисту;
  - фахівців із кіберзахисту;
  - заходи організації процесів кіберзахисту.
- **Засоби IDS/IPS** - люби комп'ютерні засоби, що дозволяють відслідковувати та реєструвати події комп'ютерного середовища (операційні системи, антивірусні засоби, фаєрволи та багато інших).
- **Мережеві IDS/IPS** (Network-based IDS/IPS, NIDS/NIPS): відстежують трафік в комп'ютерній мережі і блокують підозрілі потоки даних.
- **Хостові IDS/IPS** (Host-based IDS/IPS, HIDS/HIPS): відстежують події безпеки окремих комп'ютерів.

- IDS/IPS для бездротових мереж (**Wireless HIDS/HIPS**, WIDS/WIPS): перевіряють активність в бездротових мережах. Зокрема, виявляють невірно сконфігуровані точки бездротового доступу до мережі, атаки "людина посередині", спуфинг MAC-адрес;
- IDS/IPS окремих застосувань (**Application Protocol-based IDS/IPS, APIDS/APIPS**): для захисту окремих застосувань (E-mail, веб-серверів, баз даних та інше).
- **Засоби SIEM** призначені для виконання наступних функцій:

  Агрегація даних: збір даних з IDS, їх нормалізація до необхідного формату, поєднання та візуалізація для подальшого аналізу.

  Аналіз даних: пошук в агрегованих даних таких ознак , що дозволяють прийняти рішення про наявність подій безпеки.

  ***Підтримка прийняття рішень про відповідь на подію безпеки*;**

  Зберігання даних в історичному порядку для подальшої кореляції за часом та іншими ознаками. Важливо для подальших розслідувань складних інцидентів.

  Експертний аналіз: визначення подій безпеки по агрегованої інформації безлічі журналів від IDS різних вузлів мережи.

  Організація ефективної колективної роботи *фахівців безпеки.*
- Всі процеси інфраструктури кіберзахисту можливо поділити на дві групи:

  I. **Процеси розвідки кіберзагроз** (процеси CTI).

  II**. Процеси кіберзахисту** (процеси CD, від англ. *cyber defense*).
- процеси CTI є попередніми відносно процесів CD, забезпечують IDS ознаками подій безпеки *(індикаторами*

компрометації, IOCs), без яких не можливе детектування кіберінцидентів та формування відповіді на атаку.

- Загальнодоступні безкоштовні бази даних про вразливості та загрози NVD, MITRE ATT&CK, CAPEC, OWASP, CERT/CC.
- Процеси CD:

- IDS на основі IOCs детектують події безпеки та формують відповідну інформацію у вигляді логів;
- офіцери безпеки засобами SIEM збирають всі логі, нормалізують та аналізують на наявність кіберінцидентів;
- приймається рішення про необхідні дії (відповідь0) по реагуванню на подію безпеки;
- на основі рішення формуються команди по відновленню кібербезпеки. Реалізуються IPS.

Контрольні питання та завдання

1. Цикл керування кібербезпекою?
2. Інфраструктура кіберзахисту?
3. Засоби IDS/IPS?
4. Класифікація IDS/IPS?
5. Мережеві IDS/IPS?
6. APIDS/APIPS?
7. Основні функції SIEM?
8. Процеси розвідки кіберзагроз (процеси CTI)?
9. Процеси кіберзахисту (процеси CD)?
10. Класифікація джерел CTI?
11. Загальнодоступні безкоштовні бази даних про вразливості та загрози?
12. Визначте перелік 10 основних загроз поточного року з бази даних OWASP.
13. Визначте перелік 10 основних загроз поточного року від OWASP.
14. Визначте перелік загроз поточного року від MITRE ATT&CK.

13. РОЗВІДКА КІБЕРЗАГРОЗ

- **сутність, класифікація розвідки кіберзагроз та вимоги до розвідувальної інформації**
- **моделі поведінки зловмисників та захисників: Diamond Model; Cyber Kill Chain**
- **модель чотирьох інформаційних середовищ кібератаки.**

Основою функціонування інфраструктури кіберзахисту корпоративної інформаційної системи є процедура порівняння поточних подій в комп'ютерному середовищі з індикатором події безпеки (security event). У разі збігу індикатора з подією формується інформація безпеки (security information) про цю подію, яка передається для аналізу на засоби системи управління подіями та інформацією безпеки SIEM (Security Information and Event Management). За результатами аналізу приймається рішення про наявність інциденту кібербезпеки. На наступному етапі кіберзахисту приймається та впроваджується рішення про відповідь на інцидент, яке відновлює стан кібербезпеки. Таким чином, обов'язковою умовою ефективної роботи інфраструктури кіберзахисту є наявність знань про можливі кіберзагрози та відповідні ознаки (індикатори) подій безпеки на технічному рівні комп'ютерних систем.

За формування ознак подій безпеки відповідає розвідка кіберзагроз (Cyber Threat Intelligence, CTI), або просто – розвідка загроз (Threat Intelligence, TI). В умовах масштабного застосування звичайних повторюваних кібератак основною функцією CTI було визначення простих технічних ознак, які мають назву індикаторів компрометації (Indicators Of Compromise, IOC). В якості таких IOCs використовуються бітові послідовності (сигнатури). Наприклад, IP-адреси хостів зловмисника, що реалізують DDOS атаку. Хеш-образ MD5 шкідливого файлу також є прикладом простого індикатору компрометації. Застосування таких простих IOCs ефективно в рамках реалізації реактивної стратегії кіберзахисту. Всі IOCs

визначаються тільки за результатами аналізу зареєстрованих атак та потім швидко розповсюджуються в середовищі спільноти кіберзахисників.

В умовах масштабного застосування APT атак актуальною стає проактивна (попереджувальна) стратегія кіберзахисту на основі переходу CTI до парадигми прогнозування можливих кібератак на конкретну інформаційну систему (ІС) та формування відповідних складних наборів ознак подій безпеки для їх виявлення ще до кінця реалізації останнього етапу атаки. Стримуючим фактором розвитку у цьому напрямку є комплекс семантичних невизначеностей стосовно базових аспектів функціонування CTI. Основні з них:

- сутність, цілі та методи CTI;
- складові та механізми реалізації;
- класифікація видів CTI;
- моделі поведінки зловмисника та захисника.

В цьому розділі для пояснення сутності розвідки кіберзагроз було обрано інформаційний підхід до представлення комплексу наступних пов'язаних процесів:

підготовки та реалізації кібератаки зловмисником;

організації захисту від цього нападу за допомогою інфраструктури кіберзахисту:

забезпечення розвідкою загроз інформацією, що необхідна для результативного функціонування інфраструктури кіберзахисту.

