# ТЕМА 8. КОНВЕНЦІЙНІ ЗЛОЧИНИ. КІБЕРЗЛОЧИНІСТЬ

**План:**

1. Конвенційний злочин як явище міжнародного права.
2. Кіберзлочинність
3. Характеристика кіберзлочину. Санкції

Функціонування та взаємодія галузевих принципів міжнародного кримінального права «подвійної кримінальності» та «переслідування особи лише за злочини, закріплені у міжнародних договорах» наголошують на існуванні специфічного явища, яке зумовлює міжнародне співробітництво. У науковій літературі його характеризують поняттями «злочин міжнародного характеру» або «конвенційний злочин». Беззаперечно, назва явища зазвичай залежала від того, які наслідки для суб'єктів міжнародного права породжували протиправні діяння індивіда. Кримінальному праву відомі декілька моделей протиправної поведінки фізичної особи, яка може бути підставою для взаємодії держав. А саме:

1. Злочин скоєно на території однієї держави, а правопорушник чи докази перебувають на території іншої.

2. Злочинну поведінку розпочато на території однієї держави, а завершено – на території іншої.

3. Злочин вчинено іноземцем на території однієї держави проти громадян, майна чи інтересів третьої держави тощо.

В усіх наведених випадках для належного переслідування та покарання особи необхідно застосовувати єдині підходи з боку договірних сторін. Тому державам украй важливо використовувати однотипні моделі правових явищ, які можливі лише у випадку спорідненості чи схожості їх національного карного законодавства, або є наслідком додаткових домовленостей та погоджень сторін щодо переслідування правопорушників.

Видається, що для цілей міжнародного співробітництва у протидії злочинності термін «конвенційний злочин» є доволі вдалим та універсальним, оскільки його конструкція вже містить характеристику протиправності поведінки (діяння) правопорушника та факт криміналізації її різними державами із використанням механізмів міжнародного співробітництва.

Розмежування міжнародних злочинів та злочинів міжнародного характеру (конвенційних злочинів) отримало загальне визнання. У західній науці виокремлюють crimes under international law та **crimes against international law**[1]. Міжнародні документи також вживають термін «найсерйозніші злочини, що викликають занепокоєння всієї міжнародної спільноти».

Суть конвенційного злочину як стандарту протиправної поведінки розкривається через галузевий принцип подвійної кримінальності у

[1] Теорія та практика міжнародного кримінального права : підручник / заза ред. проф. Зелінської Н. А. Одеса, 2017. 582 с. С. 128.

міжнародному кримінальному праві. Сторони розглядають поведінку фізичної особи у повному її обсязі як протиправну, заборонену і карану. Склад злочину в обох випадках теж збігається, практично збігається і санкція, визначена державами за вчинене. Лише за наявності цих умов буде збігатися і застосовуване державами переслідування правопорушника. Тобто відмінності у підходах до переслідування та покарання індивіда з боку однієї чи іншої держави не буде, а наближеність розміру санкції повністю захистить інтереси обох сторін.

Формування стандартів конвенційних злочинів здійснюється зазвичай шляхом узгодження єдиного переліку протиправних дій, застосування універсальної термінології та узгодження однотипних санкцій в національному законодавстві сторін. Вважаємо, що поєднання цих складових забезпечує міжнародний (транснаціональний, конвенційний) характер конкретного злочину. Основні принципи міжнародного права є імперативними нормами і володіють вищою юридичною силою. Видозмінити зміст міжнародних зобов'язань допустимо лише прийняттям норми аналогічної юридичної сили. На цьому наголошує ст. 64 Віденської конвенції про право міжнародних договорів 1969 р[2]. Видається, що така процедура тривала у 1975 р., коли у Заключному акті НБСЄ було кодифіковано принцип: «повага прав людини та основних свобод, включаючи свободу думки, совісті, релігії та переконань»[3].

Основні принципи міжнародного права володіють вищою юридичною силою і є обов'язковими для всіх держав. Можливість існування відповідних норм передбачено ст. 43 Віденської конвенції про право міжнародних договорів 1969 р. Ця стаття має назву «Зобов'язання, які володіють силою на основі міжнародного права, незалежно від договору»[4]. Зміст вимог, визначених цією статтею, передбачає необхідність виконання будь-якого зобов'язання, яке виникає із загальновизнаних норм, передбаченими іншими міжнародними договорами та міжнародними звичаями, незалежно від положень укладеного договору. Такі норми в документі отримали назву «імперативні норми загального міжнародного права (jus cogens)». Їх статус і місце в системі норм міжнародного права визначено ст. 53 названої конвенції. Договори, які в момент укладення суперечать імперативній нормі загального міжнародного права, не мають юридичної сили[5].

Система конвенційних злочинів у міжнародному праві має практичне значення у сенсі формування уявлень про такі злочини. Науковці зазвичай групують окремі склади злочинів з огляду на зміст міжнародних зобов'язань суб'єктів міжнародного права щодо вжиття заходів для попередження протиправної поведінки чи ліквідації або локалізації її негативних наслідків.

