МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ЗАПОБІГАННЯ І ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: КРАЩІ МІЖНАРОДНІ ПРАКТИКИ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ В УКРАЇНІ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Алла ПОСВЯЩЕННА

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувачка вищої освіти гр. УБДМ 61
Алла ПОСВЯЩЕННА

Керівник:
к. держ. упр., доц Тетяна МУЖАНОВА

Рецензент:

_____

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачці Посвященній Аллі В'ячеславівні
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "ЗАПОБІГАННЯ І ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: КРАЩІ МІЖНАРОДНІ ПРАКТИКИ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ В УКРАЇНІ"

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к. держ. упр., доц.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. № 145.

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р.
3. Вихідні дані до кваліфікаційної роботи: кібербезпека, кіберзлочинність, запобігання і протидія кіберзлочинності, кращі міжнародні практики і досвід України щодо подолання кіберзлочинності.
4. Перелік питань, які потрібно розробити:
   1. З'ясувати характеристики кіберзлочинності як однієї з основних загроз кібербезпеці.
   2. Проаналізувати нормативно-правове забезпечення кібербезпеки і подолання кіберзлочинності в ЄС.
   3. Дослідити засади запобігання та протидії кіберзлочинності в Україні на основі міжнародного досвіду.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Вивчення характеристик кіберзлочинності як однієї з основних загроз кібербезпеці.	27.10.2023	
4.	Аналіз нормативно-правового забезпечення кібербезпеки і подолання кіберзлочинності в ЄС.	10.11.2023	
5.	Дослідження засад запобігання та протидії кіберзлочинності в Україні на основі міжнародного досвіду.	15.11.2023	
6.	Формулювання висновків за результатами дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	.01.2024	

Здобувачка вищої освіти _____ Алла ПОСВЯЩЕННА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувачка Посвященна А.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "ЗАПОБІГАННЯ І ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: КРАЩІ МІЖНАРОДНІ ПРАКТИКИ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ В УКРАЇНІ"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка **ПОСВЯЩЕННА Алла** у кваліфікаційній роботі з'ясувала характеристики кіберзлочинності як однієї з основних загроз кібербезпеці; проаналізувала нормативно-правове забезпечення кібербезпеки і подолання кіберзлочинності в ЄС; дослідила засади запобігання та протидії кіберзлочинності в Україні на основі міжнародного досвіду. **ПОСВЯЩЕННА Алла** показала хороші теоретичні та практичні знання, вміння проводити наукове дослідження і самостійно вирішувати наукові завдання, проявила аналітичні навички у процесі вивчення нормативно-правового та інституційного забезпечення ЄС та України. Результати дослідження апробовані на Всеукраїнській науково-практичній конференції "Актуальні проблеми кібербезпеки" 2023 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувачки **ПОСВЯЩЕННОЇ Алли** на позитивну оцінку та присвоїти їй кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Посвященна А.В. допускається до захисту даної роботи в Державній екзаменаційній комісії.

Завідувач кафедри
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

Здобувачки вищої освіти Посвященної Алли В'ячеславівни
На тему: ЗАПОБІГАННЯ І ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: КРАЩІ МІЖНАРОДНІ ПРАКТИКИ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ В УКРАЇНІ

Актуальність: Стрімкий розвиток ІТ, цифровізація, створення глобального кіберпростору сформували принципово нові реалії, які мають невичерпний позитивний потенціал для соціально-економічного розвитку. Однак, створення інформаційного суспільства призвело до виникнення багатьох загроз кібербезпеці, серед яких - зростання обсягів кіберзлочинності.

Запобігання і протидія кіберзлочинності сьогодні набули особливого значення, оскільки кіберінциденти стають дедалі частішими, більш організованими і збитковішими для держави, підприємств і громадян.

В останні роки ЄС та провідні держави світу здійснили ряд нормативно-правових нововведень, а також посилюють інституційне забезпечення процесів подолання кіберзлочинності, що є хорошим прикладом для адаптації в Україні.

З огляду на це дослідження кращих міжнародних практик запобігання і протидії кіберзлочинності та особливостей їх реалізації в Україні є актуальним.

Позитивні сторони. У кваліфікаційній роботі з'ясовано характеристики кіберзлочинності як однієї з основних загроз кібербезпеці; проаналізовано нормативно-правове забезпечення кібербезпеки і подолання кіберзлочинності в ЄС; досліджено засади запобігання та протидії кіберзлочинності в Україні на основі міжнародного досвіду.

Робота оформлена відповідно до вимог. Структура роботи забезпечує досягнення поставленої мети. Кваліфікаційна робота засвідчила розуміння здобувачкою наукової проблеми, володіння методами дослідження та здатність вирішувати прикладні завдання, наявність хороших аналітичних навичок.

Недоліки

1. Доцільно було б ширше розглянути досвід інституційного забезпечення протидії кіберзлочинності інших провідних держав світу, зокрема США.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на достатньому науково-методичному рівні, заслуговує позитивної оцінки і рекомендується до захисту, а здобувачка Посвященна Алла В'ячеславівна заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент:

_____ _____

підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 92 стор., 7 рис., 1 табл., 76 джерел.

Метою роботи є дослідження кращих міжнародних практик запобігання і протидії кіберзлочинності та особливостей їх реалізації в Україні.

Об'єктом дослідження є засади запобігання і протидії кіберзлочинності.

Предмет дослідження - кращі міжнародні практики запобігання і протидії кіберзлочинності та особливості їх реалізації в Україні.

Методи дослідження. Для вирішення завдань дослідження використовувалися методи аналізу та синтезу, уточнення понятійного апарату, узагальнення й порівняння, класифікації, історико-правовий і системний методи, а також вивчення кращих практик - бенчмаркінг.

Короткий зміст роботи. Як результат у роботі з'ясовано характеристики кіберзлочинності як однієї з основних загроз кібербезпеці; проаналізовано нормативно-правове забезпечення кібербезпеки і подолання кіберзлочинності в ЄС; досліджено засади запобігання та протидії кіберзлочинності в Україні на основі міжнародного досвіду.

Галузь застосування. Результати дослідження кращих міжнародних практик запобігання і протидії кіберзлочинності та особливостей їх реалізації в Україні можуть бути використані при плануванні та реалізації стратегії кібербезпеки в Україні.

Ключові слова : КІБЕРБЕЗПЕКА, КІБЕРЗЛОЧИННІСТЬ, ЗАПОБІГАННЯ І ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ, КРАЩІ МІЖНАРОДНІ ПРАКТИКИ І ДОСВІД УКРАЇНИ ЩОДО ПОДОЛАННЯ КІБЕРЗЛОЧИННОСТІ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 92 pages, 7 figures, 1 table, 76 sources.

The purpose of the work is to research the best international practices of preventing and countering cybercrime and the peculiarities of their implementation in Ukraine.

Object of research is the principles of preventing and countering cybercrime.

Subject of research is the best international practices of preventing and countering cybercrime and the peculiarities of their implementation in Ukraine.

Research methods Methods of analysis and synthesis, clarification of the concepts, generalization and comparison, classification, historical-legal, systemic methods and benchmarking were used to solve the research tasks.

Brief content of research. As a result, the work clarified the characteristics of cybercrime as one of the main threats to cyber security; the regulatory and legal provision of cyber security and overcoming cybercrime in the EU is analyzed; the principles of preventing and countering cybercrime in Ukraine based on international experience were studied.

Field of research. The results of the study of the best international practices for preventing and countering cybercrime and the peculiarities of their implementation in Ukraine can be used in the planning and implementation of the cyber security strategy in Ukraine.

KEYWORDS: CYBER SECURITY, CYBERCRIME, PREVENTION AND COMBATING CYBERCRIME, BEST INTERNATIONAL PRACTICES AND EXPERIENCE OF UKRAINE IN COMBATING CYBERCRIME.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

CEPOL	European Union Agency for Law Enforcement Cooperation
CERT	Computer Emergency Response Team
CSIRT	Security Incident Response Team
EC3	The European Cybercrime Centre
ENISA	European Union Agency for Network and Information Security
ESTI	European Telecommunications Standards Institute
FIRST	The Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IMPACT	International Multilateral Partnership Against Cyber Threats
IOCTA	Internet Organised Crime Threat Assessment
NIST	National Institute of Standards and Technology
OECP	Organisation for Economic Co-operation and Development
SOC	Security Operations Center

ВСТУП

Актуальність теми. Стрімкий розвиток інформаційних технологій, комп'ютеризація, створення глобального кіберпростору сформували принципово нові реалії - інформаційне суспільство і цифровий ринок - які мають невичерпний потенціал і відіграють головну роль в економічному і соціальному розвитку країн світу. Однак, створення інформаційного суспільства призвело до виникнення багатьох загроз кібербезпеці, серед яких - зростання обсягів кіберзлочинності.

Запобігання і протидія кіберзлочинності сьогодні набули особливого значення, оскільки кіберінциденти стають дедалі частішими, більш організованими і збитковішими для державних установ, підприємств і громадян.

В останні роки спостерігається безпрецедентно високий рівень активності у галузі кібербезпеки багатьох провідних держав світу, а також Європейського Союзу, який за останні роки прийняв ряд передових нормативно-правових актів, а також посилив інституційне забезпечення процесів подолання кіберзлочинності. Міжнародний досвід є хорошим прикладом для України, а його адаптація у вітчизняних умовах дозволить пом’якшити існуючі проблеми у сфері кібербезпеки шляхом удосконалення стратегій і заходів, спрямованих на запобігання злочинам у кіберпросторі й нейтралізацію їхніх потенційно шкідливих наслідків для держави і суспільства.

З огляду на це дослідження кращих міжнародних практик запобігання і протидії кіберзлочинності та особливостей їх реалізації в Україні є актуальним науковим завданням.

Метою роботи є дослідження кращих міжнародних практик запобігання і протидії кіберзлочинності та особливостей їх реалізації в Україні.

Об’єктом дослідження є засади запобігання і протидії кіберзлочинності.

Предмет дослідження - кращі міжнародні практики запобігання і протидії кіберзлочинності та особливості їх реалізації в Україні.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. З'ясувати характеристики кіберзлочинності як однієї з основних загроз кібербезпеці.

2. Проаналізувати нормативно-правове забезпечення кібербезпеки і подолання кіберзлочинності в ЄС.

3. Дослідити засади запобігання та протидії кіберзлочинності в Україні на основі міжнародного досвіду.

Методи дослідження. Для вирішення завдань дослідження використовувалися методи аналізу та синтезу, уточнення понятійного апарату, узагальнення й порівняння, класифікації, історико-правовий і системний методи, а також вивчення кращих практик - бенчмаркінг.

Наукова новизна одержаних результатів. У роботі досліджені кращі зразки міжнародного досвіду нормативно-правового й інституційного забезпечення протидії кіберзлочинності, проаналізовані недоліки й перспективні завдання адаптації передових закордонних практик у сфері кібербезпеки в Україні, в результаті впровадження яких буде підвищена ефективність державної політики подолання кіберзлочинності.

Практичне значення одержаних результатів. Результати дослідження кращих міжнародних практик запобігання і протидії кіберзлочинності й особливостей їх реалізації в Україні можуть бути використані при плануванні та реалізації стратегії кібербезпеки в Україні.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», жовтень 2023 року.