Обраний інформаційний підхід заснований на такому розумінні сутності інформації, що дозволяє з однакових позицій представити вісь комплекс зазначених процесів. Для цього була обрана концепція атрибутивно-трансферної *природи інформації (Attributive*-Transfer Nature of Information, ATNI). Ця концепція дозволяє представити основні процеси, що складають сутність CTI, у вигляді сукупності різних інформацій та операцій з цією інформацією. На відміну від інших підходів

до інформації ATNI дозволяє представити конкретну інформацію та її зміст (семантику) в явному вигляді як окремий фізичний об'єкт. В свою чергу, кожне перетворення інформації (інформаційний процес) може бути представлено фізичним процесом з особливими властивостями. Крім цього, ATNI дозволяє кожен інформаційний об'єкт описати за допомогою математичної мови теорії множин. Такий опис відкриває можливості для подолання невизначеності вербального опису і переходу до формалізованого опису процесів CTI та кіберзахисту за допомогою обчислювальних алгоритмів. Це сприяє розробці відповідних програмних засобів автоматизації. Більш детально сутність цього підходу було розглянуто в розділі 2.

13.1. Сутність, класифікація розвідки кіберзагроз та вимоги до розвідувальної інформації

Можливо зустріти багато різних сенсів терміну розвідка кіберзагроз, які пов'язуються з інформацією, даними або знаннями про різни аспекти діяльності у сфері кіберзахисту. Це приводить до значної невизначеності відносно організації процесів розвідки як корпоративної CTI, так і процесів ефективної кооперації спільноти кіберзахисників. Розглянемо деякі, найбільш розповсюджені, приклади.

Дослідницька компанія Gartner дає наступне визначення [19]:

Розвідка про загрози — це знання, засновані на доказах, включаючи контекст, механізми, показники, наслідки та корисні поради, про існуючу або виникаючу загрозу чи небезпеку для активів, які можна використовувати для прийняття рішень щодо реакції суб'єкта. до цієї загрози чи небезпеки.

Відома фірма IBM дає наступне тлумачення [20]:

Розвідка про загрози, яку також називають «розвідкою про кіберзагрози» (cyber threat intelligence, CTI) або «розвідкою

про загрози» (threat intel, TI)— це дані, що містять докладні відомості про загрози кібербезпеці, спрямовані на організацію. Розвідка про загрози допомагає командам безпеки бути більш проактивними, дозволяючи їм вживати ефективних дій на основі даних, щоб запобігти кібератакам до того, як вони відбудуться. Це також може допомогти організації краще виявляти поточні атаки та реагувати на них.

Національний інститут стандартів і технологій (NIST) США пропонує свій варіант [21]:

Розвідка про загрози - це інформація про загрози, яка була зібрана, перетворена, проаналізована, інтерпретована або збагачена, щоб забезпечити необхідний контекст для процесів прийняття рішень.

Фірма VMware, яка виробляє спеціалізовані засоби для CTI, надає більш детальне визначення [22]:

Threat Intelligence – це заснована на фактах інформація про кібератаки, яку організовують і аналізують експерти з кібербезпеки. Ця інформація може включати:

- *механізми нападу;*
- *порядок визначення факту атаки;*
- *як різні типи атак можуть вплинути на бізнес;*
- *орієнтовані на дії поради щодо захисту від атак.*

Всі ці визначення та багато інших подібних мають загальний характер та потребують багато уточнень, що необхідні для організації ефективної корпоративної служби CTI. До засобів такого уточнення можна віднести:

- класифікацію по видам CTI;
- набори вимог до розвідувального продукту;
- моделі поведінки зловмисників та захисників;
- способи прогнозування APTs, які дозволяють формувати таки шаблоні ознак подій безпеки, які можливо застосовувати комп'ютерними засобами інфраструктури кіберзахисту.

Розглянемо ці аспекти послідовно.

Класифікація CTI. Широко розповсюджена наступна класифікація по рівням організації CTI [19]:

- стратегічна CTI: стратегічна розвідка про загрози – це інформація високого рівня, яка розглядає загрозу в контекст порушення інформаційних технологій та відповідних наслідків. Це нетехнічна інформація, яку організація може представити раді директорів. Прикладом стратегічної розвідки про загрози є аналіз ризиків про окремі бізнес-рішення, що можуть зробити організацію вразливою до кібератак;

- оперативна CTI: оперативна розвідка про загрози – це збір інформації, яку можливо використовувати як частину активного керування загрозами для вжиття заходів проти конкретної атаки. Це інформація про намір атаки, а також про її характер та час. В ідеалі ця інформація збирається безпосередньо від зловмисників, що ускладнює її отримання;

- тактична CTI: тактичний аналіз загроз включає деталі того, як загрози здійснюються та можливі заходи захисту від них, включаючи вектори атак, інструменти та інфраструктуру, які використовують зловмисники, типи бізнесу або технології, на які спрямовано напад, і стратегії уникнення. Це також допомагає організації зрозуміти, наскільки ймовірно вона стане мішенню для різних типів атак. Експерти з кібербезпеки використовують тактичну інформацію, щоб приймати обґрунтовані рішення щодо контролю безпеки та керування захистом;

- технічна CTI: збір даних про технічні характеристики процесів в комп'ютерних системах, які є конкретними доказами того, що відбувається атака. Такими характеристиками, наприклад, можуть бути ідентифікатори шкідливих додатків фішингових повідомлень електронної, IP-адреси інфраструктури C2 або артефакти з відомих зразків шкідливого програмного забезпечення.

Вимоги до розвідувального продукту. Типовим прикладом рівня якості розвідувального продукту є наступні вимоги [19]:

- достовірність (на основі доказів): щоб будь-який розвідувальний продукт був корисним, його спочатку потрібно отримати за допомогою належних методів збору доказів. Таким чином, аналітики, які покладаються на нього, можуть бути впевнені в його достовірності;
- корисність: щоб розвідка загроз мала позитивний вплив на результат інциденту безпеки або стан безпеки організації, вона повинна мати певну корисність. Розвідувальні дані повинні надати ясність з точки зору контексту та даних про конкретну поведінку або методи, щоб визначити, чи оцінює аналітик інцидент у порівнянні з іншими інцидентами подібного характеру.
- можливість практичного використання: розвідувальні дані повинні стимулювати конкретні дії щодо покращення стану безпеки відносно кіберзагроз, з якими найбільш ймовірно зіткнеться організація, існують механізми застосування в рамках заходів кіберзахисту.

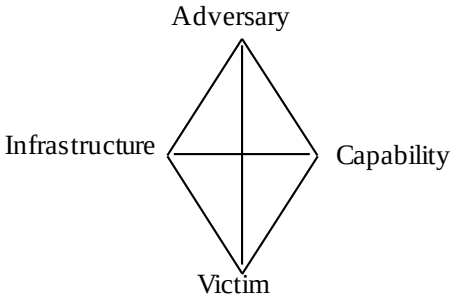
13.2. Моделі поведінки зловмисників та захисників

Для прогнозування загроз та методів захисту від них в рамках CTI широко застосовуються моделі різного рівня складності від загального вербального та графічного опису до рівня математичної інтерпретації дій. Найбільш затребуваними є моделі, в яких математична інтерпретація супроводжується набором правил, які пов'язують дані в журналах подій з елементами математичних конструкцій.

На рівні загального опису найбільш відомі наступні моделі процесів атаки та захисту.

13.2.1. Діамантова модель

Діамантова модель (Diamond Model, DM) [23], що за допомогою схеми діаманта (мал.1) візуально поєднує основні аспекти загрози.