---

[2] Віденська конвенція про право міжнародних договорів. URL: https:// zakon.rada.gov.ua/laws/show/995_118#Text

[3] Заключний акт НБСЄ в Хельсінкі. URL: http://kimo.univ.kiev.ua/MVZP/75. htm

[4] Віденська конвенція про право міжнародних договорів. URL: https:// zakon.rada.gov.ua/laws/show/995_118#Text

[5] Там само

Крім того, з огляду на чітку структуру національного кримінального законодавства, групування конвенційних за чітко визначеними критеріями дає можливість державам краще розуміти сферу протиправних посягань та адаптувати зміст кримінально-правових норм до вимог своїх міжнародних зобов'язань. Отже, формування міжнародно-правових норм, які відображають ознаки злочинів, і поєднання їх за визначеними критеріями дасть змогу більш повно співвіднести ці норми із нормами національного кримінального законодавства.

Зазвичай для універсалізації злочинних діянь використовуються правові конструкції, напрацьовані у багатосторонніх міжнародних договорах. Міжнародно-правові норми, які характеризують подібні або суміжні конвенційні злочини, групують за різними критеріями, зокрема: за об'єктом посягань, суспільною небезпекою, складністю поведінки тощо.

Першою ознакою, за якою об'єднують конвенційні злочини, є їх підвищена суспільна небезпека. На користь такого твердження виступають: значна вразливість національного і міжнародного співтовариства від окремих видів злочинної діяльності, обмежені можливості держав і міжнародного співтовариств щодо попередження, контролю і протидії такими злочинами, а також істотний обсяг і великий розмір шкоди, завданої суспільству і людству загалом. Суспільна небезпека конвенційних злочинів насамперед дає можливість виокремити їх із середовища інших злочинів, передбачених національним карним законодавством.

Залежно від об'єкта посягання та ступеня міжнародної небезпеки конвенційні злочини поділяють на такі групи:

1. Конвенційні злочини, які посягають на нормальне здійснення міжнародних відносин.

2. Конвенційні злочини, які посягають на нормальне здійснення міжнародних економічних відносин.

3. Конвенційні злочини, які посягають на особу, майнові та інші права, моральні устої суспільства тощо.

4. Конвенційні злочини, які передбачені спеціальними конвенціями. Проаналізуємо підстави та причини поєднання різних протиправних дій, а також стан імплементації їх у положення Кримінального кодексу України 2001 р. встановлення кримінальної відповідальності за конвенційні злочини.

## 2. Кіберзлочинність

***Кіберзлочинність*** - це глобальне явище, яке стосується всіх держав, і воно так само безмежне, як і сам інтернет.

Згідно з останньою оцінкою загроз організованої злочинності в інтернеті (IOCTA), кіберзлочинність стає все більш агресивною та конфротаційною. Це можна побачити в різних формах кіберзлочинності, включаючи злочини у сфері високих технологій, витік даних та сексуальне здирство.

**Кіберзлочинністю** є будь-яка злочинна активність у віртуальному просторі (кіберпросторі). У деяких кіберзлочинах здійснюються прямі атаки

на комп'ютери або інші пристрої для виведення їх з ладу. В інших кіберзлочинах комп'ютери використовуються кіберзлочинцями для поширення шкідливих програмних кодів, отримання незаконної інформації, розкрадання особистих даних з метою шахрайства. Отже**, кіберзлочини** - це злочини, скоєні в кіберпросторі (з використанням мережі інтернет чи іншої комп'ютерної мережі), як компонент злочину. До таких злочинів належать: використання ботнетів - мереж пристроїв, заражених шкідливими програмами без відома їх користувачів - для передачі вірусів, які незаконно отримують віддалений контроль над пристроями, крадуть паролі та відключають антивірусний захист; створення «чорних ходів» на скомпрометованих пристроях для крадіжки грошей та даних або віддалений доступ до пристроїв для створення ботнетів; створення онлайн-форумів обміну хакерським досвідом; абузостійкий хостинг та створення противірусних сервісів; відмивання традиційних та віртуальних валют; здійснення онлайн-шахрайства, наприклад через системи онлайн-платежів, кардинг та соціальну інженерію; різні форми сексуальної експлуатації дітей в інтер-неті, включаючи поширення в інтернеті матеріалів про сексуальне насильство над дітьми та прямі трансляції сексуального насильства над дітьми; онлайн-хостинг операцій із продажу зброї, фальшивих паспортів, підроблених та клонованих кредитних карток, наркотиків, а також хакерські послуги'

Питання правового регулювання інформаційного простору, захисту осіб у кіберпросторі, протидії злочинам, які скоюються з використанням можливостей кіберпростору тощо є обговорюваними як на універсальному, так і на регіональному міжнародному рівні. Зокрема, у межах ООН вони є в центрі уваги головних органів організації, інституцій, спеціалізованих організацій, установ, форумів, які діють під егідою організації (Генеральна Асамблея, Економічна і Соціальна Рада, Комісія із запобігання злочинності і кримінального правосуддя, конгреси ООН із запобігання злочинності і кримінального правосуддя, Міжнародний союз електрозв'язку (МСЕ), Організація Об'єднаних Націй із питань освіти, науки і культури (ЮНЕСКО), Конференція ООН із торгівлі і розвитку (ЮНКТАД), Управління ООН із наркотиків і злочинності (ЮНОДК), Інтерпол тощо), які акцентують увагу на тому, що кіберзлочинність є одним із нових політичних питань у сфері запобігання злочинності і кримінального правосудля, яке потребує розроблення шляхів і засобів його вирішення.