Розділ 1.
ХАРАКТЕРИСТИКИ КІБЕРЗЛОЧИННОСТІ ЯК ОДНІЄЇ З ОСНОВНИХ ЗАГРОЗ КІБЕРБЕЗПЕКИ

1.1 Передумови розширення масштабів кіберзлочинності

Як свідчить практика, впродовж останніх десятиліть масштаби злочинної діяльності у кіберпросторі значно зросли. Така ситуація є наслідком сукупної дії кількох чинників, серед яких широке застосування локальних мереж і всесвітньої мережі Інтернет, відсутність механізмів контролю глобального цифрового простору, невпинне зростання кількості користувачів; автоматизація та швидкість використання і передачі даних; анонімність діяльності в Інтернеті, проблема територіальної юрисдикції в кіберпросторі та правової співпраці тощо.

Відсутність механізмів контролю. Основною проблемою боротьби з кіберзлочинністю в мережі Інтернет є її транснаціональна природа й відсутність реальних і діючих механізмів контролю. Власне відсутність таких внутрішніх механізмів контролю мережі, а також доступність і легкість її використання є важливою передумовою виникнення основних проблем глобального інформаційного співтовариства. Децентралізованість і плоска структура мережі Інтернет, відсутність державних кордонів у кіберпросторі сприяють зростанню злочинності й гальмують процеси розробки механізмів правового й соціального контролю засад використання інформаційних мереж для вчинення неправомірної діяльності в кіберпросторі.

Упродовж останніх років інформаційні мережі розвиваються настільки швидко й динамічно, що діючі контрольні механізми не встигають реагувати на виникаючі проблеми. Хмарні обчислення, автоматизація атак, незахищеність персональних даних та іншої конфіденційної інформації особи в Інтернеті й

соціальних мережах, використання різноманітної «інформаційної зброї» є тими викликами, на які ще немає адекватного правового регулювання й адекватного реагування.

Як тільки держава долучається до інформаційного обміну з використанням мережі Інтернет, вона, а також її громадяни й організації стають вразливими до загроз з будь-якої точки планети. Механізми контролю, запобігання та розслідування подій у кіберпросторі на сьогодні є досить обмеженими як у соціальному, так і технологічному аспектах.

Так, як свідчить досвід багатьох атак на об’єкти критичної інфраструктури різних держав світу, навіть їх відключення від глобальної інформаційної мережі не гарантує захисту від потенційних загроз. Для прикладу, вірус Stuxnet розповсюджувався через портативні пристрої зберігання інформації, які підключалися до комп`ютера через USB-порт. У той час, як від’єднати від мережі Інтернет усю державу задля запобігання загрозам її інфраструктури є не можливим, оскільки інформаційні технології сьогодні відіграють ключову роль у життєзабезпеченні суспільства.

Кількість користувачів. Ключову роль у зменшенні рівня безпеки кіберпростору відіграє чинник збільшення кількості користувачів всесвітньої мережі Інтернет та інформаційно-комунікаційних технологій. У зв’язку з цим посилюються такі тенденції:

– зростає залежність суспільства від інформаційних технологій, а, отже, і вразливість людини до різних інформаційних та кіберзагроз;

– з кожним днем розширюються можливості використання мережі як середовища вчинення злочинів, а будь-який користувач, організація чи держава стають потенційними жертвами застосування ІТ в злочинних цілях;

– вчинення кіберзлочину в сучасних умовах не вимагає великих зусиль і затрат: достатньо мати комп`ютер, необхідне програмне забезпечення і під’єднання до комп’ютерної мережі;

– для здійснення правопорушення в кіберпросторі навіть не потрібно мати глибоких технічних знань. Навіть новачок може скористатися спеціальними форумами, де можна придбати все: ПЗ для вчинення злочинів, номери кредитних карток, ідентифікаційні дані користувачів, а також скористатися детальними порадами щодо здійснення електронних крадіжок і атак на комп`ютерні системи або навіть замовити такі послуги за відносно невеликі гроші.

Автоматизація та швидкість використання даних і їх передачі. Сьогодні електронні дані за кілька секунд передаються на великі відстані в тисячі кілометрів. Крім того, фактично будь-яка передача мережевих даних відбувається через територію кількох країн, оскільки інформація поділяється на частини і спрямовується найбільш доступними і зручними каналами. Здійснювати контроль передавання даних з огляду на їх обсяг і кількість користувачів є дуже важким завданням, яке часто є неможливим. Крім того, нерідко зловмисник і жертва, а також сервер з необхідними даними перебувають у різних країнах чи навіть материках. У такій ситуації для розслідування злочину необхідною є співпраця органів правопорядку багатьох країн.

Внаслідок автоматизації збільшуються ризики здійснення множинних злочинів без значних фінансових витрат і часу. Навіть більше, автоматизація дозволяє порушникам накопичувати більший фінансовий дохід шляхом розкрадання невеликих сум у великої кількості користувачів. При цьому, виявити злочини стає все складніше, зокрема й тому, що власник банківського рахунку часто просто не помічає зникнення коштів, а порушити кримінальну справу є проблематичним. Крім того, навіть якщо власник банківського рахунку звернеться до поліції з заявою про зникнення невеликої суми грошей, правоохоронцям буде досить важко встановити масштаби розкрадання.

Анонімність діяльності в Інтернеті, вразливість бездротових мереж і використання проксі-серверів. Зазначені чинники істотно ускладнюють виявлення кіберзлочинців. Так, для здійснення протиправного діяння в Інтернеті нерідко використовують «ланцюжок» серверів, входять в мережу

через точки загального доступу в громадських місцях, «зламують» бездротову мережу Wi-Fi інших користувачів. Крім зазначених існує багато інших способів злочинної діяльності з використанням ІКС, які значно ускладнюють розслідування.

Проблема територіальної юрисдикції в кіберпросторі та правового співробітництва. Розслідування правопорушень у всесвітній мережі Інтернет вимагає оперативного збирання, аналізу і зберігання цифрових даних, які самі по собі є об'єктами злочинних зазіхань і можуть бути швидко пошкоджені або знищені. У таких випадках традиційні механізми правового партнерства і взаємодопомоги, а також принцип суверенітету, відповідно до якого слідчі дії на території певної держави можуть проводити виключно її органи правопорядку, вимагають багатьох формальних узгоджень, ускладнюючи розслідування транснаціональних кіберзлочинів.

Крім проблеми спрощення й узгодження механізмів співпраці правоохоронних органів різних держав, яке вимагає багато часу і дотримання низки формальностей, гострою є проблема дотримання фундаментального принципу nullum crimen, nulla poena sine lege, згідно з яким ніхто не може бути покараний за провину, не заборонену законом. У різних державах кримінальне законодавство відрізняється, а у випадку розслідування транскордонних кіберзлочинів необхідна подвійна криміналізація діяння: як у державі, з території якої діяв злочинець, так і в державі, де перебуває жертва. Відмінності у криміналізації злочинного діяння, визначенні тяжкості вчиненого правопорушення, насамперед щодо злочинів проти громадського порядку, релігійного й екстремістському характеру, а також пов'язаних з нелегальним контентом, значно ускладнюють, а часто й унеможливлюють співробітництво правоохоронних органів різних держава.

Також серед передумов поширення кіберзлочинів виділяють:

– різкий перехід від традиційної технології обробки, зберігання й передавання даних з використанням паперових носіїв до електронної з одночасним відставанням засобів захисту інформації на машинних носіях;

– широке застосування локальних та глобальної мережі Інтернет і розширення можливостей доступу до інформації та мережевих ресурсів;

– безперервне ускладнення програмних засобів, що має наслідком збільшення кількості вразливостей і, відповідно, зменшення рівня надійності ПЗ;

– наявність можливостей замовлення злочинних «кіберпослуг» онлайн за відносно невеликі гроші.

Для України є характерними ще кілька чинників зростання кіберзлочинності:

– відставання процесів розвитку спеціального законодавства з різних аспектів комп'ютерної злочинності на тлі прогресування й виникнення нових видів правопорушень у кіберпросторі;

– технологічна залежність від закордонних виробників програмних продуктів і, як наслідок, іноземних держав;

– широко розповсюджена практика несанкціонованого копіювання, в т.ч. неліцензійного ПЗ;

– неналежне фінансування науково-технічних досліджень, що створює передумови для «витоку мізків» і здійснення різного роду «інформаційних» диверсій;

– недостатність виділення державних коштів на заходи забезпечення інформаційної та кібербезпеки, проблеми з визначенням економічної доцільності таких заходів.

Крім того, з початком повномасштабного вторгнення РФ в Україну зросли масштаби й інтенсивність здійснення кіберзлочинів, спрямованих на системи автоматизованого управління й інші інформаційно-комунікаційні системи об’єктів критичної інфраструктури держави.

1.2 Кіберзлочинність: історія, поняття й характерні риси

Історія виникнення комп'ютерних злочинів. Поява й розвиток кіберзлочинності нерозривно пов'язана з винайденням і використанням електронно-обчислювальної техніки. У 1953 році компанія IBM випустила першу наукову ЕОМ з використанням транзисторів і надовго стала лідером на ринку цифрових технологій. Спочатку комп'ютер використовували для вирішення наукових задач, в режимі «закритих» установ, тому доступ до комп'ютерів, був практично неможливим. Розповсюдження комп'ютерів у всі сфери життєдіяльності призвело до виникнення потреби їх об'єднання в мережі.

У 1961 р. Агентство передових досліджень Міністерства оборони США почало роботу над проектом по створенню експериментальної мережі передачі пакетів інформації. В 1969 р. була створена комп'ютерна мережа ARPAnet, яка поєднувала комп'ютерні центри Міністерства оборони та ряду академічних організацій. Цей проект був успішним, і багато організацій побажало увійти до цієї мережі для використання при щоденній передачі даних.

У кінці 80-х рр. мережа поєднувала комп'ютери не тільки в США, але й у інших країнах. При цьому інформація, що передавалася каналами зв'язку, відображалась на екранах моніторів тільки текстовими символами. У 1989 р. Європейський інститут фізики часток запропонував протоколи передачі графічної інформації та започаткував розгалужену гіпермедіа систему. З розробкою у середині 90-х рр. програм-браузерів, налагодженням зв'язків між виробниками та споживачами інформації як у середині країн, так і міжнародних, почався стрімкий розвиток глобальної мережі.

На початку 1980-х років з мережі ARPAnet та інших локальних мереж була створена всесвітня комп'ютерна мережа Інтернет, унікальність якої полягає в тому, що вона не знаходиться у володінні будь якої фізичної особи, приватної компанії, державного відомства або окремої країни. Завдяки цьому практично у всіх її складових відсутнє централізоване регулювання обміну

інформаційними ресурсами, цензура та інші методи здійснення контролю.

Зазначені чинники сприяють тому, що мережа Інтернет виступає не тільки як знаряддя вчинення комп'ютерних злочинів, але й як середовище для ведення різноманітної злочинної діяльності. Розповсюдження комп'ютерних систем, поєднання їх в мережі, підключення до глобальних комп'ютерних мереж користувачів все більшої кількості держав надали можливості електронного проникнення до них і вчинення злочинів.