Мал. 13.1. Діамантова модель (Diamond Model, DM).

В моделі відображаються наступні сутності:

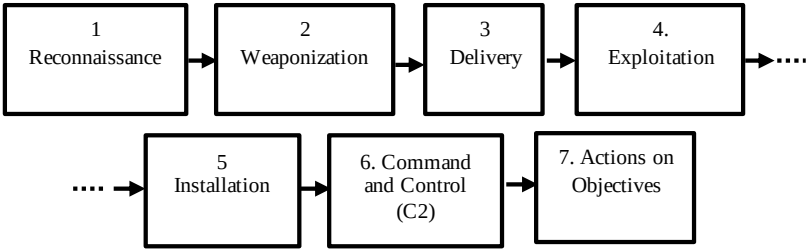
- Adversary (Противник) — це будь-хто, хто прагне скомпрометувати ресурси інформаційної системи, щоб просуватись у напрямку досягнення зловмисних цілей. Противником може бути зловмисник із внутрішнього або зовнішнього середовища системи, групи осіб або, навіть, організації;
- Victim (Жертва) – це об'єкти, що є ціллю втручання (окремі особи, групи осіб, організації, або окремі ресурси інформаційної системи (наприклад, електронна адреса, домен або база даних);
- Infrastructure (Інфраструктура) – це сукупність складових IT-середовища, що використовують хакери для реалізації своїх спроможностей в напрямку досягнення цілі. Діапазон складових може бути від простих складових (доменні імена, заголовки IP-пакетів, IP-порти, облікові записи) до обчислювальних процесів та окремих пристроїв (USB-пристрої, комутатори, маршрутизатори, проміжні сервери зловмисного програмного забезпечення тощо);

- Capability (Спроможність) — це набір засобів/інструментів та заходів/технік, які застосовуються нападником для реалізації загрози та/або захисником для попередження загрози.

Схема у вигляді діаманта (ромба) візуально формує 4-мірний простір, в рамках якого можливо формувати прогнози про загрози та відповідні заходи безпеки. Прогнозування може бути з різної ступеню деталізації. Недолік моделі – відсутні доступні пояснення яким чином можливо перейти від вербального опису до опису на основі технічних характеристик, що можуть «зрозуміти» комп'ютерним пристроям системи кіберзахисту.

13.2.2. Ланцюжок кіберзнищення (Cyber Kill Chain)

Наступна відома модель загального опису - Ланцюжок кіберзнищення (Cyber Kill Chain, CKC). Запропонована трьома фахівцями корпорації Lockheed Martin [24]. Вона представляє дії зловмисника в рамках APT у вигляді послідовності етапів (мал. 2).



Мал. 13.2. Ланцюжок кіберзнищення (Cyber Kill Chain, CKC)

Сутність цих етапів ланцюжка знищення є така:

1. Розвідка (Reconnaissance) – дослідження, ідентифікація та вибір цілей, збір та аналіз інформації про жертву з відкритих джерел (веб-сайти організацій, відомості про організацію з

Інтернет, матеріали конференцій, списки розсилки для адрес електронної пошти, соціальні мережі, інше).

2. Озброєння (Weaponization) — розробка стратегії атаки та комплексу необхідних засобів (зброї), що поєднує в собі засоби віддаленого доступу, необхідне для атаки програмне забезпечення та засоби автоматизованої активації цього програмного забезпечення. Відомі приклади таких засобів - файли даних клієнтських програм, такі як Adobe Portable Document Format (PDF) або документи Microsoft Office з активованими макросами.

3. Доставка (Delivery) - передача (проникнення) зброї в комп'ютерне середовище цільової організації. Три найпоширеніші вектори доставки озброєння учасниками APT — це вкладення електронної пошти, веб-сайти та змінні носії USB.

4. Експлуатація (Exploitation) - після того, як зброя доставлена, починається експлуатація вразливостей комп'ютерного середовища цільової організації. Найчастіше експлуатація націлена на вразливість програми або операційної системи, але вона також може простіше використовувати вразливості самих користувачів (фишинг) або використовувати функцію операційної системи, яка дозволяє автоматично виконувати зловмисний код.

5. Встановлення (Installation) - встановлення несанкціонованого каналу віддаленого доступу (бекдору) в систему-жертву, що дозволяє зловмиснику підтримувати стійкість у середовищі.

6. Командування та керування (Command and Control, C2) – за допомогою несанкціонованого каналу управління (бекдору) у реальному часі забезпечується дистанційне керування зловмисним програмним забезпеченням та/або функціями операційних систем в кіберсегменті жертви.

7. Дії щодо цілей або цільова акція (Actions on Objectives) - після проходження перших шести підготовчих етапів (тактик), зловмисники можуть вживати заходів для досягнення своїх

стратегічних цілей. Як правило, це є викрадання даних, яке передбачає збір, шифрування та вилучення інформації з середовища жертви; порушення цілісності даних або їх доступності; також стратегічною ціллю може бути порушення роботи промислових об'єктів.

Модель дозволяє прогнозувати можливі APT атаки на ресурси корпоративної інформаційної системи шляхом вербального опису. Недолік цієї моделі – також відсутні доступні пояснення про перехід від вербального опису до опису, що зможуть «зрозуміти» комп'ютерні пристрої інфраструктури кіберзахисту.

Існує багато інтерпретацій цієї моделі, що відрізняються ступеню деталізації, межами та відмінностями змісту етапів. Широке розповсюдження знайшла інтерпретація корпорації Mitre [25], що використовує CKC для структурування знань про тактики та прийоми противника, що засновані на реальних спостереженнях. База знань про загрози (фреймворк) MITRE ATT&CK дозволяє детально прогнозувати поведінку зловмисника за допомогою широко відомого концепту як тактики, техніки та процедури (Tactics, Techniques, Procedures, далі - TTPs).

1. Тактика (TA) - це проміжна технічна ціль супротивника, причина виконання дії та те, чого він намагається досягти. Кожна тактика прив'язана до етапу CKC. Досягнення стратегічної цілі реалізується через сукупність досягнення тактичних цілей. Наприклад, зловмисник може захотіти отримати облікові дані, щоб отримати доступ до цільової мережі.

2. Техніки (прийоми, T) представляють собою набір заходів, за допомогою яких противник досягає тактичної мети. Наприклад, зловмисник може попередньо скинути облікові дані, щоб потім отримати доступ до цих даних.

3. Підтехніки – це різні варіанти технік з більш детальним описом. Не всі техніки мають підтехніки.

4. Процедури (P) — це набір необхідних засобів та ресурсів, що дозволяє реалізувати техніки (підтехніки).

В рамках MITRE ATT&CK всі техніки, підтехніки та процедури зв'язані з конкретною тактикою (етапом атаки). Кожна тактика, техніка та підтехніка мають унікальні ідентифікатори (ID). Наприклад, в рамках тактики Reconnaissance (Розвідка, ID: TA0043) може бути застосовано 9 технік, одна з яких – Активне Сканування (Active Scanning, ID: T1595). В свою чергу, техніка T1595 має три підтехніки T1595: 001; 002; 003. З цією технікою також пов'язані рекомендації щодо пом'якшення наслідків загрози (Mitigations, ID: M1056) та опис способів детектування техніки (Detection, ID: DS0029). Крім того, для кожної техніки додаються посилання на джерела (References), що на основі аналізу реальних спостережень деталізують відповідні процедури. Таким чином, ресурси MITRE ATT&CK дозволяють аналітикам CTI формувати деталізовані карти атаки (attack map) на основі технічних відомостей про TTPs.