ООН ще в 1994 р. опублікувала Керівництво із запобігання злочинності, пов'язаній із застосуванням комп'ютерів, і боротьби з нею, у якому зазначалось, що «потенційна сфера охоплення комп'ютерної злочинності така ж широка, як і сфера охоплення міжнародних телекомунікаційних систем». Хоча в Керівництві слово «інтернет» згадується одноразово, а термін «кіберзлочинність» взагалі не використовується, висновки, які воно містить, є далекоглядними. Основну увагу приділено поняттю «комп'ютерний злочин», формулюванню терміна «кіберзлочинність». Рішучість щодо прийняття заходів задля того, щоб усі могли користуватися благами нових технологій, особливо інформаційних і комунікаційних, відповідно до рекомендацій,

зазначених у Декларації міністрів на сесії ЕКОСОР 2000 р., була висловлена Декларацією тисячоліття ООН 2000 р. (ст. 20), підтверджена Цілями сталого розвитку ООН (Ціль 9).

Також слід зазначити, що станом на 2023 р. на міжнародному універсальному рівні не було прийнято єдиного акта щодо криміналізації кіберзлочинів. Оскільки в ході злочинної діяльності зловмисники все частіше вдаються до використання електронних систем оброблення даних та впливають на роботу їх, для вирішення цієї проблеми постало питання щодо необхідності розроблення положень кримінального права, і це питання було вирішено на регіональному рівні в межах Ради Європи, яка прийняла Конвенцію про кіберзлочинність 2001 р. (СЄД № 185) - також відому як Будапештська конвенція - для вирішення питання про злочини, вчинені проти і за допомогою електронних мереж. Конвенція стала першим міжнародним договором про злочини, що скоюються через інтернет та інші комп'ютерні мережі, особливо щодо порушень авторських прав, комп'ютерного шахрайства, дитячої порнографії та порушень мережної безпеки. Вона також містить низку функцій та процедур, таких як пошук комп'ютерних мереж та перехоплення. Основну мету договору викладено у преамбулі, і вона полягає у проведенні загальної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, особливо шляхом ухвалення відповідного законодавства та розвитку міжнародного співробітництва.

Конвенцію спрямовано головним чином на гармонізацію елементів внутрішнього кримінального матеріального права щодо правопорушень та пов'язаних із ними положень у сфері кіберзлочинності; надання внутрішньодержавним кримінально-процесуальним законам повноважень, необхідних для розслідування та судового переслідування таких злочинів, а також інших злочинів, скоєних за допомогою комп'ютерної системи або пов'язаних із використанням електронних доказів інших злочинів; встановлення швидкого та ефективного режиму міжнародного співробітництва.

Застосовуючи Конвенцію (СЄД № 185), сторони дотримуються обов'язків урядів захищати людей від злочинів, скоєних онлайн або офлайн шляхом ефективного кримінального розслідування та судового переслідування. Деякі сторони Конвенції вважають, що вони пов'язані міжнародним зобов'язанням надавати засоби захисту від злочинів, скоєних за допомогою комп'ютерної системи із посиланням на процедури та повноваження для кримінальних розслідувань або розглядів, які сторони повинні встановити відповідно до Конвенції.

Конвенцію відкрито для приєднання державами, які не є членами Ради Європи.

Конвенція про кіберзлочинність є найвпливовішою міжнародною угодою, що регулює питання порушення закону через інтернет або інші інформаційні мережі. Вона вимагає від сторін модернізувати і гармонізувати своє кримінальне законодавство проти дій хакерів та інших порушень безпеки, включаючи порушення авторських прав, шахрайство за допомогою

комп'ютера, дитячу порнографію та іншу протиправну кібердіяльність. Ковенція також передбачає процесуальні повноваження, що охоплюють обшук комп'ютерних мереж і перехоплення комунікацій у контексті боротьби з кіберзлочинністю. Нарешті, вона створює можливості для ефективного міжнародного співробітництва. Хоча Конвенція насправді не є інструментом забезпечення захисту персональних даних, вона криміналізує діяльність, яка може порушувати право суб'єкта даних на захист своїх даних. Вона також зобов'язує договірні сторони передбачити при виконанні Конвенції адекватний рівень захисту прав і свобод людини, у тому числі прав, гарантованих Конвенцією про захист прав людини і основоположних свобод 1950 р., як право на захист персональних даних.

Додатковий протокол до Конвенції про злочини у сфері комп'ютерної інформації, про інкримінування расистських актів та скоєного ксенофобу за допомогою інформаційних систем (СЄД № 189) 2003 р. розширює сферу дії Конвенції про кіберзлочинність, включаючи її суттєві, процедурні та присвячені міжнародному співробітництву положення, охоплюючи також правопорушення, пов'язані з расистською та ксенофобською пропагандою. Таким чином, крім гармонізації суттєвих правових аспектів такої поведінки, Протокол спрямовано на розширення можливостей сторін щодо використання коштів і напрямків міжнародного співробітництва, викладених у Конвенції (СЄД № 185) у цій галузі.