Перші комп'ютерні злочини були зареєстровані в США у 1969 та 1973 роках і мали корисливі мотиви. А. Конфесор вчинив податковий злочин на суму 620 тис. доларів і в 1969 році став перед американським судом. У 1973 році касир нью-йоркського Сітібанку, використавши службовий комп'ютер, без особливих труднощів переказав на свій рахунок 2 млн. доларів [1].

Перші хакери з'явилися ще на початку 70-х років у Массачусетському технологічному інституті, з якого, до речі, вийшла майже вся еліта американського програмного бізнесу на чолі з Гейтсом і Алленом. Саме хакери створили більшість прикладних програм та технічних удосконалень, без яких робота на персональному комп'ютері зараз просто неможлива. Саме вони перетворили свого часу військову мережу ARPAnet на транскордонне павутиння, відоме нині як Інтернет.

Перший злочин, скоєний з використанням ЕОМ у колишньому СРСР, було зареєстровано у 1979 році у Вільнюсі. Це було розкрадання, збитки від якого становили понад 78 тис. руб. На території сучасної України з комп'ютерним злочином вперше зіткнулися співробітники управління по боротьбі з організованою злочинністю УВС Дніпропетровської області, які у 1994 році присікли спробу провідного інженера комп'ютерних систем регіонального управління Промінвестбанку викрасти 864 млн. карбованців шляхом несанкціонованого проникнення до електронної системи платежів.

Одним із перших прикладів зловмисного використання комп'ютерних технологій злочинною групою є схема розкрадання металу працівниками Криворізького металургійного комбінату, розкрита наприкінці 1998 р. У ході

оперативно-слідчих заходів попереджено розкрадання металу на 358 тис. грн.

Наведені приклади ще раз доводять суспільну небезпеку цього кримінального явища. З цими проявами поки що досить складно вести ефективну боротьбу як з точки зору кримінального переслідування, так і застосування організаційно-управлінських і кримінологічних заходів з метою їхнього попередження.

Поняття кіберзлочину та кіберзлочинності. Термін «комп'ютерна злочинність» спочатку з'явився в американській, а потім і в іншій зарубіжній літературі в 60-ті роки XX століття. Пов'язано це було з виявленням перших випадків вчинення злочинів за допомогою комп'ютерної техніки. З точки зору кримінального права поняття комп'ютерного злочину може існувати тільки в тих державах, в яких є відповідне кримінальне законодавство. Але, не зважаючи на цю обставину, цей термін широко став використовуватись практичними працівниками правоохоронних органів та вченими багатьох країн [2].

Вітчизняні й зарубіжні наукові видання, фахівці в сфері протидії комп'ютерним злочинам, засоби масової інформації оперують різними поняттями, які відзначають ті чи інші нові прояви кримінального характеру в комп'ютерній галузі. Зустрічаються терміни:

– «комп'ютерний злочин/кіберзлочин» - суспільно небезпечне винне діяння в кіберпросторі та/ або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [3];

– «кіберзлочинність» - сукупність кіберзлочинів;

– «інформаційні злочини» - незаконні дії спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань. До основних видів кіберзлочинності можна віднести такі: розповсюдження шкідливого програмного забезпечення, крадіжка номерів кредитних карт і банківських рахунків, злом паролів, порушення авторських прав [4];

– «кібератака» - цілеспрямовані (навмисні) дії в кіберпросторі, які здійснюють за допомогою засобів електронних комунікацій (включаючи ІКТ, 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 [6].

Суб'єктами злочинної діяльності є:

– «хакер» - злочинець, який зламує чужі комп’ютери, переважно за допомогою Інтернету, краде паролі, секретну й особисту інформацію, наживається на цьому;

– «кракер» - спеціаліст в галузі комп'ютерних технологій, діяльність якого пов'язана з намаганням отримати несанкціонований доступ до систем із секретною (конфіденційною) інформацією, комп'ютерний злочинець [7];

– «кіберпанк» - людина, яка не може обходитися без комп'ютера й новітніх інформаційних технологій, для якої прогрес технологій є найважливішим у житті;

– «кібервандал» - порушник, який здійснює несанкціонований доступ до інформаційно-комунікаційних систем і даних з метою їх бездумного, безцільного руйнування або пошкодження [5].

Розходження в термінології вказує не тільки на занепокоєність суспільства новою загрозою, але й на відсутність повного розуміння її суті. Виникнення комп'ютерної індустрії, чия самостійність і перспектива розвитку цілком залежать від точного регулювання правовідносин, захопило нашу країну в складний політичний та економічний період і зажадало термінового

регулювання виникаючих на її шляху проблем. Як відомо, правові механізми можуть бути включені і стають ефективними лише тоді, коли суспільні відносини, які підлягають регулюванню, на достатньому рівні стабілізувалися.

Зараз, коли створено і прийнято цілий ряд базових нормативних актів в галузі інформаційних відносин, настав час для їхнього застосування на практиці, однак на цьому шляху неминучі помилки. Важливо те, що термінологічна неточність викладення закону або методологічної рекомендації з його виконання може спричинити неправильне його застосування, а отже, і спричинити негативні наслідки.

Думки з цього приводу різняться не тільки у різних авторів, але й у одного й того ж тільки в різні часи. Так, наприклад, Ю.М. Батурін спочатку вказував на те, що комп'ютерних злочинів як особливої групи злочинів у юридичному змісті не існує, однак при цьому відзначав, що багато традиційних видів злочинів модифікувалися через залучення до них обчислювальної техніки, і тому вірніше було б говорити лише про комп'ютерні аспекти злочинів, не виділяючи їх у відокремлену групу.

Однак пізніше це й же автор вказує на те, що до комп'ютерних злочинів відносять «злочини, пов'язані із втручанням в роботу комп'ютерів, і злочини, в яких використовують комп'ютери як необхідні технічні засоби». Інші автори визначають комп'ютерні злочини як протизаконні дії, об'єктом чи знаряддям вчинення яких є електронно-обчислювальні машини.

Детальне дослідження основних компонентів змісту поняття даного явища відіграє важливу роль для загального однакового розуміння суті явища. Однак має місце ще одна досить суттєва розбіжність, вона полягає в тому, як визначити даний вид злочинів: комп'ютерні, інформаційні чи комп'ютерно-інформаційні.

З цього приводу існують різні точки зору. Наприклад, В.В. Крилов вважає, що підхід, відповідно до якого в законодавстві варто відображати певні технічні засоби, себе вичерпав, і тому недоцільно приймати термін «комп'ютерні злочини» за основу для найменування всієї сукупності злочинів в

галузі інформаційних відносин. Він пропонує розглядати як базове поняття «інформаційні злочини», виходячи з того, що сформована система правовідносин в галузі інформаційної діяльності дозволяє абстрагуватися від конкретних технічних засобів і визначає, що під інформаційними злочинами слід розуміти «суспільно небезпечні діяння в галузі інформаційних відносин, які заборонені кримінальним законом під загрозою покарання» [8].

Узагальнюючи різні точки зору, можна зробити висновок про те, що в даний час існують два основні напрямки наукової думки щодо досліджуваної проблеми. Одна частина дослідників відносить до комп'ютерних злочинів дії, у яких комп'ютер є або об'єктом, або знаряддям посягань. Дослідники ж другої групи відносять до комп'ютерних злочинів тільки протизаконні дії в сфері автоматизованої обробки інформації. В якості головної ознаки, яка класифікує і дозволяє віднести ці злочини до відокремленої групи, виділяється спільність способів, знарядь та об'єктів злочинних посягань. Іншими словами, предметом злочинного посягання є інформація, оброблювана в комп'ютерній системі, а комп'ютер є знаряддям злочинного зазіхання. Треба відзначити, що законодавство багатьох країн, у тому числі й України, стало розвиватися саме цим шляхом.

Отже, можна зробити висновок, що під інформаційно-комп'ютерними злочинами слід розуміти передбачені кримінальним законом суспільно небезпечні дії, у яких машинна інформація є об'єктом злочинного зазіхання. У даному випадку як предмет чи знаряддя злочину буде виступати комп'ютер, комп'ютерна система чи комп'ютерна мережа.

При цьому необхідно враховувати ще одну особливість - комп'ютер у злочинах може виступати одночасно і як предмет, і як знаряддя вчинення злочину.

Розглянувши поняття комп'ютерного злочину логічно перейти до визначення поняття інформаційно-комп'ютерної злочинності. За останні роки точки зору на визначення поняття комп'ютерної злочинності в деяких аспектах змінилися. Так, спеціалісти НАВСУ вказують на те, що це «всі протизаконні

дії, при яких електронне опрацювання інформації було знаряддям їх вчинення або їх об'єктом».

Ряд інших авторів надає більш широке визначення, відповідно до якого комп'ютерна злочинність є «суспільно небезпечною діяльністю чи бездіяльністю, яка здійснюється з використанням сучасних технологій та засобів комп'ютерної техніки з метою нанесення збитку майновим чи суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським організаціям і громадянам, а також правам особи». У наведених формулюваннях комп'ютер виступає як засіб учинення таких злочинів, як розкрадання, шпигунство, незаконне збирання відомостей, які складають комерційну таємницю, і таке інше [9].

Іншої думки дотримуються експерти ООН, які під комп'ютерною злочинністю розуміють «кіберзлочинність» і визначають її так: «охоплює будь-який злочин, який можна вчинити при допомозі комп'ютерної системи або мережі, в межах комп'ютерної системи або мережі або проти комп'ютерної системи або мережі». З вищевказаного можна зробити висновок що це поняття охоплює будь-який злочин, який може бути вчинений в кіберсередовищі.

При цьому, згідно цих же даних, існує дві категорії кіберзлочинів:

1) кіберзлочин у вузькому розумінні (комп'ютерний злочин) - будь-яке протиправне діяння, яке вчиняється завдяки електронним операціям, метою яких є подолання систем захисту комп'ютерних систем і даних, які в них оброблюються;

2) кіберзлочин у широкому розумінні (злочин, який пов'язаний з використанням комп'ютерів) - це будь-яке протиправне діяння, яке вчиняється завдяки або у зв'язку з комп'ютерною системою або мережею; до складу таких злочинів відносяться незаконне зберігання, надання або розповсюдження інформації при допомозі комп'ютерної системи або мережі.

Виходячи з вищенаведеного можна визначити, що під кіберзлочинністю слід розуміти будь-які протиправні дії, які спрямовані проти захисту системи даних завдяки електронним операціям.

Слід також звернути увагу на те, що кіберзлочинність має ряд ознак і характерних особливостей, які значно відрізняють її від інших видів злочинності.

1. Це міжнародне явище, яке не має кордонів, а способи і методи боротьби з нею в нашій країні тільки починають вивчатися. Розвиток міжнародних (регіональних, континентальних, глобальних) комп'ютерних мереж та супутникового зв'язку створює не тільки можливість розвитку міжнародного інформаційного співробітництва, а й має тенденцію щодо розширення можливостей вчинення злочинів, зокрема трансграничного характеру.

2. Латентність даного виду злочинної діяльності за підрахунками спеціалістів складає майже 95 %. Шансів бути виявленим у комп'ютерного злочинця набагато менше, ніж у грабіжника банку, і навіть при його затриманні в нього менше шансів бути притягнутим до кримінальної відповідальності. Виявляється в середньому один відсоток комп'ютерних злочинів, а можливість того, що за вчинення цього виду злочинів злочинець буде притягнений до кримінальної відповідальності, менше десяти відсотків.