Спеціалісти Агентства кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency, CISA) рекомендують використовувати картографування атак (attack mapping) для створення набору детальних карт можливих атак на інформаційну систему [9]. При цьому остаються невідомими способи формування відповідних шаблонів ознак події безпеки, що дозволять автоматизовано детектувати атаки за часом і простором інформаційної системи за допомогою комп'ютерних засобів IDS та SIEM.

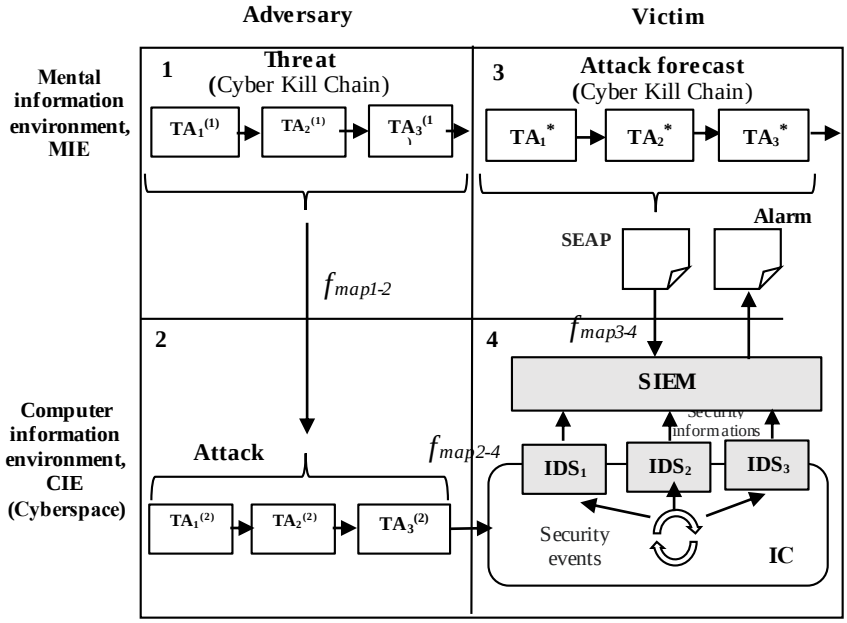
12.4. Модель чотирьох інформаційних середовищ кібератаки

В якості прикладу підходу, що дозволяє деталізувати сутність розвідки кіберзагроз, розглянемо *модель чотирьох інформаційних середовищ кібератаки* (*model of four CyberAttack Information Environments,* далі - *4CAIE*). Ця модель за допомогою інформаційного підходу на основі концепції ATNI (розділ 2) дозволила поєднати та деталізувати:

- діамантову модель (Diamond Model, DM);
- модель ланцюжка кіберзнищення (Cyber Kill Chain, CKC);
- цикл керування кібербезпекою;
- інфраструктури кіберзахисту.

13.3.1. Структура моделі

Структура моделі 4CAIE представлена на малюнку 13.3. Основою моделі є інформаційне середовище кібератаки (CyberAttack Information Environment, CAIE) , що складається з 4-х сегментів, в яких відображаються різні основні аспекти кібератаки та захисту від ней. Сегменти моделі сформовані наступними сутностями: противник (Adversary), жертва (Victim), ментальне інформаційне середовище (Mental Information Environment, MIE), комп'ютерне інформаційне середовище (Computer Information Environment, CIE), або його розповсюджена назва – кіберпростір (Cyberspace).



Мал. 13.3. Модель 4-х інформаційних середовищ кібератаки (4CIE)

CAIE як множину можливо представити декартовим добутком двох кортежей:

$$CAIE = (Adversary, Victim) \times (MIE, CIE). \quad (13.1)$$

У подальшому в рамках моделі будемо розглянемо наступні сегменти CAIE:

- сегмент 1 (MIE, Adversary) – це ментальне середовище противника, де визначається цільова жертва та формується план атаки на інформаційну систему жертви, (тобто, це сегмент загрози):
- сегмент 2 (CIE, Adversary) - це комп'ютерне середовище противника, засобамиякого противник реалізує атаку на основі семантики раніше сформованої загрози (тобто, це сегмент атаки):
- сегмент 3 (MIE, Victim) - це ментальне середовище жертви, де формуються прогнози можливих кібератак (Attack Forecast) (далі, сегмент кіберзахисту);
- сегмент 4 (CIE, Victim) - це комп'ютерне середовище жертви, що реалізовано в інформаційної системі. В сегменті відображаються впливи атаки противника та дії жертви щодо кіберзахисту від цієї атаки (далі, сегмент кіберзахисту).

Сегменти 1-2 та 2-3 пов'язані між собою інформаційними впливами, які можливо представити наступними операторами:

$f_{map1\text{-}2}$ - оператор інформаційного впливу, що дозволяє перетворювати семантичні конструкції MIE в конструкції CIE. Реалізується людиною шляхом маніпулювання комп'ютерними засобами вводу-виводу даних (тобто, використовується людино-машинний інтерфейс);

$f_{map2\text{-}4}$ - оператор інформаційного впливу, що дозволяє перетворювати семантичні конструкції CIE сегменту 2 в семантичні конструкції CIE сегменту 4, шляхом передачі необхідних даних на відстань між сегментами за допомогою електромагнітних сигналів;

$f_{map3\text{-}4}$ - оператор інформаційного впливу, що дозволяє по аналогії з $f_{map1\text{-}2}$ перетворювати семантичні конструкції MIE

жертви (прогнози атак) в конструкції CIE (шаблони індикаторів компрометації (SEAP) для засобів SIEM). Тобто це сегмент розвідки загроз.

13.3.2. Концепція моделі 4CIE

В рамках чотирьох інформаційних середовищ (сегментів) моделі можливо деталізувати та поєднати події, що розкривають сутність підготовки та реалізації APT, процеси захисту від неї та завдання розвідки кіберзагроз. Послідовно розглянемо події по сегментам.

1. Почнемо з сегменту 4. Його основу складає інформаційна система (ІС, або англомовною термінологією – система інформаційних технологій, IT-system). Для противника ця ІС виступає у ролі жертви. Комп'ютерні апаратні та програмні засоби ІС дозволяють реалізовувати різні технології обробки інформації (TOI) в інтересах персоналу ІС. Кожна TOI представляє собою динамічну за часом комбінацію, що складається з необхідної кількісті елементарних подій трьох видів відносно бітових наборів:

a) набори бітів, що зберігаються у комп'ютерному інформаційному середовищі – файли;

b) набори бітів, якими обмінюються комп'ютери – трафіки;

c) перетворення одних наборів бітів в інші за допомогою процесорів та відповідних програм комп'ютера – обчислювальні процеси (ОП).