У 2021 р. розроблено Другий Додатковий протокол до Конвенції про кіберзлочинність щодо розширення співпраці та розкриття електронних доказів. Протокол спрямовано на подальше зміцнення співпраці у боротьбі з кіберзлочинністю та розширення можливостей органів кримінального правосуддя щодо збирання доказів в електронній формі про кримінальний злочин для цілей конкретних кримінальних розслідувань або розглядів за допомогою додаткових інструментів, що стосуються більш ефективної взаємодії та інших форм співробітництва між компетентними органами; співробітництво у надзвичайних ситуаціях (тобто у ситуаціях, коли існує значний та безпосередній ризик для життя або безпеки будь-якої фізичної особи); та пряме співробітництво між компетентними органами і постачальниками послуг та іншими суб'єктами, які володіють відповідною інформацією або контролюють її. Таким чином, мета Протоколу полягає в тому, щоб доповнити Конвенцію та, у відносинах між сторонами, Перший Протокол.

Протокол містить такі розділи: 1. Загальні положення. II. Заходи щодо розширення співпраці. III. Умови та гарантії. IV. Заключні положення.

Загальні положення глави I охоплюють мету та сферу застосування Протоколу. Як і у випадку з Конвенцією, Протокол стосується конкретних кримінальних розслідувань або судових розглядів не лише щодо кіберзлочинів, а й щодо будь-яких кримінальних злочинів, пов'язаних із доказами в електронній формі, які також називаються «електронними доказами» або «цифровими доказами». У цьому розділі наводяться визначення Конвенції, що застосовуються до Протоколу, і містяться додаткові визначення

термінів, які часто використовуються у Протоколі. Крім того, ураховуючи, що мовні вимоги для взаємної допомоги та інших форм співпраці часто знижують ефективність процедур, було додано статтю про мову, щоб забезпечити більш прагматичний підхід у цьому відношенні. Глава II містить основні статті Протоколу, які описують різні методи співробітництва, доступні сторонам. До кожного типу співробітництва застосовують різні принципи. Глава III передбачає умови та гарантії. Крім того, цей розділ включає докладний перелік заходів для захисту персональних даних

Негативною ознакою сьогодення стало використання ІКТ у скоєнні терористичних злочинів. У 2015 р. ПАРЄ прийняла рекомендацію № 2070 щодо зміцнення співробітництва у протиборстві з кібертероризмом та іншими масовими атаками в мережі інтернет. Рекомендація підкреслює значення Ради Європи у вирішенні глобального виклику, пов'язаного з безпекою комп'ютерних мереж у зв'язку з появою кібертероризму та інших масових атак, що діють на/через комп'ютерні системи, являючи собою серйозну загрозу національній безпеці, громадській безпеці та добробуту країн.

Кіберзлочинність також є одним із пріоритетів ЄС у боротьбі з серйозною та організованою злочинністю в рамках EMPACT 2022-2025.

Кіберзлочинність - проблема, що зростає, для таких країн, як держави - члени ЄС, у більшості яких добре розвинено інтернет-інфраструктуру і платіжні системи знаходяться в режим онлайн. Але не лише фінансові дані, а й дані загалом є ключовою мішенню для кіберзлочинців. Кількість та частота витоків даних зростають, що, своєю чергою, призводить до збільшення кількості випадків шахрайства та здирництва. Європейський Союз доклав зусиль до узгодження законодавства щодо кіберзлочинності, яке діє на території держав-членів, зокрема: Директива № 2000/31/ЄС Європейського парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, таких як електронна торгівля на внутрішньому ринку; Повідомлення Європейського парламенту, Ради та Комітету регіонів: Загальна політика боротьби з кіберзлочинністю (COM(2007) 267 final від 22 травня 2007 р.); Директива 2011/93/ЄС Європейського парламенту та Ради від 13 грудня 2011 р. про боротьбу із сексуальним насильством та сексуальною експлуатацією дітей та дитячою порнографією, яка замінює Рамкове рішення Ради 2004/68/JHA, Повідомлення Комісії Раді та Європейському парламенту: Боротьба зі злочинністю в наш цифровий вік: створення Європейського центру кіберзлочинності (COM(2012) 140 final від 28 березня 2012 р.); Директива 2013/40/ЄС Європейського парламенту та Ради від 12 серпня 2013 р. про атаки на інформаційні системи, яка замінює Рамкове рішення Ради 2005/222/JHA, Директива (ЄС) 2016/1148 - кібербезпека мереж та інформаційних систем; Рішення (CFSP) 2019/797 - обмежувальні заходи проти кібератак, що загрожують ЄС або його державам-членам; Регламент (ЄС) 2019/796 - обмежувальні заходи проти кібератак, що загрожують ЄС або його державам-членам; Стратегія Союзу безпеки ЄС 2020 р., Регламент (ЄС) 2021/1149 про створення Фонду внутрішньої безпеки (спрямований на забезпечення

високого рівня безпеки в Європейському Союзі, зокрема шляхом запобігання та протидії тероризму і ради-калізації, серйозній і організованій злочинності та кіберзлочинності); Регламент (ЄС) 2021/887 про створення Європейського промислового, технологічного та науково-дослідного центру кібербезпеки та мережі національних координаційних центрів. У березні 2022 р. Європейська комісія прийняла нову загальноєвропейську пропозицію щодо Директиви про боротьбу з насильством стосовно жінок і насильством у сім'ї, спрямовану на введення цільових мінімальних правил щодо прав цієї групи жертв злочинів і криміналізації найбільш важких форм насилля стосовно жінок і кібернасилля.