Високому рівню латентності сприяють такі обставини: відсутність достатньої кількості підготовлених фахівців, необхідних технічних засобів для гарантованого виявлення комп'ютерних злочинів та їхнього розкриття; небажання потерпілих у більшості випадків сповіщати про вчинення злочинів до правоохоронних органів; прихований характер цих злочинів, оскільки їх можна вчинити з будь-якої відстані та з будь-якої держави; поширення персональних комп'ютерів у світі та можливість підключення їх до будь-якої інформаційної мережі; «розрив» між моментом вчинення комп'ютерних злочинів та проявом їхніх наслідків. З рівнем латентності тісно пов'язані й труднощі розкриття комп'ютерних злочинів (лише 10-15%).

3. Збиток, який нанесено комп'ютерним злочином, в десятки разів більший, ніж збиток, нанесений від вчинення загальнокримінальних корисних злочинів. За даними ФБР США «середньостатистичний» збиток від одного злочину складає: при пограбуванні банку - 9 тисяч доларів США; при використанні фіктивних документів та інших аналогічних засобів викраденнях -

25 тисяч доларів США; при неправомірному доступі до комп'ютерних систем та мереж банків та інших кредитно-фінансових установ - 650 тисяч доларів США.

4. Складність своєчасного виявлення та ідентифікації правопорушників; можливість вчинення злочинів з використанням засобів віддаленого доступу, що обумовлюється відсутністю зловмисника на місці злочину; труднощі у визначенні «місце знаходження» злочину та слабкі зв'язки в системі доказів.

5. Використання злочинцями сучасних новітніх інформаційних технологій та засобів шифрування інформації (криптографія, стеганографія тощо), які потребують спеціальної освіти та високого інтелектуального рівня. На цей час найбільш ефективними методами шифрування інформації є криптографія та стеганографія, які найчастіше застосовуються в сукупності.

6. Останнім часом простежується взаємозв'язок організованої та комп'ютерної злочинності. Вивчення досвіду боротьби з організованою злочинністю, аналіз літератури, присвяченої цій темі, свідчить про виникнення порівняно нових, але достатньо швидко прогресуючих і небезпечних її форм, однією з яких є організовані злочинні формування комп'ютерних злочинців.

Раніше вважалося, що значна частина комп'ютерних злочинів здійснюється хакерами індивідуально. Але останнім часом спостерігається тенденція до співучасті у групових посяганнях. Як зазначають експерти, кримінальна практика свідчить, що 38% злочинців діяли без співучасників, тоді як 62% вчиняли злочини у складі організованих злочинних груп і формувань.

На наш погляд, це пов'язано з такими чинниками: по-перше, діяльність стійких злочинних організованих структур є часткою великомасштабного легального і нелегального бізнесу; по-друге, із організацій, які використовують комп'ютерні системи, значно простіше і зручніше «витягувати» гроші при допомозі комп'ютерних технологій; по-третє, оскільки сили безпеки і поліції використовують комп'ютерні технології для боротьби зі злочинністю, то, відповідно, щоб попередити їхнє стеження й розгадати плани правоохоронців, лідери злочинних угруповань широко використовують, як могутню зброю протидії, комп'ютерні технології.

На сьогоднішній день можна говорити про різноманітні організовані формування комп'ютерних злочинців, які відрізняються одне від іншого структурою, технічними можливостями, злочинними цілями. Обумовлено це специфікою комп'ютерних злочинів, які вчиняє та або інша група та залежить від поставленої мети. На наш погляд, організовані формування комп'ютерних злочинців можливо класифікувати таким чином:

1. Організоване злочинне формуваннями комп'ютерних злочинців. Ці формування складаються з професійних комп'ютерних злочинців, з яскраво вираженим корисливим напрямком. Злочинці даної групи характеризуються систематичним багаторазовим учиненням комп'ютерних злочинів із обов'язковим виконанням дій, які спрямовані на підготовку та їхнє приховування. Особи цієї групи володіють сталими злочинними навичками і знаннями. Дослідження показують, що злочинці даного формування добре організовані, мобільні та технічно оснащені висококласним обладнанням і спеціальною технікою (нерідко оперативно-технічного характеру). Ці формування частіше всього виконують так звані «комп'ютерні злочини на замовлення» або займаються шпигунством, як комерційним, так і політичним.

2. Організоване злочинне формування, яке має у своєму складі структурний підрозділ, який складається з комп'ютерних злочинців. Це формування утримує даний структурний підрозділ, який складається з двох або трьох комп'ютерних злочинців, для обслуговування своїх потреб. Це може бути приховування іншого злочину комп'ютерним, отримання необхідної для злочинної діяльності інформації, передача необхідної інформації та здійснення постійного зв'язку з іншими злочинними формуваннями завдяки сучасним ІТ.

3. Віртуальні злочинні формування комп'ютерних злочинців. Комп'ютерні злочинці об'єднуються у віртуальну групу та здійснюють напад на конкретну систему. Протистояти такому нападу практично неможливо, тому що він ведеться водночас із різних комп'ютерів, які можуть бути розташовані в різних країнах світу. Для даного злочинного формування характерно те, що його члени фактично не знають один одного, а спілкуються тільки через мережу.

4. Організовані злочинні формування, які використовують для досягнення злочинної мети за наймом фахівців у галузі комп'ютерних технологій (програмістів, хакерів та інших).

Відомі випадки, коли злочинними формуваннями наймалися хакери, яким надавалось окреме приміщення, яке було під охороною та обладнане найсучаснішими технологіями, для того, щоб вони здійснювали викрадення грошей шляхом незаконного проникнення до комп'ютерних мереж великих комерційних банків; тому найбільш розповсюдженими є комп'ютерні злочини, які вчиняються шляхом несанкціонованого доступу.

1.3 Класифікація кіберзлочинів

Вперше види злочинів у сфері комп'ютерних технологій були сформульовані в 1979 р. на Конференції американської асоціації адвокатів у Далласі і містили: використання або спроба використання комп'ютера, обчислювальної системи або мереж, комп'ютерів з метою отримання грошей, власності або послуг шляхом прикриття фальшивими кодами або видання себе за іншу особу; умисна несанкціонована дія, що має на меті зміну, пошкодження, знищення або викрадення комп'ютера, обчислювальної системи, комп'ютерної мережі або систем математичного забезпечення, які містяться в них, програм або даних; умисне незаконне порушення зв'язку між комп'ютерами, обчислювальними системами або комп'ютерними мережами.

Питання класифікації кіберзлочинів, як і питання про їхнє визначення, є дуже суперечливим і потребує детального дослідження. Враховуючи той факт, що не існує однозначного поняття кіберзлочину та класифікації кіберзлочинів, і те, що законодавець залишив це питання відкритим, розглянемо основні класифікації кіберзлочинів.

Наразі найпоширеніша класифікація кіберзлочинів базується на структурі

Конвенції Ради Європи про кіберзлочинність [9]. Ця класифікація наразі слугує «еталоном», оскільки існуючі міжнародні, регіональні документи та наукові практики використовують цю класифікацію (Рис. 1.1).

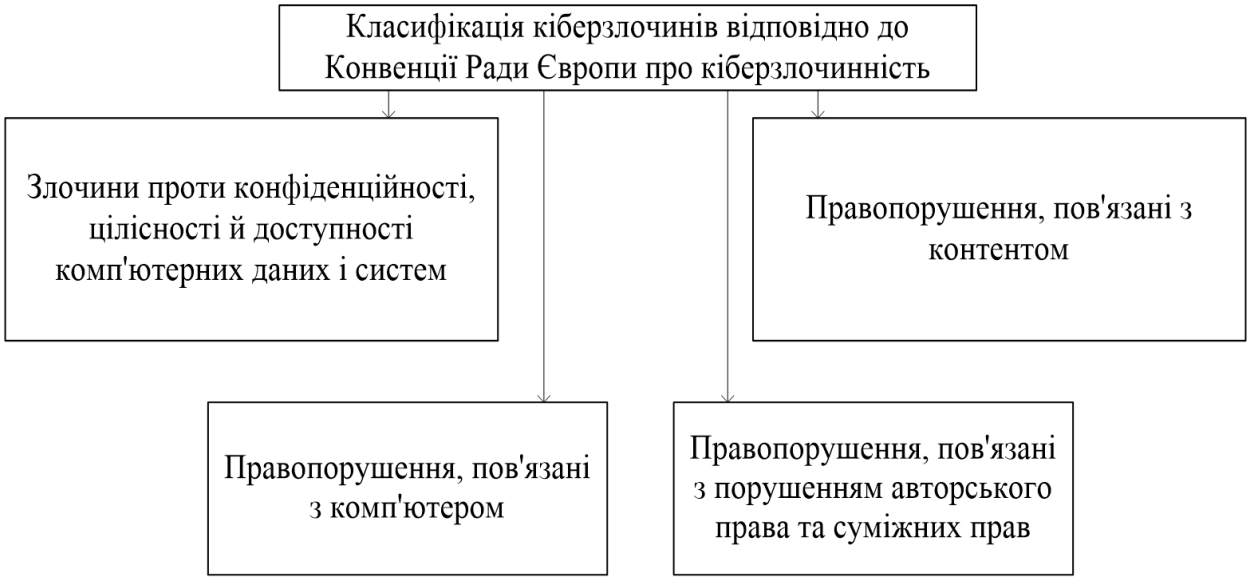

Рис. 1.1. Класифікація кіберзлочинів відповідно до Конвенції Ради Європи про кіберзлочинність

1) Злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем:

- Несанкціонований доступ - умисний несанкціонований доступ до всієї або частини комп'ютерної системи, з метою отримання комп'ютерних даних або з будь-якою іншою неналежною метою;
- Втручання в дані - навмисне пошкодження, знищення, спотворення, зміна або приховування комп'ютерних даних без належних на те прав;
- Системне втручання - навмисне і суттєве втручання у функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, спотворення, зміни або приховування комп'ютерних даних без належних на те прав;
- Незаконне використання пристрою, тобто його виготовлення, продаж, придбання з метою використання, розповсюдження або надання в користування іншим способом;

2) Правопорушення, пов'язані з комп'ютером

- Підробка, пов'язана з комп'ютерами;
- Шахрайство, пов'язане з комп'ютерами.

3) Правопорушення, пов'язані з контентом

- Правопорушення, пов'язані з дитячою порнографією.

4) Правопорушення, пов'язані з порушенням авторського права та суміжних прав.

Також часто до кіберзлочинів відносять акти расизму та ксенофобії, вчинені через комп'ютерні мережі [10].

Відповідно до опису, який був підготовлений Організацією економічного співробітництва та розвитку в 1985 році, а також рекомендацій Ради Європи 1989 року, правопорушення, які пов'язані з конфіденційністю, цілісністю або доступністю, включають:

1. Несанкціонований доступ, тобто неправомірний доступ до комп'ютерної системи або мережі шляхом подолання засобів захисту.

2. Пошкодження комп'ютерних даних або комп'ютерних програм, тобто неправомірне видалення, пошкодження, погіршення стану або пригнічення комп'ютерних даних чи комп'ютерних програм.