2. Кожна елементарна подія в ІС може бути зареєстрована сенсором подій (комп'ютерний апаратний або апаратно-програмний засіб), який формує інформацію про цю подію (відповідний запис в журналі подій). Для відстеження подій, що впливають на стан кібербезпеки, використовуються сенсори безпеки, які прийнято називати засобами системи виявлення вторгнень (Intrusion Detection System, IDS). Вся інформація про події безпеки (інциденти кібербезпеки) від всіх IDS збирається для подальшого аналізу засобами системи керування

інформацією та подіями безпеки SIEM. За результатами аналізу даних засобами SIEM приймається рішення про наявність вторгнення в ІС.

3. Ментальне інформаційне середовище сегменту 1 фізично розміщується в голові зловмисника. В ньому на основі інформації про вразливості ІС жертви та відомостей про засоби та методи нападу формується план (семантична конструкція) проведення APT атаки. На малюнку 13.3. цей план представлений у вигляді ланцюжка кіберзнищення (Cyber Kill Chain, CKC) та позначається як Threat (загроза). CKC складається з послідовності тактик (етапів) $TA_i^{(j)}$ (i – номер етапу, верхній індекс j – номер сегменту). На мал. 13.3. – тільки три тактики TA). Тобто, загрозу можливо представити наступним чином

$$Threat = (TA_1^{(1)}, TA_2^{(1)}, \ldots, TA_i^{(1)}). \qquad (13.3)$$

Шляхом маніпуляцій в сегменті 2 зловмисник реалізує загрозу в у вигляді семантик його кіберсередовища. Для цього за допомогою відповідних комп'ютерних засобів він реалізує оператор інформаційного впливу $f_{map1\text{-}2}$. Тобто, семантики сегменту 1 перетворюються у семантики сегменту 2:

$$\begin{aligned} Attack &= f_{map1\text{-}2}(Threat) = \\ &= f_{map1\text{-}2}[(TA_1^{(1)}, TA_2^{(1)}, \ldots, TA_i^{(1)})] = \\ &= (TA_1^{(2)}, TA_2^{(2)}, \ldots, TA_i^{(2)}) \end{aligned} \qquad (13.4)$$

4. Результатом реалізації семантик $(TA_1^{(2)}, TA_2^{(2)}, \ldots, TA_i^{(2)})$ є інформаційний вплив $f_{map2\text{-}4}$ на середовище 4. Цей вплив реалізується передачею необхідних даних на відстань між сегментами за допомогою електромагнітних сигналів. Вплив

може бути реалізований або в режимі *on-line* (трафік через Інтернет), або в режимі *off-line* (приклад, зараження вірусом Stuxnet через USB-flash накопичувач, атака на ядерні об'єкти Ірану, 2010 рік).

5. З метою захисту від можливих атак розвідкою кіберзагроз в сегменті 3 формується прогноз атаки

$$Attack\ forecast = (TA_1^{(3)}, TA_2^{(3)}, \ldots, TA_i^{(3)}). \qquad (13.5)$$

Прогноз атаки, що формується в ментальному середовищі жертви (сегмент 3), не може бути використаний в комп'ютерному середовищі інформаційної системи жертви (сегмент 4) для детектування атаки засобами кіберзахисту (IDS), якщо він носить загальний (вербальний) опис. Якщо визначені привила, за допомогою яких можливо прогноз представити у вигляді сукупності ознак елементарних подій, то можливо сформувати шаблони подій (інцидентів) безпеки SEAP.

$$SEAP = f_{map3\text{-}4}(Attack\ forecast). \qquad (13.6)$$

У випадку коли інформація про події в кіберсегменті (формується засобами IDS) буде співпадати з ознаками подій безпеки шаблону SEAP (знаходиться в SIEM), то буде формуватися сигнал попередження *Alarm*.

Представлена концепція моделі 4CAIE дозволяє конкретизувати завдання CTI:

1) за допомогою вербального опису скласти прогноз атаки у вигляді послідовності етапів моделі CKC з деталізацією тактик, технік та процедур (TTPs);
2) в рамках визначеної тактики представити можливі техніки та процедури у вигляді елементарних подій кіберсередовища (трафіки, файли, обчислювальні процеси);

3) для набору елементарних подій тактики визначити індикатори компрометації подій (як правило це будуть бітові сигнатури);

4) розробити правила, за якими можливо формувати шаблон подій безпеки SEAP для прогнозу Attack forecast;

5) сформувати методику використання SEAP в рамках конфігурації інфраструктури кіберзахисту;

6) перевірити роботоздатність методики;

7) передати SEAP та методику її використання підрозділам підтримки інфраструктури кіберзахисту.

Приклад використання моделі. За допомогою:

- кібернетичної моделі APT-атаки [п. 11.4 посібника; 26], що дозволяє представити дії зловмисника (суб'єкт керування) відносно системи-жертви (об'єкт керування) у вигляді послідовності повторюваних цифрових елементарних подій в кіберсегменті (цикл керування);
- запропонованої моделі 4CAIE, що уточнює завдання CTI відносно забезпечення інфраструктури кіберзахисту;

було розроблено спосіб визначення каналу керування APT-атакою [27]. Таки несанкціоновані канали є основою більшості APT-атак. Вони формуються, як правило, на етапі Installation моделі Cyber Kill Chain та експлуатуються зловмисником на етапі Command and Control (C2). Визначення наявності такого каналу ще до початку етапу цільової акції (Actions on Objectives) надає можливість припинити атаку. Такий підхід відповідає проактивної стратегії кіберзахисту.

Розроблений спосіб складається з наступних основних етапів:

1) формування структури багатоіндикаторного шаблону SEAP на основі конкретних характеристик корпоративної інформаційної системи;

2) визначення індикаторів каналу керування;

3) налаштування мережевих і хостових IDS відповідно до структури шаблону та визначених індикаторів;

4) збір інформації про події безпеки за простором та часом ІТ-системи;

5) аналіз інформації шаблону та формування гіпотези про наявність каналу керування;

6) подальший збір та аналіз інформації в рамках підтвердження гіпотези;

7) в разі підтвердження гіпотези – відслідковування подальшої поведінки зловмисника.

Шаблон SEAP для визначення каналу керування був розроблений у вигляді таблиці послідовності циклів, комірки якої містять індикатори подій двостороннього обміну даними (двійкові сигнатури). Така структура шаблону дозволяє визначати наявність каналу керування за результатами збору інформації про трафіки від хостових IDS та IDS на основі фаєрволу периметру системи-жертви. За результатами порівняння індикаторів шаблону з поточною інформацією про трафіки формуються мітки, які заповнюють комірки відповідних циклів. За результатами аналізу комірок послідовності циклів попередньо формуються гіпотези. Подальший аналіз гіпотез на основі міток наступних циклів підтверджує або ні наявність каналу керування атакою.