Перш за все слід зазначити, що прийняті в ЄС акти мають за мету унормувати діяльність, пов'язану з використанням ІКТ у різних сферах відносин. Так, Директива № 2000/31/ЄС Європейського парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, таких як електронна торгівля на внутрішньому ринку, встановлює стандартні правила ЄС із різних питань, пов'язаних з електронною торгівлею. Під дію Директиви підпадає широке коло онлайн-послуг, а саме: служби новин (наприклад вебсайти новин, продажі (книги, фінансові послуги, туристичні послуги тощо), реклама, професійні послуги (адвокати, лікарі, агенти з нерухомості), розважальні послуги, основні посередницькі послуги (доступ до інтернету, передача та розміщення інформації), спонсорство тощо.

У ній зазначено, що постачальники онлайн-послуг, які є звичайними постачальниками послуг кешування або хостингу, не несуть відповідальності за інформацію, яку вони передають або розміщують, якщо вони виконують певні умови. Щодо постачальників послуг хостингу: вони звільняються від відповідальності, якщо вони не знали про незаконну діяльність чи інформацію та якщо вони, отримуючи таку інформацію, негайно діють, щоб видалити чи заблокувати доступ до інфо-мації.

Національні уряди не можуть накладати на цих «посередників» будь-яких спільних зобов'язань щодо моніторингу інформації, яку вони надсилають або зберігають, для виявлення незаконної діяльності та запобігання їй.

Директиву 2013/40/ЄС Європейського парламенту та Ради від 12 серпня 2013 р. про атаки на інформаційні системи, яка замінює Рамкове рішення Ради 2005/222/JHA', спрямовано на боротьбу з кіберзлочинністю та забезпечення інформаційної безпеки завдяки суворішому державному законодавству, суворішим кримінальним покаранням та більш тісній співпраці між надмірними податками. Директива запроваджує нові правила, що гармонізують криміналізацію та покарання за низку правопорушень, спрямованих проти інформаційних систем. Ці правила включають заборону використання так званих ботнетів - шкідливого програмного забезпечення, призначеного для віддаленого управління мережею комп'ютерів. Вона також закликає країни ЄС використовувати ті ж контактні точки, які використовуються Радою Європи та Великою вісімкою для швидкого реагування на за-грози, пов'язані з передовими технологіями.

Основними видами кримінальних злочинів, що охоплюються Директивою, є атаки на інформаційні системи, починаючи від атак типу

«відмова в обслуговуванні», призначених для виведення з ладу сервера, і закінчуючи перехопленням даних та атаками ботнетів.

Директива зазначає, що з кіберзлочинністю необхідно ефективно боротися не тільки тоді, коли вона відбувається в конкретній державі-члені, але і коли вона відбувається в інших державах-членах. Це вимагає забезпечення криміналізації тих самих правопорушень у всіх державах-членах; надання правоохоронним органам коштів для дій та співробітництва один з одним. З цією метою Директива вимагає зближення систем кримінального права країн ЄС та розширення співробітництва між судовими органами щодо незаконного доступу до інформаційних систем, незаконного втручання в систему, незаконного втручання в дані, незаконного перехоплення.

У всіх випадках кримінальне діяння має бути здійснено навмисне, Підбурювання, підсобництво, підбурювання та замах на скоєння будь-якого з перелічених вище злочинів також підлягають покаранню.

Обтяжливими обставинами злочину с: скоєння правопорушення злочинною організацією, що завдає значної шкоди або зачіпає суттєві інтереси потерпілих; скоєння незаконного втручання в системи або незаконного втручання в дані шляхом неправомірного використання особистих даних іншої особи з метою завоювання довіри третьої сторони, тим самим завдаючи шкоди законним власникам особистих даних, якщо ці обставини не охоплюються іншим правопорушенням, караним відповідно до національного законодавства.

Директива передбачає запровадження ефективних, пропорційних та стримуючих санкцій, покладає зобов'язання на держави-члени щодо вжиття необхідних заходів для забезпечення того, щоб такі діяння, як незаконний доступ до інформаційних систем, незаконне втручання в систему, незаконне втручання в дані, незаконне перехоплення, засоби, що використовуються для скоєння правопорушень, а також підбурювання, пособництво та підбурювання і спроба скоєння означених злочинів (статті 3-8), каралися ефективними, пропорційними і кримінальними покараннями. Зокрема, встановлено, що за означені злочини, зазначені у статтях 3-7, максимальний строк позбавлення волі має становити не менше двох років, принаймні у випадках, які не є незначними; за незаконне втручання в систему і незаконне втручання в дані, скоєні навмисно, має бути передбачено покарання у вигляді позбавлення полі на максимальний термін не менше трьох років, якщо значну кількість інформаційних систем було порушено за допомогою засобів, розроблених чи адаптованих насамперед для цієї мети; у випадку скоєння ненавмисного втручання в систему, незаконного втручання в дані максимальний строк ув'язнення повинен передбачати не менше ніж п'ять років. якщо їх скоєно я рамках злочинної організації, як це визначено в Рамковому рішенні 2008/841/3НА, незалежно від передбаченого в ньому покарания; вони завдають серйозної шкоди: або вони здійснюються проти критичної інформаційної системи інфраструктури.