3. Комп'ютерний саботаж, тобто введення, зміна, видалення або пригнічення комп'ютерних даних або комп'ютерних програм чи вхід до комп'ютерної системи з метою перешкоджання функціонуванню комп'ютера або телекомунікаційної системи;

4. Несанкціоноване перехоплення, тобто перехоплення без дозволу та з використанням технічних засобів, повідомлень, які надходять до комп'ютерної системи або мережі або виходять із комп'ютерної системи чи мережі, або таких, що циркулюють у межах такої системи або мережі.

5. Комп'ютерний шпіонаж, тобто придбання, розголошення, передання або використання даних, які складають комерційну таємницю, без дозволу або юридичної засади з метою або нанесення економічного збитку особі, яка має право на збереження таємних відомостей, або набуття незаконних переваг для себе чи в інтересах третьої особи.

У 1994 році ООН опублікувала Керівництво із запобігання злочинів, пов'язаних із застосуванням комп'ютерів, і боротьби з ними, де надано широкий огляд новітніх форм комп'ютерних злочинів і злочинів, пов'язаних із використанням комп'ютерів, із зазначенням історії, масштабу і характеру порушень, а також пропонованих рішень.

У наведеному Керівництві надається наступна класифікація «звичайних видів» комп'ютерних злочинів:

– шахрайство шляхом маніпуляцій на комп'ютері;

– комп'ютерна підробка;

– заподіяння збитку чи зміна комп'ютерних даних чи програм;

– несанкціонований доступ до комп'ютерних систем і послуг;

– несанкціоноване копіювання комп'ютерних програм, які охороняються законом.

З розвитком глобальної мережі Інтернет, яка є відкритим середовищем і надає користувачам можливість вчиняти певні дії за межами місця перебування, експерти ООН прийшли до висновку, що використання мережі Інтернет полегшує відмивання грошей, здійснення шахрайства й інших видів махінацій. За класифікацією ООН злочини в Інтернеті поділяються на такі види (Рис. 1.2).

Рис. 1.2. Класифікація злочинів в мережі Інтернет

1. Промисловий шпіонаж. Це викрадення промислових таємниць

(технічна документація, інформація про нові продукти та маркетингові стратегії). В області економіки до 90% злочинів, за даними ООН, здійснюється співробітниками компаній, які незадоволені діяльністю адміністрації компанії.

2. Саботаж. Головну загрозу являють «поштові бомби»: злочинці тероризують власників електронної пошти, паралізуючи роботу пошти мегабайтами зайвої рекламної інформації.

3. Вандалізм. Злочинці дістають доступ до певного Web-сайту чи бази даних, знешкоджують їх чи змінюють інформацію.

4. Викрадення паролів. Викрадення паролів у власників з метою здійснення злочину під чужим ім'ям. Для цього використовують спеціальне програмне забезпечення.

5. Спуфінг (маскування). Використання різних технічних вивертів для зламу захищених чужих комп'ютерів з метою викрадення конфіденційної інформації. Цим способом скористався знаменитий хакер Кевін Митник у 1996 р. для зламу захисту домашнього комп'ютера експерта з комп'ютерної безпеки ФБР (США).

6. Дитяча порнографія. Масштаби цієї проблеми надзвичайні й поширюються у геометричній прогресії. В останні роки, за оцінками експертів, кількість цих злочинів у США збільшується в чотири рази на рік.

7. Азартні ігри. Електронні азартні ігри за останні роки переросли в глобальний бізнес. Маючи доступ до Інтернету, громадяни тих держав, де азартні ігри заборонені чи потребують ліцензування (електронні біржі, тоталізатори, віртуальні казино тощо), грають у своє задоволення.

8. Шахрайство. Від цього виду злочину, передусім, завдається шкода електронній комерції, електронній торгівлі акціями, цінними паперами, продажу та купівлі товарів у віртуальних магазинах через Internet. Шахраї вміло використовують прогалини в законодавстві окремих держав та інше [11].

У науковій літературі представлено класифікацію кіберзлочинів за метою правопорушення [12], яка включає (Рис. 1.3):

Рис. 1.3. Класифікація кіберзлочинів за метою правопорушення

– злочини, що порушують конфіденційність, цілісність і доступність комп'ютерних даних та комп'ютерних мереж;

– економічні комп'ютерні злочини;

– комп'ютерні злочини проти недоторканності прав особи і приватного простору;

– комп'ютерні злочини проти суспільних і державних інтересів.

Однак варто зазначити, що багато кіберзлочинів впливають на декілька об'єктів одночасно. Ще однією категорією правопорушень є крадіжка особистих даних, тобто викрадення, передача або використання персональних даних у злочинних цілях.

Також у науковій літературі представлений підхід, відповідно до якого кіберзлочини поділяють на:

1) наступальні - кібертероризм, погрози фізичного насильства (наприклад, надіслані електронною поштою), кіберпереслідування, кіберсталкінг (незаконні сексуальні домагання або переслідування інших осіб через Інтернет), дитяча порнографія (створення порнографічних матеріалів із зображень дітей; розповсюдження цих матеріалів, отримання доступу до них);

2) неагресивні - кіберкрадіжки, кібервандалізм, кібершахрайство, кібершпигунство, спам та віруси [7].

Як свідчить практика, найбільш поширеними кіберзлочинами є: скімінг

карток, фішинг, вішинг, онлайн-шахрайство, хакерство, спільне використання карток, соціальна інженерія, переслідування, незаконний контент і рефайлінг [13].

Враховуючи статистичні дані та приклади, можна зробити висновок, що правопорушення, пов'язані з Інтернетом, можна розділити на дві великі групи:

– злочини, спрямовані на мережі та системи обробки інформації;

– злочини, в яких мережі використовуються як засоби здійснення і зв'язку.

У першу категорію входять кіберзлочини, пов'язані з несанкціонованим доступом, зміною або пошкодженням даних, незаконним користуванням послугами. До другої відносять злочини, пов'язані головним чином із «вираженням думки»: представленням насильства, расової дискримінації, порнографії. Оскільки Інтернет - всесвітній засіб для передачі текстів, зображень і звуків, він ідеально підходить для вчинення таких злочинів.

За даними досліджень, мотиви скоєних в даний час комп'ютерних злочинів включають: отримання вигоди (41%); загрози з боку невдоволеного персоналу (27%); корпоративне шпигунство і диверсії (26%); політичні мотиви (26%) та міждержавні кібервійни (24%) (Рис. 1.4) [14]. Крім цього серед поширених мотивів кіберпорушників називають дослідницький інтерес, хуліганство і помсту.

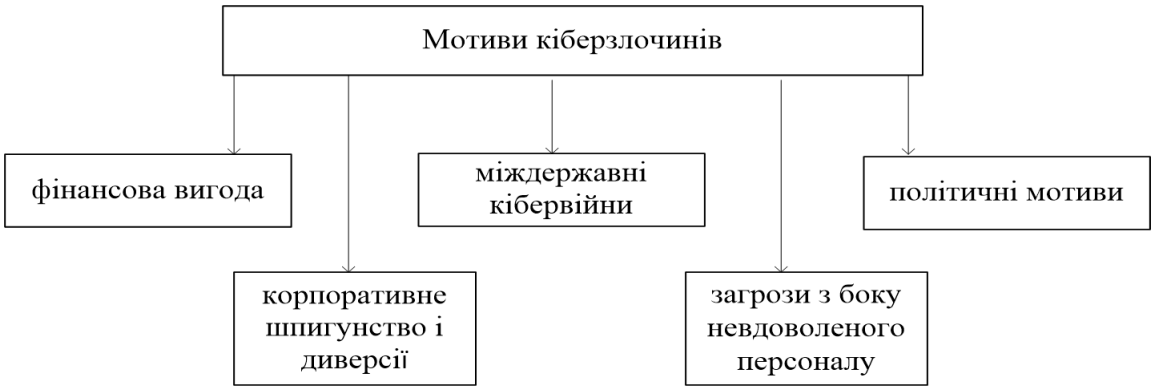

Рис. 1.4. Мотиви кіберзлочинів

Слід також підкреслити, що незважаючи на велику кількість класифікацій кіберзлочинів та кіберзлочинців за різними критеріями, усі їхні дії спрямовані на злом комп'ютерних систем або мереж будь-яким шляхом із застосуванням програмних та технічних засобів.

Висновки до розділу 1

Встановлено, що основними передумовами зростання кіберзлочинності є відсутність механізмів контролю в мережі Інтернет; величезна кількість користувачів; високий ступінь автоматизації та швидкість передачі електронних даних; складність розслідування кіберзлочинів, які мають транскордонний характер; постійне ускладнення програмних засобів з одночасним зменшенням їх надійності та збільшення кількості вразливостей; відставання технологій захисту інформації та законодавчого регулювання проблем кібербезпеки тощо.

У результаті аналізу вітчизняного законодавства й наукових джерел запропоновано розуміти під кіберзлочином (комп’ютерним злочином) будь-яке протиправне діяння, яке вчиняється завдяки електронним операціям, метою яких є подолання систем захисту комп'ютерних систем та даних, які в них обробляються, а під кіберзлочинністю - сукупність кіберзлочинів.

Зроблено висновок, що кіберзлочинність має ряд характерних ознак, зокрема відсутність кордонів; латентність (прихований характер); великі обсяги збитків у порівнянні з іншими кримінальними діяннями; складність своєчасного виявлення та ідентифікації правопорушників; використання злочинцями новітніх інформаційних технологій; взаємозв'язок організованої та комп'ютерної злочинності.

Вивчення підходів до класифікації показало, що наразі найпоширенішими є класифікації кіберзлочинів провідних міжнародних та європейських організацій, зокрема ООН, ОЕСР, Ради Європи (Конвенція про кіберзлочинність) та інших. У науковій літературі кіберзлочини поділяють на окремі види за такими критеріями як мета і мотиви правопорушення, роль комп’ютерних систем і мереж у їх здійсненні тощо.

Розділ 2
НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ І ПОДОЛАННЯ КІБЕРЗЛОЧИННОСТІ В ЄС

2.1 Регулювання кібербезпеки в ЄС

Правова база ЄС у сфері кібербезпеки розвивається з урахуванням потреб цифрового ринку ЄС. Важливим є стратегічне бачення та заклик до більш всеохоплюючого, перехресного політичного підходу до формування кіберстійкості в рамках спільного цифрового ринку ЄС.

Концептуалізація кібербезпеки як сфери політики та правового регулювання відбувається поступово і достатньо динамічно. У Європейському Союзі прийняті численні регуляторні акти, які сприяють забезпеченню кібербезпеки громадян, підприємств і державних інституцій, що стосуються конкретних заходів мережевої та інформаційної безпеки, електронних комунікацій та протидії кіберзлочинності.

Офіційне визнання «кібербезпеки» як нового напряму політики в ЄС було визнано у 2013 році з прийняттям Першої стратегії кібербезпеки Європейського Союзу (ЄС)[15]. Це визнання було довгоочікуваним розвитком, який визнав розмиття ліній у трьох спочатку окремих, але суміжних сферах політики мережевих таінформаційних заходів безпеки, які націлені на операторів основних послуг і постачальників критичних і цифрових інфраструктур; електронні комунікації, включаючи питання конфіденційності та захисту даних; протидія кіберзлочинності.