Висновки за розділом 13

- За формування ознак подій безпеки відповідає розвідка кіберзагроз (Cyber Threat Intelligence, CTI).
- Основна функція CTI - визначення технічних ознак подій безпеки, які мають назву індикаторів компрометації (Indicators Of Compromise, IOC). Наприклад, IP-адресихостів зловмисника, що реалізують DDOS атаку. Хеш-образ MD5 шкідливого файлу також є прикладом простого індикатору компрометації.
- *Розвідка загроз* – це отримання достовірної інформації про можливі кібератаки на інформаційну систему, яку можна аналізувати експертам кібербезпеки з метою визначення

ефективних заходів захисту. Інформація CTI може включати відомості про:

- механізми нападу;
- порядок визначення факту атаки;
- як різні типи атак можуть вплинути на бізнес;
- орієнтовані на дії поради щодо захисту від атак.

- Класифікація CTI:

- *стратегічна CTI* - формування інформації високого рівня, яка розглядає загрозу в контексті порушення інформаційних технологій та відповідних наслідків Приклад, аналіз ризиків про окремі бізнес-рішення, що можуть зробити організацію вразливою до кібератак;
- *оперативна CTI* - це збір інформації, яку можливо використовувати для активного керування загрозою конкретної атаки. Це інформація про намір атаки, а також про її характер та час;
- *тактична CTI* – формування інформації про деталі реалізації загрози та конкретні заходи захисту, включаючи вектори атак, інструменти та інфраструктуру зловмисника, типи бізнесу або технології, на які спрямовано напад, і стратегію уникнення.
- *технічна CTI* - збір даних про технічні характеристики процесів в комп'ютерних системах, які є конкретними доказами того, що відбувається атака.

- Вимоги до розвідувального продукту CTI:

- достовірність (на основі доказів);
- корисність (може вплинути на стан кібербезпеки);
- можливість практичного використання (існують механізми застосування в рамках заходів кіберзахисту).

- *Діамантова модель* (Diamond Model, DM) за допомогою схеми діаманта візуально поєднує основні аспекти кібернападу та захисту від нього: Adversary (Противник), Victim (Жертва), Infrastructure (Інфраструктура), Capability

(Спроможність). Дозволяє аналізувати загрози з різних сторін.

- *Ланцюжок кіберзнищення* (Cyber Kill Chain, CKC) – модель, що представляє дії зловмисника в рамках APT атаки у вигляді послідовності тактик (етапі).
- *Тактики, техніки та процедури* (Tactics, Techniques, Procedures, далі - TTPs) - концепт, який дозволяє деталізувати дії зловмисника.
- *Тактика (TA)* - це проміжна технічна ціль атаки, причина необхідності її досягнення виконання, можливі результати реалізації. Кожна тактика прив'язана до етапу CKC.
- *Техніки (прийоми, T)* - набір заходів для досягнення тактичної мети. Наприклад, зловмисник може попередньо скинути облікові дані, щоб потім отримати доступ цих даних.
- *Підтехніки* – це різні варіанти технік з більш детальним описом. Не всі техніки мають підтехніки.
- *Процедури (P)* — це набір необхідних засобів та ресурсів, що дозволяє реалізувати техніки (підтехніки).

В рамках бази знань MITRE ATT&CK всі техніки, підтехніки та процедури зв'язані з конкретною тактикою (етапом атаки). Кожна тактика, техніка та підтехніка мають унікальні ідентифікатори (ID). Дозволяють аналітикам CTI формувати деталізовані карти атаки (attack map) на основі технічних відомостей про TTPs.

- *Модель чотирьох інформаційних середовищ кібератаки* (*model of four CyberAttack Information Environments*, далі - *4CAIE*) – за допомогою інформаційного підходу на основі концепції ATNI (розділ 2) дозволяє поєднати та деталізувати:

- діамантову модель (Diamond Model, DM);
- модель ланцюжка кіберзнищення (Cyber Kill Chain, CKC);
- цикл керування кібербезпекою;
- компоненти інфраструктури кіберзахисту.

Контрольні питання та завдання

1. Розвідка кіберзагроз (Cyber Threat Intelligence, CTI)?
2. Основна функція CTI?
3. Індикатори компрометації (Indicators Of Compromise, IOCs)?
4. Класифікація CTI?
5. Стратегічна CTI?
6. Оперативна CTI?
7. Тактична CTI?
8. Технічна CTI?
9. Вимоги до розвідувального продукту CTI?
10. Діамантова модель (Diamond Model)?
11. Ланцюжок кіберзнищення (Cyber Kill Chain)?
12. Тактики, техніки та процедури (TTPs)?
13. Модель чотирьох інформаційних середовищ кібератаки (модель *4CAIE*)?
14. За допомогою бази знань MITRE ATT&CK визначте всі тактики, де може бути застосована техніка Active Scanning, (ID: T1595)?
15. За допомогою бази знань MITRE ATT&CK визначте всі тактики, де може бути застосована техніка Active Scanning, (ID: T1595)?
16. За допомогою бази знань MITRE ATT&CK визначте всі техніки, що можуть бути застосовані в рамках тактики *Reconnaissance* (ID: TA0043)?

14. АУДИТ КІБЕРБЕЗПЕКИ

- **базові терміни, визначення та характеристики**
- **концепція аудиту кібербезпеки інформаційної системи**
- **концептуальна модель процесів аудиту кібербезпеки**

14.1. Базові терміни, визначення та характеристики

Термін "аудит" (від лат. *Audit* - слухати) має декілька значень. У вузькому сенсі (історично – перше значення) це перевірка даних бухгалтерського обліку і показників фінансової звітності суб'єкта господарювання з метою висловлення незалежної думки аудитора про її достовірність в усіх суттєвих аспектах та відповідність вимогам нормативним актам.

У загальному сенсі "аудит" - це незалежна діяльність з метою формування *об'єктивної оцінки* про стан особи, організації, системи, процесів, підприємства, проекту або продукту.

Інтуїтивно зрозуміло, що аудит пов'язаний з обробкою інформації. З позицій *вербальної формалізації* та *інформаційного підходу на основі концепції ATNI* (розділ 2), які вже неодноразово використовувались в цьому посібнику, покажемо цей зв'язок. Для цього розглянемо наступні суміжні поняття, що допоможуть більш детально уявити загальний сенс аудиту:

Оцінка - інформація про значення властивостей об'єкта.

Оцінювання – процес формування інформації про значення *властивостей* об'єкту (тобто, формування оцінки).

Розрізняють поняття:

Об'єктивна оцінка – оцінка, що отримана у процесі вимірювання (порівняння) якогось об'єкту з відомим зразком.

Наприклад:

1) кількість продукту порівнюється (вимірюється) на вагах, шляхом порівняння з різними гирями. Вага продукту в 1,5 Кг – це об'єктивна оцінка;

2) лікар вимірює температуру пацієнта за допомого ртутного градусника. Результат 36,6 ^{0}C – це також об'єктивна оцінка, що була отримана безпосереднє з градусника.

Суб'єктивна оцінка - це оцінка, що отримана в ході розумового процесу суб'єкта оцінювання на основі його особистого сприйняття і досвіду.

1) на запитання про вагу товару продавець назвав 2,5 Кг – це оцінка на основі уяви продавця;
2) пацієнт оцінив свою температуру у 38,0 ^{0}C – це також суб'єктивна оцінка на основі особистих уявлень.

Експертна оцінка – суб'єктивна оцінка, яка виражена експертом (досвідченим спеціалістом у відповідної галузі).