Директива також запроваджує відповідальність юридичних осіб та встановлює санкції, які повинні включати кримінальні чи некримінальні штрафи та можуть містити інші санкції, зокрема: виключення з права на одержання суспільної допомоги або допомоги; тимчасове чи постійне позбавлення права займатися комерційною діяльністю; судова ліквідація; тимчасове чи постійне закриття закладів, які використовувалися для скоєння злочину.

Директива передбачає встановлення юрисдикції державами-членами щодо вищеозначених злочинів, якщо злочин було скоєно: повністю або частково на їхній території; або одним з їхніх громадян, принаймні у випадках, коли діяння є правопорушенням там, де його було вчинено. Якщо кілька країн мають юрисдикцію щодо правопорушення, вони мають співпрацювати, щоб вирішити, яка з них буде здійснювати судовий розгляд щодо винної особи.

Рішення (CFSP) 2019/797 - обмежувальні заходи проти кібератак, що загрожують ЄС або його державам-членам, Регламент (ЄС) 2019/796 - обмежувальні заходи проти кібератак, що загрожують ЄС або його державам-членам, запроваджують структуру, яка дозволяє ЄС вводити санкції для стримування та реагування на кібератаки, які становлять зовнішню загрозу для ЄС чи країн ЄС. Ці кібератаки включають атаки на країни, які не є членами ЄС, або міжнародні організації, коли дії вважаються необхідними для досягнення спільних цілей зовнішньої та безпекової політики ЄС.

Ця структура дозволяє ЄС накладати санкції на осіб чи організації, які відповідальні за кібератаки чи спроби кібератак, надають фінансову, технічну чи матеріальну підтримку таким атакам чи беруть участь у них в інший спосіб. Санкції можуть також застосовуватись до пов'язаних із ними осіб або організацій. Обмежувальні заходи включають заборону на в'їзд до ЄС та заморожування активів. На країни ЄС покладено зобов'язання встановлення мір покарання за порушення.

Кібератаки, які підпадають під дію цього режиму санкцій, мають значні наслідки: виникають чи здійснюються за межами ЄС; або з використанням інфраструктури поза ЄС; або здійснюються фізичними чи юридичними особами, що засновані та діють за межами ЄС; або здійснюються за підтримки фізичних чи юридичних осіб, що діють за межами ЄС.

Кібератаки, які становлять загрозу для країн ЄС, включають атаки, що стосуються інформаційних систем, а також: критичної інфраструктури, необхідної для життєдіяльності суспільства чи здоров'я громадян, безпеки, захисту й економічного чи соціального благополуччя; послуг, необхідних для основної соціальної та економічної діяльності, зокрема енергетика, транспорт, банківська справа; фінансів, охорони здоров'я, питної води, цифрової інфраструктури; найважливіших державних

Функцій, зокрема оборони, управління та функціонування інститутів, публічних виборів, економічної та громадянської інфраструктури, внутрішньої безпеки і зовнішніх зв'язків, включаючи дипломатичні місії; зберігання чи оброблення секретної інформації; або урядових аварійно-рятувальних загонів.

Особливу стурбованість ЄС викликають, так звані кіберзалежні злочини - це правопорушення, які можуть бути скоєні лише з використанням комп'ютера, комп'ютерних мереж чи інших форм інформаційно-комунікаційних технологій. До них відносяться такі правопорушення, як шкідливе програмне забезпечення (ПЗ): розроблення та поширення шкідливого ПЗ продовжує залишатися наріжним каменем більшості кіберзлочинів. Шкідливі програми для крадіжки інформації, такі як банківські трояни, як і раніше, становлять серйозну загрозу. Цей тип шкідливих програм зазвичай краде дані користувача, такі як номери кредитних карт і облікові дані для входу, із заражених комп'ютерів для подальшого використання злочинцями в шахрайських цілях.

3 кінця 2013 р. криптопрограми (програми-вимагачі, які використовують шифрування) стали провідним шкідливим програмним забезпеченням з точки зору загрози та впливу. Криптовалютне програмне забезпечення шифрує створені користувачами файли жертв, відмовляючи їм у доступі, якщо жертва не платить за розшифровку своїх файлів.

Наслідуючи тенденції викрадачів інформації, кампанії шифрувального програмного забезпечення все частіше націлені на організації державного та приватного секторів.