Знадобилося понад 20-ть років, щоб поступово зростаюча кількість розпорошених ініціатив, що стосуються цифрового середовища - від цифрових підписів та електронної комерції до кіберзлочинів та критичної інфраструктури - була визнана загальним терміном «кібербезпека» в Європейському Союзі.

Для визначення кібербезпеки доцільно порівняти її крізь призму з інформаційною безпекою. Ці поняття часто межують між собою, але не є тотожними, що часто викликає, в свою чергу, проблеми з визначенням джерел при регулюванні міжнародно-правового співробітництва в цих сферах. Основна відмінність полягає в тому, що інформаційна безпека та кібербезпека різняться за сферою своєї дії. Захист інформації пов'язаний із забезпеченням безпеки даних в будь-якій формі і є трохи ширшим, ніж кібербезпека. Цей висновок виходить з визначень, які наведені в джерелах ЄС.

Стратегія кібербезпеки ЄС 2013 року представила визначення, згідно з яким кібербезпека зводиться до гарантій та дій, які можуть бути використані для захисту кібердоменів як у цивільному, так іу військовому секторах від тих загроз, які пов'язані або можуть зашкодити взаємозалежним мережам та інформаційній інфраструктурі [16]. У такому контексті, основними цілями кібербезпеки є забезпечення доступності та цілісності мереж та інфраструктури та конфіденційності інформації, що міститься в ній.

Можна вважати, що прийняття стратегії кібербезпеки ЄС у 2013 році стало критичним моментом, який спричинив збільшення використання цього терміну в політичних документах ЄС, що можна побачити на прикладі Повідомлення Єврокомісії «Зміцнення системи кіберстійкості Європи та сприяння конкурентоспроможній та інноваційній кібербезпеці» 2016 року [17].

Хоча дві стратегії кібербезпеки ЄС слідували за прийняттям численних законодавчих заходів, що стосуються кібербезпеки, вони висунули цілі політики, що згодом призвели до законодавства, а саме Директиву про мережеву та інформаційну безпеку [18] та Закон про кібербезпеку [19], що додатково уточнює роль і повноваження Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA). Політичні заходи з різних областей політики зрештою призвели до змін та коригувань у різних правових рамках ЄС і навпаки.

Як уже згадувалося, було прийнято численні політичні та регуляторні заходи для підвищення безпеки громадян, підприємств і державних органів у

сферах мережевої та інформаційної безпеки, електронних комунікацій і кіберзлочинності. Насправді ЄС лише нещодавно почав використовувати термін «кібербезпека» у своїх політичних документах.

Варто відзначити, що вищі урядовці та інституції ЄС часто вибирають визначення, розроблені організаціями зі стандартизації, такими як Європейський інститут з питань стандартизації (ESTI), Міжнародна організація стандартизації, або міжурядові організації, такі як Міжнародний Союз електрозв'язку. Тому на сьогодні численні визначення кібербезпеки співіснують, зосереджуючись на різних її аспектах.

Згідно зі стандартом ETSI, функції кібербезпеки складаються з постійного циклу структурованих дій:

– визначити (зрозуміти стан і ризики для систем, активів, даних і можливостей);

– захистити (впровадити відповідні гарантії);

– виявити (реалізувати здатність ідентифікувати кібербезпеку);

– відреагувати (реалізувати здатність вживати заходів у відповідь на загрозу кібербезпеці);

– відновлювати (забезпечити стійкість і відновлення порушених можливостей).

Цей самий стандарт визначає кібербезпеку як «сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, настанов, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій та технологій, які можна використовувати для захисту кіберсередовища, організації та активів користувача» [19].

Кібербезпека може розглядатися з різних сторін: як проблема, що викликає занепокоєння через ризики, що існують в Інтернеті (кіберпросторі); її можна розуміти як захист лише віртуальних активів; або вона може бути націлена лише на захист від зловмисних дій.

Такі вузькі визначення несуть за собою ризик не врахування наслідків для

людей та їх прав. Визначення, що використовуються для позначення кібербезпеки різними суб'єктами, включаючи держави-члени ЄС, як правило, представляють різні точки зору, які потенційно можуть суперечити один одному. ENISA часто розглядає кібербезпеку як лише технічну проблему; деякі держави-члени у своїх стратегіях національної безпеки розглядають кібербезпеку як питання національної безпеки.

У контексті Директиви з безпеки мережевих та інформаційних систем («ДирективаNIS»), кібербезпека розуміється як «здатність мережевих та інформаційних систем протистояти будь-якій дії, яка порушує доступність, автентичність, цілісність або конфіденційність збережених, переданих або оброблених даних або пов'язаних з ними послугами» [18].

Тим не менше, Директива NIS формально стосується «безпеки мережевих та інформаційних систем» а не кібербезпеки. Неоднозначність, яка закладена та підтримувана терміном «кібербезпека» дозволяє використовувати цей термін у різних сферах політики, згаданих вище. Що ще важливе, тут виникає питання, чи є кібербезпека ЄС автономним поняттям, що має специфічний характер у політиці ЄС на відміну від інших рівнів політики.

У 2004 році Європейська Комісія схвалила рішення про створення дорадчого органу ENISA[20], яке вже перетворилось в Агентство кібербезпеки ЄС для надавання оперативної допомоги державам-членам ЄС в протидії кібератакам. Відповідну пропозицію 13 вересня 2017 року озвучив Президент Єврокомісії Жан-Клод Юнкер: «Європа все ще не оснащена належним чином, коли мова йде про кібератаки». Ось чому сьогодні Комісія пропонує нові інструменти, включаючи Європейське агентство кібербезпеки, щоб допомогти нашому захисту проти таких атак» [21].

Агентство проводить щорічні пан-європейські навчання з кібербезпеки та обмін розвідувальною інформацією щодо кіберзагроз шляхом створення центрів обміну інформацією та аналізу. Ще однією важливою функцією Агентства визначено сертифікацію програмних продуктів на відповідність вимогам кібербезпеки в ЄС. Одночасно, Євро комісія запропонувала створити

Фонд реагування на надзвичайні ситуації з кібербезпеки, до якого можуть приєднатися держави-члени ЄС за бажанням.

Однак, започаткований наприкінці 2017 року в рамках безпекової ініціативи PESCO Європейський оборонний фонд, який серед іншого акумулював фінансові засоби й для проектів з кібероборони, фактично відсунув на другий план потребує створення окремого кіберфонду ЄС.

Можна виділити п'ять стратегічних пріоритетів кібербезпеки ЄС:

- досягнення кіберстійкості шляхом встановлення мінімальних вимог до співробітництва та координації національних компетентних органів з питань безпеки мереж та інформаційних систем;

- зменшення кіберзлочинності шляхом забезпечення швидкого впровадження вимог Директиви NIS, заохочення ратифікації положень Будапештської конвенції Ради Європи про кіберзлочинність та фінансування програми для розгортання оперативних інструментів кіберзахисту;

- розробка спільної політики та розвиток можливостей кібероборони, пов'язаних із загальною безпекою та оборонною політикою в контексті кіберзахисту ЄС, розробка політики ЄС щодо кіберзахисту, стимулювання діалогу та координації між цивільними та військовими суб'єктами в ЄС, та сприяння діалогу з міжнародними партнерами;

- розвиток промислових та технологічних ресурсів для кібербезпеки шляхом створення державно-приватної платформи з питань мережевої та інформаційної безпеки, надання технічних вказівок та рекомендацій для прийняття стандартів та практики й заохочення розвитку стандартів безпеки;

- встановлення послідовної міжнародної політики щодо кіберпростору для ЄС та сприяння включення основних цінностей ЄС у спільну зовнішню політику та політику безпеки. ЄС повинен забезпечити проведення своїх консультацій з міжнародними партнерами з питань кібербезпеки, що покликані доповнити існуючий порядок денний двостороннього діалогу між державами-членами та третіми країнами [22].

Ці консультації керуватимуться основними цінностями ЄС - людською

гідністю, свободою, демократією, рівністю, верховенством права та повагою до основних свобод. Дотримуючись цілей цього пріоритету, ЄС прагне досягти високого рівня захисту даних, включаючи захист персональних даних, переданих третім країн.

Підсумовуючи вищезазначене, термін «кібербезпека», з точки зору ЄС, передбачає поєднання державної кіберстійкості, протидію кіберзлочинності, кіберзахисту та глобальні проблеми безпеки кіберпростору. В умовах зростаючих гібридних загроз, головним завданням європейських, та й інших країн світу є вжиття заходів, що дозволять принципово зменшити негативні наслідки від кіберінцидентів, гарантуючи безпеку цифрового розвитку.

Можливість надати різне значення терміну «кібербезпека» має як переваги, так і недоліки. Це вказує на гнучкість терміну, який може адаптуватися до мінливих обставин.

У той же час постійне розширення терміну може стати надмірно інклюзивним або широким таким чином, що перешкоджатиме узгодженому регулюванню в цій галузі та таким чином перешкоджатиме розробці регуляторних заходів. Це також відкриває простір для неоднозначності у розумінні між ЄС та державами-членами, що спираються на поняття національної безпеки. Отже, таке змінне значення цього терміну може досягти прогресу в цій конкретній сфері політики важко досягти або, принаймні, менш помітним.

За декілька останніх десятиліть відбулася потужна технологічна революція в галузі використання комп'ютерів та комунікацій, яка привела до принципових змін та збільшення апаратного парку, суттєвого прискорення швидкості передачі інформації. Водночас саме стрімкий інформаційний прогрес спричинив проблему захищеності персональних даних через виникнення глобальних лідерів, що призвело до концентрації інформації в руках «великих гравців мережі» та централізації загальної інфраструктури.

Це зробило можливими великомасштабні атаки та створило великі ризики значних збитків при критичних пошкодженнях інфраструктури таких систем.

Розглядаючи питання регулювання кібербезпеки в ЄС, необхідно

враховувати принцип делегування, що є наскрізним для багатьох сфер спільної політики. ЄС може приймати законодавчі акти у сферах, що потребують колективного вирішення між державами-учасницями. зокрема й у сфері кібербезпеки, проте це вимагає надання юридичного обґрунтування, тобто правового підґрунтя [23].

Визначити потребу у запровадженні правового регулювання кібербезпеки на рівні ЄС намагалися науковці, політики та представники приватного сектору. Щоб полегшити це завдання, Європейська рахункова палата, установа, яка опікується інтересами платників податків ЄС, опублікувала звіт, що забезпечує чудовий огляд складної політики ЄС щодо кібербезпеки.

Звіт визначає багато викликів ефективному здійсненню політики, таких як: змістовна оцінка та підзвітність політики та законодавчої бази; усунення прогалин у законодавстві ЄС та нерівномірності його упровадження; узгодження рівнів інвестицій в кібербезпеку з відповідними цілями; адекватне фінансування агентств ЄС; та посилення управління інформаційною безпекою, а також оцінки загроз та ризиків [24].

Більшість правових заходів, що стосуються кібербезпеки, містяться в директивах, які є мінімальними заходами гармонізації (наприклад, Директива NIST [17] та Директива про напади на інформаційні системи [25]). На практиці це означає, що держави-члени вільні у виборі форми та методів реалізації вимог, що випливають з таких директив. Ця гнучкість може розглядатися як слабкість інструментів мінімальної гармонізації. Однак директиви вважаються найкращим інструментом при впровадженні складних законодавчих змін, таких як запровадження нової регуляторної сфери.