Кількісна оцінка – оцінка, яка виражена за допомогою чисел.

Якісна оцінка - оцінка, яка виражена словами.

Якщо кількісна оцінка виражена експертом, то вона буде відноситься до суб'єктивна оцінок. До цих оцінок також будуть відноситься всі кількісні оцінки, що отримані на основі порівняння з різними кількісними шкалами, які сформовані тільки на основі особистої уяві експерта.

Критерії оцінювання – перелік ознак, за якими визначаються значення властивостей об'єкту.

Розуміння суміжних понять дає можливість сформулювати визначення:

Аудит інформаційних технологій *(IT аудит)* **–** процес формування об'єктивної оцінки про ефективність використання інформаційних технологій в бізнес-процесах організації.

Таке визначення потребує наступних уточнень:

Інформаційна технологія – процес обробки інформації за допомогою комп'ютерних засобів.

Ефективність – це параметр, що відображає відношення результату до показника витрат.

Приклад, що пояснює сутність ефективності:

Державна установа застосовує паперову технологію (ПТ) для оформлення дозволів на імпорт товарів подвійного призначення. Для оформлення одного дозволу потрібно 5 діб. Часова ефективність такої технології буде визначатися наступним чином:

$$E(ПТ) = 1 \text{ дозвіл} / (5 \text{ діб}) = 1/5.$$

На заміну ПТ установа планує впроваджувати інформаційну технологію (ІТ). Розробники запропонували два види інформаційних технологій (ІТ-1 та ІТ-2). В рамках ІТ-1 на оформлення дозволу потрібно 2 доби, тобто:

$$E(ІТ\text{-}1) = 1 \text{ дозвіл} / 2 \text{ доби} = 1/2.$$

В рамках ІТ-2 дозвіл оформлюється за пів доби:

$$E(ІТ\text{-}2) = 1 \text{ дозвіл} / 0{,}5 \text{ доби} = 2.$$

Порівняння визначених показників показує, що ІТ-2 має найкращу часову ефективність.

Далі розглянемо два інших види аудиту.

Аудит безпеки інформації – це процес формування об'єктивної оцінки про реальний стан безпеки інформації в організації та її ефективності.

Тобто, під *час аудиту безпеки інформації* формується оцінка відносно всієї критичної інформації, носіями якої є персонал, паперові та комп'ютерні носії. Кібербезпека є частиною безпеки інформації організації, що використовує інформаційні технології, тому:

Аудит кібербезпеки - процес формування об'єктивної оцінки про реальний стан кібербезпеки в організації та її ефективності.

14.2. Концепція аудиту кібербезпеки інформаційної системи

В рамках виконання прийнятої політики безпеки інформації організація застосовує в рамках інформаційної системи комплекс заходів захисту (КЗЗ). Якщо розробка КЗЗ проводилась відповідно до стандартизованих вимог (критеріїв безпеки), то за результатами проведення експертизи на відповідність цім критеріям організація отримує документ (сертифікат, атестат або інше), що засвідчує факт відповідності вимогам безпеки (критеріям безпеки). Для випадку КСЗІ з підтвердженою відповідністю (див. розділ 4) таким документом буде атестат відповідності, що оформлюється за результатами *державної експертизи*.

Під час експлуатації інформаційної системи через низку обставин (зміна в рамках середовищ експлуатації, порушення персоналом режиму забезпечення безпеки, вихід із ладу засобів захисту або обробки інформації, удосконалення засобів і заходів кіберторгнення, інші) можуть виникати *інциденти безпеки інформації*, що приводять до значних втрат організації.

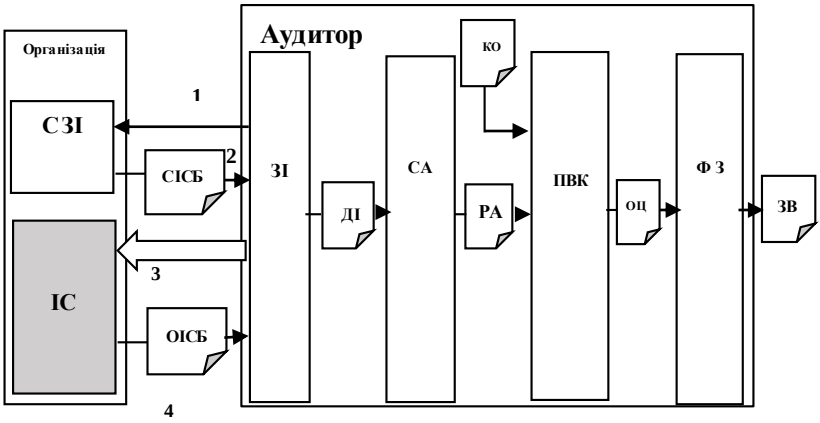
З метою визначення достовірної інформації про дійсний (актуальний) стан за ініціативою керівництва установи може проводитися *аудит безпеки інформації в інформаційної системі* (тобто, *аудит кібербезпеки*).

14.3. Концептуальна модель процесу аудиту кібербезпеки

Процеси *аудиту кібербезпеки* можуть бути уточнені графічною концептуальною моделлю, яка у вигляді інформаційно-функціональної структури представлена на малюнку 14.1.

В моделі відображені інформаційні процеси аудиту відносно інформаційної системи організації. Безпосереднє

аудит починається з запиту до служби захисту інформації (СЗІ) про поточний стан безпеки (процес 1). СЗІ надає відповідну ін-



Інформація:
СІСБ – суб'єктивна інформація про стан безпеки
ОІСБ – об'єктивна інформація про стан безпеки
ДІ – достовірна інформація аудиту
РА - результати аналізу
ОЦ - оцінка стану безпеки
ЗВ - звіт за результатами аудиту
КО - критерії оцінювання

Функції:
ЗІ – збір інформації про стан безпеки ІС
СА – системний аналіз зібраної інформації
ПВК – перевірка на відповідність критеріям безпеки (оцінювання)
ФЗ – формування звіту

Мал. 14.1. Концептуальна модель аудиту кібербезпеки

формацію (СІСБ), яка для аудитора є суб'єктивною(процес 2). Далі аудитор проводить заходи безпосереднього впливу на ІС, включаючи тестування на проникнення (процес 3). За результатами впливу формується та збирається об'єктивна інформація про стан безпеки (ОІСБ, процес 4). Потім послідовно здійснюються системний аналіз цієї інформації, її

перевірка на відповідність критеріям аудиту (тобто, оцінювання) та формування звіту.