**Мережеві атаки** розрізняються за способом дії та метою. Пошкодження вебсайтів - це поширена, але малоефективна атака, яка часто є торговельною маркою груп хактивістів, орієнтованих на урядові або загальнодоступні вебсайти. Мережеві вторгнення, які призводять до незаконного доступу або розкриття особистих даних (витік даних) або інтелектуальної власності, стають дедалі частішими та масштабнішими, при цьому щороку компрометуються сотні мільйонів записів у всьому світі. Скомпрометовані дані можуть використовуватися для різних злочинних цілей, включаючи шахрайство та здирництво, і високо цінуються злочинцями, мотивованими фінансовими міркуваннями.

Деякі держави - члени ЄС наголошують на особливій загрозі, яку інсайдери становлять для безпеки компанії. Будь-який сектор чи мережа, у яких зберігаються дані, які можна монетизувати, є метою таких атак.

**Крадіжка особистих даних**: дані стали ключовим товаром злочинців. Розширення можливостей підключення громадян, підприємств та державного сектору до інтернету, а також кількість підключених пристроїв і датчиків у рамках інтернету речей, що експонентно зростає, відкриють нові можливості для кіберзлочинців. Шкідливе програмне забезпечення, націлене на інтелектуальні пристрої, призведе до нових джерел витоку даних та компрометації мережі, а також до створення нових ботмереж. Ураховуючи простоту входу в кіберзлочинність, використання кіберінструментів та послуг традиційними ОЗУ для покращання або розширення своїх можливостей, імовірно, стане більш поширеним явищем.

Мережеві вторгнення з метою незаконного отримання даних мають серйозні наслідки в усьому світі, призводячи до втрати інтелектуальної власності та компрометації великих обсягів даних, які можуть бути

використані для скоєння подальших злочинів, включаючи шахрайство та здирство.

**Криптовалюта** (здирники, які використовують шифрування) с серйозною загрозою для ЄС, націленою не лише на громадян, а й на організації державного та приватного секторів.

**Шахрайство з платіжними дорученнями**: злочинці використовують шахрайські накази про переведення для обману організацій приватного та державного секторів. Шахраї значною мірою покладаються на методи соціальної інженерії та шкідливе програмне забезпечення для здійснення цього виду шахрайства.

**Шахрайство з платіжними картками** — це діяльність із низьким рівнем ризику та високим прибутком. Скомпрометовані дані картки легко доступні на форумах, торговельних майданчиках і в автоматизованих магазинах карток у глибокій мережі та даркнеті. Злочинці використовують шахрайські накази про переведення для обману організацій приватного та державного секторів. Шахраї значною мірою покладаються на методи соціальної інженерії та шкідливе програмне забезпечення для здійснення цього виду шахрайства.

**Сексуальна експлуатація дітей в інтернеті (CSE):** матеріали для сексуальної експлуатації дітей (CSEM) усе частіше використовуються для отримання фінансової вигоди. Зростаюча кількість форумів даркнету, що полегшують обмін CSEM, у поєднанні з простотою доступу до цих мереж призводить до збільшення обсягу матеріалів, якими обмінюються через даркнет. Примус та сексуальне насильство все частіше використовуються для віктимізації дітей. Правопорушники використовують ці методи для отримання додаткових матеріалів щодо жорстокого поводження з дітьми, для отримання фінансової вигоди або фізичного доступу до жертви.

Слід констатувати, що, крім дій, запроваджених на міжнародному універсльному рівні, на рівні європейських регіональних організацій -

Ради Європи, ЄС, в останні роки в різних регіонах світу було застосовано низку організаційно-правових підходів щодо боротьби з кіберзлочинністю. Так, прийняту в 2010 р. Арабську конвенцію про боротьбу зі злочинами, пов’язаними з технологіями, спрямовано на покращання співпраці між арабськими державами в боротьбі з правопорушеннями у сфері інформаційних технологій для захисту безпеки та інтересів арабських держав, а також безпеки їхніх спільної і окремих осіб. Договір містить визначення злочинів, пов’язаних із використанням інформаційних технологій, процесуальні положення та механізми правової і судової співпраці між державами-учасницями в цій сфері.

Конвенцію Африканського Союзу про кібероезпеку та захист особистих даних 2014 р. спрямовано на створення законодавчої бази для кібербезпеки та захисту персональних даних. Договір покладає на держави-учасниці зобов’язання щодо розроблення національної політики кібербезпеки та відповідного інституційного механізму управління; розроблення законодавства та створення інститутів у сфері протидії кіберзлочинності;

забезпечення моніторингу та реагування на інциденти і попередження; здійснення національної і транскордонної координації та глобальної співпраці.

Угода про співпрацю держав - учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації 2001 р. передбачає співпрацю сторін з метою забезпечення ефективного запобігання злочинам у сфері комп'ютерної інформації, виявлення, припинення, розкриття та розслідування їх; встановлює перелік кримінальних діянь; визначає компетентні органи, на які покладається співробітництво в цій сфері; визначає форми співробітництва; окреслює шляхи вирішення спірних питань сторонами щодо тлумачення або застосування положень Угоди

Юрисдикцією щодо означених злочинів наділено держави - учасниці відповідних угод.