У деяких сферах, які є традиційно регламентовані більш суворо, таких як захист персональних даних та охорона здоров'я, спостерігається тенденція до прийняття більш гармонізованого регулювання. Наприклад, Загальний регламент про захист персональних даних (GDPR) [26], що скасовує попередню Директиву про захист даних 95/46.

2.2 Еволюція законодавства ЄС у галузі кібербезпеки

Європейському Союзу знадобилось 20 років для розгортання кібербезпекових ініціатив та вирішення питань, що стосуються цифрового середовища - від цифрових підписів до електронної комерції, протидії кіберзлочинності й захисту критичної інфраструктури. До того ж, кібербезпека, зовсім недавно охопила питання кібероборони.

Починаючи з 2000-х років Європейська Комісія починає приділяти все більше уваги питанням кібербезпеки. Зокрема, в 2001 році було опубліковане повідомлення щодо безпеки мереж та інформації [27], де відзначено, що безпека комунікацій та інформації стає ключовим пріоритетом ЄС з огляду на їх критичне значення для соціально-економічного розвитку суспільства. У 2006 році була схвалена Стратегія безпечного інформаційного суспільства [28], в якій наголошено на важливості забезпечення інформаційної та мережевою безпеки для створення єдиного європейського простору.

У подальшому кібербезпека стає невід'ємною складовою безпекових документів Євросоюзу. У 2009 році була схвалена нова стратегічна комунікація «Захист критичної інформаційної інфраструктури» [29]. У 2012 році в ЄС була створена Група з питань реагування на інциденти в галузі комп'ютерної безпеки, відповідальна за безпеку інформаційних систем інституцій ЄС.

У лютому 2013 року, як відзначалося раніше, схвалена перша стратегія кібербезпеки ЄС «Відкритий, надійний і безпечний кіберпростір», яка ознаменувала офіційне визнання кібербезпеки як нового напрямку політики ЄС. Кіберстратегія визначає такі стратегічні пріоритети ЄС: кіберстійкість, зменшення кіберзлочинності, розвиток можливостей і політики кіберзахисту, індустріальних і технологічних ресурсів кібербезпеки, послідовної міжнародної політики з кіберпростору [15].

Глобальна стратегія із зовнішньої і безпекової політики ЄС, схвалена в червні 2016 року, стала основою для розробки інших секторальних та

операційних документів. У ній кібербезпека виведена в окрему без пекову сферу, яка включає розвиток технологічних можливостей для протидії кіберзагрозам, скорочення кіберзлочинності, посилення стійкості критичної інфраструктури, мереж і сервісів [30].

Пізніше, в липні 2016 року, ЄС схвалив Директиву з безпеки мережевих та інформаційних систем (ДирективаNIS). Відповідно до неї, держави-члени ЄС повинні були схвалити відповідні національні закони до 9 травня 2018 року і визначити операторів основних послуг (essential services providers) у цій сфері до 9 листопада 2018 року. Директивою була створена Група співробітництва NIS, на яку покладені функції забезпечення стратегічного співробітництва та обміну інформацією між державами-членами з питань кібербезпеки. Група здійснює безпосередню координацію мережі Груп реагування на інциденти комп'ютерної безпеки [17].

У вересні 2017 року ЄС доповнив Стратегію кібербезпеки 2013 року, схваливши Спільну комунікацію Європейського парламенту й Ради ЄС з розбудови належної кібербезпеки ЄС [28]. Цей документ визначив пакет додаткових заходів, спрямованих, перш за все, на посилення Агентства кібербезпеки ЄС (ENISA), створення загальної для ЄС схеми сертифікації з кібербезпеки, розвиток Плану відповіді на масштабні кібератаки і кризи, посилення досліджень.

Наприкінці 2017 року в ЄС було запущено Постійне структуроване співробітництво (PESCO), до якого приєдналися 25 із 29 держав-членів Євросоюзу [31]. Одним із напрямків цієї співпраці стала кібербезпека, зокрема, розпочалось створення Груп швидкого реагування на кіберзагрози. Позитивним для України рішенням є те, що треті країни можуть запрошуватися до участі в окремих проектах PESCO, включаючи сферу кіберзахисту.

Восени 2017 року Європейська Комісія та Верховний представник Союзу із закордонних справ та політики безпеки оприлюднили спільне повідомлення до Європейського Парламенту та Ради ЄС під назвою «Стійкість, стримування та захист: побудова міцної кібербезпеки для ЄС» (Стратегія ЄС з кібербезпеки 2017

року) [32], яке базувалося на попередніх ініціативах та галузевій структурі.

Друга стратегія кібербезпеки ЄС передбачила правові рамки для електронних комунікацій і комерції,електронних підписів, а також містила політичні та регуляторні заходи. Ця стратегія кібербезпеки наголосила на необхідності заходів, які дозволять підвищити стійкість ЄС до кібератак, посилення механізмів виявлення кібератак і міжнародного співробітництва у галузі кібербезпеки. Стратегія підкреслила необхідність аналізу наслідків появи нових технологій і впровадження заходів для усунення ризиків, які внаслідок цього виникають. У документі висловлено обіцянку переглянути існуюче законодавство ЄС щодо новітніх технологій, включаючи робототехніку, штучний інтелект та 3D-друк.

У цьому ж році в рамках агентства Європол почав свою роботу Європейський Центр протидії кіберзлочинності, який був створений для посилення реагування правоохоронних органів ЄС на кіберзлочинність. З моменту заснування Центр зробив значний внесок у боротьбу з кіберзлочинністю і брав участь у багатьох резонансних операціях. Основні зусилля підрозділу зосереджуються на таких типах кіберзлочинів: кіберзалежна злочинність, сексуальна експлуатація дітей, шахрайство з платіжними засобами, а також злочинність у Dark Web і на альтернативних платформах [33].

У вересні 2018 року Єврокомісія схвалила рішення про створення мережі центрів компетентності [34] в державах-членах за координації Європейського центру досліджень і компетентності з кібербезпеки, яка сприяє розвитку засобів і технологій протидії кіберзагрозам.

З метою більшого залучення приватного сектору до протидії кіберзагрозам, в ЄС була створена Європейська платформа публічно-приватного партнерства стійкості (PPP), в рамках якої передбачено обмін інформацією, відстеження кіберзагроз і реагування на інциденти безпеки, організація наукових досліджень, підготовка кадрів, підвищення цифрової грамотності тощо [35, 36].

У 2019 році Європейський Парламент, Європейська Рада і Європейська

Комісія досягли політичної згоди щодо Акту з кібербезпеки [18], який посилює повноваження ENISA, встановлює рамки для сертифікації з кібербезпеки, прискорює розвиток онлайн-сервісів з кібербезпеки, що сприяє окресленню інституційного виміру кібербезпеки ЄС загалом.

«Стратегія кібербезпеки ЄС на цифрове десятиліття» (2020) [37] спрямована на захист глобального та відкритого Інтернету, одночасно пропонуючи захисні заходи не лише для забезпечення безпеки, але й для захисту європейських цінностей та основних прав кожного.

Спираючись на досягнення минулих років, документ містить конкретні пропозиції щодо регуляторних, інвестиційних та політичних ініціатив у трьох сферах дій ЄС.

Єврокомісія пропонує реформувати правила безпеки мережевих та інформаційних систем відповідно до директиви про заходи щодо високого загального рівня кібербезпеки в усьому Союзі з метою збільшення рівня кіберстійкості критично важливого державного та приватного секторів: лікарні, енергосистеми, залізниці, а також центри обробки даних, державні адміністрації, дослідницькі лабораторії та виробництво критично важливих медичних виробів та ліків, а також іншої критичної інфраструктури та послуг.

Комісія також пропонує запустити мережу операційних центрів безпеки по всьому ЄС, що працюють на основі штучного інтелекту, що буде справжнім «щитом кібербезпеки» для ЄС, здатного досить рано виявляти ознаки кібератаки та забезпечувати активність дії до виникнення пошкодження.

Додаткові заходи включатимуть спеціальну підтримку малого та середнього бізнесу в рамках центрів цифрових інновацій, а також посилення зусиль для підвищення кваліфікації робочої сили, залучення та збереження найкращих талантів у галузі кібербезпеки та інвестування у відкриті наукові дослідження та інновації, конкурентоспроможні та засновані на досконалості.

ЄС активізує роботу з міжнародними партнерами з метою зміцнення глобального порядку, заснованого на правилах, сприяння міжнародній безпеці та стабільності в кіберпросторі та захисту прав людини та основних свобод в

Інтернеті. Він сприятиме розвитку міжнародних норм та стандартів, що відображають основні цінності ЄС, співпрацюючи зі своїми міжнародними партнерами в ООН.

ЄС і надалі зміцнюватиме свій набір інструментів кібердипломатії ЄС та збільшуватиме зусилля з розбудови кібернетичного потенціалу для країн третього світу шляхом розробки порядку денного розбудови зовнішнього кіберпотенціалу ЄС. Буде активізований кібердіалог з регіональними та міжнародними організаціями, а також спільнотою з багатьма зацікавленими сторонами. ЄС також сформує мережу кібердипломатії у всьому світі для просування свого бачення кіберпростору.

ЄС прагне підтримувати нову стратегію кібербезпеки, щоб перейти на новий рівень кібербезпеки протягом наступних семи років через наступний довгостроковий бюджет, зокрема програму цифрової Європи та Horizon Europe. Таким чином, державам рекомендується повною мірою використовувати механізм відновлення та стійкості для посилення кібербезпеки та відповідності інвестиціям на рівні ЄС. Мета полягає в тому, щоб досягти до 4,5 млрд. євро спільних інвестицій з державами, зокрема в рамках центру компетенції з питань кібербезпеки та мережі координаційних центрів.

Стратегія також спрямована на зміцнення промислового й технологічного потенціалу ЄС у галузі кібербезпеки, в тому числі за допомогою проектів, що підтримуються спільно з ЄС та національними бюджетами. ЄС має унікальну можливість об'єднати свої активи для підвищення своєї стратегічної автономії та просування свого лідерства в галузі кібербезпеки у цифровому ланцюжку поставок (включаючи дані та хмари, процесорні технології наступного покоління, надзахищені підключення та мережі 5G) відповідно до своїх цінностей та пріоритетів [37].

Існуючі заходи на рівні ЄС, спрямовані на захист ключових послуг та інфраструктур як від кібератак і від фізичних ризиків, потребують оновлення. Ризики кібербезпеки продовжують розвиватися із зростанням цифровізації та взаємозв'язку. Фізичні ризики також ускладнилися після прийняття у 2008 р.

правил ЄС щодо критичної інфраструктури [38], які наразі охоплюють лише енергетичний і транспортний сектори. Ці перегляди мають на меті оновити правила, дотримуючись логіки кіберстратегії Європейського Союзу.