Висновки за розділом 14

- **Аудит** (у вузькому сенсі) - це перевірка даних бухгалтерського обліку і показників фінансової звітності суб'єкта господарювання з метою висловлення незалежної думки аудитора про її достовірність в усіх суттєвих аспектах та відповідність вимогам нормативним актам.
- **Аудит** (у загальному сенсі) - це незалежна діяльність з метою формування *об'єктивної оцінки* про стан особи, організації, системи, процесів, підприємства, проекту або продукту.
- **Оцінка** - інформація про значення властивостей об'єкта.
- **Оцінювання** – процес формування інформації про значення *властивостей* об'єкту (тобто, формування оцінки).
- **Об'єктивна оцінка** – оцінка, що отримана у процесі вимірювання (порівняння) якогось об'єкту з відомим зразком.
- **Суб'єктивна оцінка** - це оцінка, що отримана в ході розумового процесу суб'єкта оцінювання на основі його особистого сприйняття і досвіду.
- **Експертна оцінка** – суб'єктивна оцінка, яка виражена експертом (досвідченим спеціалістом у відповідної галузі).
- **Кількісна оцінка** – оцінка, яка виражена за допомогою чисел.
- **Якісна оцінка** - оцінка, яка виражена словами.
- **Критерії оцінювання** – перелік ознак, за якими визначаються значення властивостей об'єкту.
- **Інформаційна технологія** – процес обробки інформації за допомогою комп'ютерних засобів.
- **Ефективність** – це параметр, що відображає відношення результату до показника витрат.

• **Аудит інформаційних технологій (IT аудит) –** процес формування об'єктивної оцінки про ефективність використання інформаційних технологій в бізнес-процесах організації.

• **Аудит безпеки інформації** – це процес формування об'єктивної оцінки про реальний стан безпеки інформації в організації та її ефективності.

• **Аудит кібербезпеки** - процес формування об'єктивної оцінки про реальний стан кібербезпеки в організації та її ефективності.

• Інформаційні процеси а*удиту кібербезпеки*: 1) збір достовірної інформації про стан безпеки ІС шляхом безпосереднього впливу аудитора, включаючи тестування на проникнення; 2) системний аналіз зібраної інформації; 3) перевірка результатів аналізу на відповідність критеріям безпеки (оцінювання); 4) формування звіту.

Контрольні питання та завдання

1. Аудит (у загальному сенсі)?
2. Оцінка, оцінювання?
3. Об'єктивна оцінка, суб'єктивна оцінка?
4. Аудит інформаційних технологій (IT аудит)?
5. Аудит безпеки інформації?
6. Аудит кібербезпеки?
7. Концепція аудиту кібербезпеки?
8. Інформаційні процеси аудиту кібербезпеки?
9. Визначте характеристики мережі інформаційної системи, які можуть бути перевірені в рамках тестування на проникнення.
10. Визначте засоби тестування на проникнення.

Інформаційні джерела

1. Закон України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017 № 2163-VIII.
2. Daniel, Schatz,; Rabih, Bashroush,; Julie, Wall, "Towards a More Representative Definition of Cyber Security", Journal of Digital Forensics, Security and Law, vol. 12(2), ISSN 1558-7215. *Archived* from the original on 28 December 2017. [Online]. Available: https://commons.erau.edu/jdfsl/vol12/iss2/8/ .
3. ISO/IEC 27032:2012. Information technology - Security techniques - Guidelines for cybersecurity.
4. Дубов Д.В. *Кіберпростір як новий вимір геополітичного суперництва: монографія.* Київ, Україна: НІСД, 2014, - 328с. [Електронна версія]. Доступно:
5. Закон України “Про захист інформації в інформаційно-комунікаційних системах” від 05.07.1994 № 80/94-ВР.
6. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
7. НД ТЗІ 1.1-003-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

9. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах. Затверджено постановою Кабінету Міністрів України від 29 березня 2006 р. N 373.
10. "Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури". Затверджено постановою Кабінету Міністрів України від 19 червня 2019 р. № 518.
11. Закон України "Про критичну інфраструктуру", від 16 листопада 2021 року № 1882-IX.
12. Яковів І. Б. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. Збірник наукових праць "Інформаційні технології і безпека". Том 5, № 2. К.: ІССЗІ, 2017.
13. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.
14. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
15. Методичні рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601.
16. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518.
17. Настанова для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity, далі - NIST CSF), видано у 2014 році та оновлен у 2018 році Національним

інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology). https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf
18. ДСТУ ISO/IEC TS 27110:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанови щодо розроблення інфраструктури кібербезпеки (ISO/IEC TS 27110:2021, IDT).
19. Gerard Johansen. Digital Forensics and Incident Response. An intelligent way to respond to attacks. Published by Packt Publishing Ltd. Livery Place 35 Livery Street Birmingham B3 2PB, UK, 2017.
20. What is threat intelligence? IBM. 2023. [Online]. Available: https://www.ibm.com/topics/threat-intelligence
21. NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing, 2016. [Online]. Available: https:/nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
22. What is Threat Intelligence? VMware by Broadcom. 2023. [Online]. Available: https://www.vmware.com/topics/glossary/content/threat-intelligence.html
23. Blake E. Strom Andy Applebaum Doug P. Miller Kathryn C. Nickels Adam G. Pennington Cody B. Thomas. MITRE ATT&CK: Design and Philosophy. The MITRE Corporation. 2020.
24. Яковів І.Б. Кібернетична модель APT атаки. *Information Technology and Security*, vol. 6, №2 (2018), pp. 46-58, Kyiv, Ukraine, 2018. [Online]. Available: http://its.iszzi.kpi.ua/article/view/153140/152522/.
25. Ігор Яковів, Андрій Трохименко, Кирило Глум. Спосіб визначення каналу керування APT-атакою. Information Technology and Security, vol. 10, №2 (2021), pp. 176-188, 2021. DOI10.20535/2411-1031.2021.9.2.249899

26. Методичні рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами, затверджені наказом Адміністрації Держспецзв'язку від 29.05.2021 № 463.
27. NIST Special Publication 800-82. Revision 2. Guide to Industrial Control Systems (ICS) Security. U.S. Department of Commerce. National Institute of Standards and Technology. May 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Електронне мережеве навчальне видання

Ігор ЯКОВІВ

СИСТЕМНІ ОСНОВИ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА НАЦІОНАЛЬНИХ ЕЛЕКТРОННИХ РЕСУРСІВ

Навчальний посібник

Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
вул. Верхньоключова, 4, м. Київ, Україна
Тел. 454-91-51

В навчальному посібнику за допомогою атрибутивно-трансфертного підходу до природи інформації розглянуто системні основи забезпечення кібербезпеки інформаційних технологій та національного сегменту електронних ресурсів. Посібник знайомить курсантів з нормативно-правовими та організаційно-технічними аспектами кіберзахисту інформаційно-комунікаційних систем, особливостями складу, структури і функціонування Національної системи кібербезпеки та Національної системи захисту критичної інфраструктури. Окремі розділи знайомлять з принципами формування інфраструктури кіберзахисту та її застосування для проактивної протидії APT атакам, проведення розвідки кіберзагроз і аудиту кібербезпеки.

Навчальний посібник призначений здобувачам вищої освіти за спеціальностями 122 Комп'ютерні науки і 172 Електронні комунікації та радіотехніка. Також він може бути корисним для здобувачів за спспеціальностями 125 Кібербезпека та захист інформації та 126 Інформаційні системи і технології

УДК 004.056.5 (075.8)

В авторської редакції
Обсяг 11,3 авт. арк.

Видано
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
проспект Берестейський, 37, м. Київ, 03056
https://kpi.ua

Свідоцтво про внесення до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 5354 від 25.05.2017 р.