### 3. Характеристика кіберзлочину. Санкції

Відповідно до міжнародного кримінального права кіберзлочини віднесено до окремого виду міжнародних правопорушень. Кіберзлочини е складними не лише за своїми юридичними ознаками, але й томя, що вони часто мають транснаціональний характер, тобто це діяння, ініціювання, запобігання чи наслідки яких зачіпають більш ніж одну країну, і вони мають багатонаціональний характер. Крім того, вони є видом професійної діяльності організованих злочинних груп.

Кіберзлочини охоплюють широкий спектр об'єктів посягання. Вони послаблюють економіку держав, впливаючи (прямо і опосеред-ковано) на економічні витрати урядів і тягнуть за собою кримінальну діяльність, яка може загрожувати стабільності держав, особливо у випадку поєднання з транснаціональною злочинністю, включаючи відмивання грошей, контрабанду зброї, торгівлю наркотичними речовинами. Крім того, вони посягають на права і свободи людини (крадіжка особистих даних фізичних осіб, насилля щодо неповнолітніх).

Об'єктивна сторона злочину полягає в умисних діях, направлених на виконання протиправних дій. Кіберзлочинність включає незаконне проникнення, крадіжку і заподіяння шкоди; незаконний доступ до особистих даних та інформації шляхом зламування комп'ютера; здійснення незаконного контролю над майном та інформацією жертв, позбавляючи жертви їхніх особистих даних, тощо.

Однією з основних складових кіберзлочинів є неправомірне використання інструментів та програмного забезпечення. Кіберзлочинці використовують електронну пошту, шпигунське ПЗ та троянских коней з кейлогтерами та фішинговими електронними листами з метою зламування комп'ютера та отримання особистих даних. Вони використовують законні інструменти, такі як кейлоггери та інструменти віддаленого доступу, які було розроблено для доступу до систем із метою ремонту, а не для доступу та крадіжки інформації. Кейлоггери було створено, щоб корпорації могли контролювати своїх співробітників в інтернеті, але кіберзлочинці

використовують їх для відстеження активності в інтернеті та отримання інформації. Кіберзлочинці користуються перевагами технологій, аж до використання мікрофонів та камер на особистих комп'ютерах, щоб спостерігати за потерпілими (жертва-ми) та стежити за комп'ютерною активністю.

Ще одним компонентом кіберзлочину є видача себе за іншу особу.

Злочинці ховаються за підробленими рекламними акціями, такими як форми для конкурсів, купони, безкоштовні роздачі та ваучери, щоб спробувати змусити людей відмовитися від своєї особистої інформації.

Вони намагаються змусити людину почуватися в безпеці, сказавши, що її інформацію не буде передано третім особам. Кіберзлочинці також знають, як створювати законні електронні листи, щоб видавати себе за такі установи, як банки. Вони отримують доступ до особистої ін-формації, наприклад, попросивши особу підтвердити пароль або номер рахунку в онлайн-банку під приводом наявності проблеми з обліковим записом в інтернеті, для вирішення якого особа повинна увійти до системи.

Суб'єктом злочину є фізична, винна, осудна особа, яка досягла віку кримінальної відповідальності, передбаченого законодавством держав.

Суб'єктом може бути визнано і юридичну особу. Крім того, суб'єктом відповідальності може бути визнано й злочинну організацію, під якою, відповідно до Рамкового рішення Ради 2008/841/ЈНА від 24 жовтня 2008 р. щодо боротьби з організованою злочинністю', слід розуміти структуроване об'єднання, створене протягом певного періоду часу, що складається з більш ніж двох осіб, які діють спільно з метою ско-ення злочинів, караних позбавленням волі або ув'язненням на строк не менше чотирьох років або більш серйозним покаранням для отримання, прямо або побічно, фінансової чи іншої матеріальної вигоди.

Слід зазначити, що скоєння злочину злочинною організацією, що має наслідком завдання значної шкоди, кваліфікується як обтяжлива обставина (наприклад Директива 2013/40/ЄС Європейського парламенту та Ради від 12 серпня 2013 р. про атаки на інформаційні системи, яка замінює Рамкове рішення Ради 2005/222/ЈНА).

Злочин може бути скоєно у співучасті. Підбурювання, пособництво, підбурювання та замах на скоєння будь-якого з кіберзлочинів також визнаються правопорушеннями і підлягають покаранню.

Суб'єктивна сторона характеризується навмисною формою вини.

*Санкції.* Міжнародні акти з протидії кіберзлочинності, як і більшість договорів, що криміналізують протиправні діяння, не передбачають конкретних мір покарання за скоєння означеного протиправного діяння і покладають це зобов'язання на держави-учасниці, які мають встановити відповідні кримінальні та некримінальні санкції за такі злочини з урахуванням тяжкості їхнього характеру, акцентуючи увагу на відшкодуванні шкоди, заподіяної злочином. Виключення становлять законодавчі акти ЄС, якими передбачено конкретні міри покарання за скоєння злочину (наприклад Директива 2013/40/ЄС Європейського парламенту та Ради від 12 серпня 2013

р. про атаки на інформаційні системи, яка замінює Рамкове рішення Ради 2005/222/ЈНА, диференціює строки покарання залежно від виду злочину, наявності обтяжливих обставин, скоєння злочину організованою групою).