Відповідно до Стратегії кібербезпека має бути інтегрована в усі ці цифрові інвестиції, зокрема в такі ключові технології, як штучний інтелект, шифрування та квантові обчислення, використовуючи стимули, зобов'язання й контрольні показники. Це буде стимулювати зростання європейської індустрії кібербезпеки та забезпечити упевненість, необхідну для полегшення поступової відмови від застарілих систем. Запобігання зловживанням технологіями, захист критичної інфраструктури та забезпечення цілісності ланцюгів постачання також уможливлює дотримання ЄС норм, правил і принципів відповідальної поведінки.

Таким чином, можна запропонувати такі основні етапи розвитку кібербезпекової політики ЄС (Таблиця 2.1).

Таблиця 2.1.

Етапи розвитку політики кібербезпеки ЄС

Роки	**Здобутки**
до 2001	Зародження кібербезпекової політики ЄС
2001 - 2004	Прийняття та реалізація першого стратегічного документу «Безпека мереж та інформації: пропозиції до європейської політики»
2004 - 2012	Утворення і розвиток Агентство ЄС з мережевої та інформаційної безпеки агентства ENISA
2013 - 2016	Стратегія кібербезпеки «Відкритий, надійний і безпечний кіберпростір»
2017 - 2019	Стратегія кібербезпеки «Стійкість, стримування та захист: побудова міцної кібербезпеки для ЄС»
з 2020	Стратегія кібербезпеки ЄС на цифрове десятиліття

2.3 Законодавче й інституційне забезпечення протидії кіберзлочинності в ЄС

Проблема запобігання і протидії кіберзлочинності займає одне із центральних місць у політиці безпеки Європейського Союзу. Про це свідчить, зокрема, велика кількість нормативних актів, присвячених питанням кіберзлочинності безпосередньо, а також їх регулювання в законах з кібербезпеки.

Основою усіх діючих документів щодо правопорушень у кіберпросторі є насамперед положення Конвенції Ради Європи про кіберзлочинність [9], яка наголошує на необхідності законодавчого регулювання питань зупинення правопорушень в комп'ютерних системах, мережах та їх використання в злочинних цілях, проти комп'ютерних даних, а також встановлення кримінальної відповідальності за їх вчинення, сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньо-державному, так і на міжнародному рівнях.

Перелічені нижче нормативні акти ЄС свідчать, що Єврокомісія добре розуміє обсяги та потенційні наслідки впливу кіберзлочинності на економіку й соціально-політичну систему ЄС, а також потребу в захищеності ключових інтересів і прав громадян Євросоюзу. Тим більше, що масштаби та складність кібератак постійно зростають, а кіберзлочинці використовують все більш витончені методи для проникнення в інформаційні системи, викрадення важливих даних з метою викупу, економічного шпигунства та фінансованої іншими державами протиправної діяльності в кіберпросторі.

Питання подолання кіберзлочинності регулюють, зокрема, такі нормативні документи Єврокомісії:

– Директива про атаки на інформаційні системи (2013), яка спрямована на боротьбу з широкомасштабними кібератаками, вимагає від країн ЄС посилити національне законодавство про кіберзлочинність і запровадити більш

жорсткі кримінальні санкції. Директива до найбільш значущих відносить такі види кіберзлочинів: створення та використання ботнетів; загальні злочини з метою незаконного доступу і втручання в інформаційну систему, незаконного втручання в дані та незаконного перехоплення; атаки об’єкти критичної інфраструктури ЄС і держав-членів; викрадення особистих даних та інші злочини, пов'язані з особистими даними [17].

– Стратегія кібербезпеки (2013) наряду з іншими виділяє завдання щодо різкого скорочення обсягів кіберзлочинності, відзначаючи, що першим чинником успішної протидії кіберзлочинності є сильне та ефективне законодавство як загального характеру, так і спрямованого на подолання окремих видів кіберзлочинів, наприклад сексуальної експлуатації дітей в Інтернеті та дитячої порнографії, ускладнених атак на інформаційні системи з використанням ботнетів [15].

Відзначено, що для боротьби з кіберзлочинністю необхідно забезпечити розширення оперативного потенціалу, покращити координацію на рівні ЄС, держав-членів, об’єднати зусилля правоохоронних і судових органів, державних і приватних зацікавлених сторін з ЄС та за його межами.

– Стратегія кібербезпеки (2017) для подолання кіберзлочинності ставить такі завдання: забезпечення швидкого реагування на кібератаки як чинника пом’якшення їхнього впливу; вдосконалення механізмів виявлення зловмисників; підвищення ефективності реагування правоохоронних органів; поглиблення державно-приватного співробітництва проти кіберзлочинності; посилення стримування кібербезпеки через держав-членів, а також розвиток міжнародного співробітництва у запобіганні, реагуванні й розслідуванні кіберінцидентів [32].

Стратегія для цифрового десятиліття (2020), яка наголошує на проблемі розширення масштабів і появі нових форм кіберзлочинів передбачає виконання широкого переліку завдань, значна частина з яких безпосередньо пов’язані з протидією кіберзлочинності. Так, для досягнення цілі з розбудови операційної спроможності для запобігання, стримування та реагування на кіберінциденти

заплановано створення спільного кіберпідрозділу для співпраці між різними спільнотами з кібербезпеки ЄС; підвищення ефективності боротьби з кіберзлочинністю; розробка і впровадження набору інструментів кібердипломатії ЄС; посилення можливостей кіберзахисту.

Види кіберзлочинів. Незважаючи на те, що в законодавчих документах немає визначень поняття кіберзлочинність (cybercrime) таку інформацію можна знайти на офіційних сторінках установ ЄС, зокрема на сайті Директорату міграції та внутрішніх справ зазначено, що кіберзлочинність складається із злочинних дій, вчинених в Інтернеті з використанням електронних комунікаційних мереж та інформаційних систем.

У ЄС кіберзлочинність класифікують за трьома широкими визначеннями:

– злочини, характерні для Інтернету, такі як атаки на інформаційні системи або фішинг (наприклад, фальшиві веб-сайти банків для запиту паролів, що дозволяють отримати доступ до банківських рахунків жертв);

– онлайн-шахрайство та підробка: широкомасштабне шахрайство може бути скоєне онлайн за допомогою таких інструментів, як крадіжка особистих даних, фішинг, спам і шкідливий код;

– незаконний онлайн-контент, включаючи матеріали сексуального насильства над дітьми, підбурювання до расової ненависті, підбурювання до терористичних актів і прославлення насильства, тероризму, расизму та ксенофобії [39].

Крім того, багато видів злочинності, включно з тероризмом, торгівлею людьми, сексуальним насильством над дітьми й торгівлею наркотиками, перемістилися в Інтернет або їм сприяють онлайн. Як наслідок, більшість кримінальних розслідувань мають цифрову складову.

Відповідно до глосарію Європейського центру боротьби з кіберзлочинністю (EC3) до злочинів у сфері високих технологій відносять (Рис. 2.1):

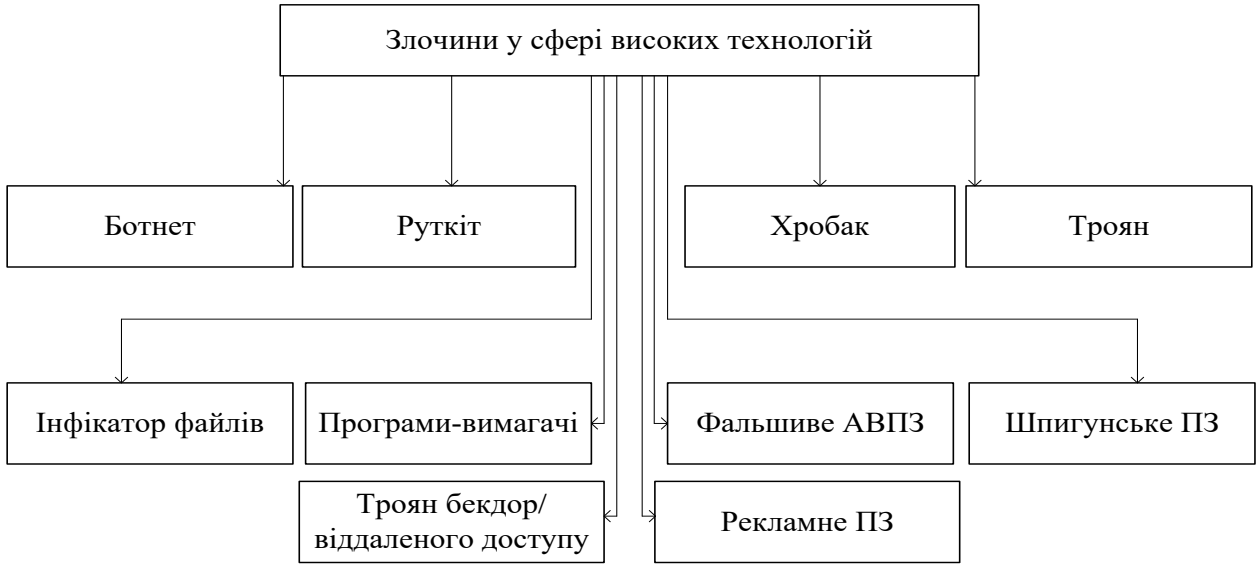

Рис. 2.1. Злочини у сфері високих технологій

Ботнет (скорочення від robot network) складається з комп'ютерів, які контактують один з одним через Інтернет. Командно-контрольний центр використовує їх для надсилання спаму, проведення розподілених атак типу «відмова в обслуговуванні» (DDoS) та вчинення інших злочинів.

Руткіт набір програм, які забезпечують доступ до комп'ютера або комп'ютерної мережі на рівні адміністратора, дозволяючи зловмиснику отримати root або привілейований доступ до комп'ютера та, можливо, інших машин у тій же мережі.

Хробак розмножується в комп'ютерній мережі та виконує шкідливі дії без керівництва.

Троян, який видає себе за законну програму або вбудований у неї, розроблено для зловмисних цілей, таких як шпигунство, викрадення даних, видалення файлів, розширення ботнету та виконання DDoS-атак.

Інфікатор файлів заражає виконувані файли (наприклад, .exe), перезаписуючи їх або вставляючи заражений код, який їх вимикає.

Троян бекдор/віддаленого доступу (RAT) отримує віддалений доступ до комп'ютерної системи або мобільного пристрою. Він може бути встановлений іншим шкідливим ПЗ. Це дає майже повний контроль зловмиснику, який може виконувати широкий спектр дій, зокрема:

– моніторинг дій, виконання команд;

– відправка файлів і документів назад зловмиснику;

– реєстрація натискань клавіш;

– робити знімки екрана.

Програми-вимагачі не дозволяють користувачам отримати доступ до їхніх пристроїв і вимагають від них заплатити викуп за відновлення доступу, здійснивши певні онлайн-платежі. Варіант поліцейського програмного забезпечення-вимагача використовує символи правоохоронних органів, щоб надати авторитетності повідомленню про викуп.

Підроблене антивірусне програмне забезпечення (Scareware), яке нібито сканує і знаходить шкідливі програми/загрози безпеці на пристрої користувача, щоб він заплатив за його видалення.

Шпигунське програмне забезпечення встановлюється на комп'ютер без відома власника, щоб контролювати його діяльність і передавати інформацію третій стороні.

Рекламне ПЗ відображає рекламні банери або спливаючі вікна, які містять код для відстеження поведінки користувача в Інтернеті [39].

Законодавство щодо протидії окремим видам кіберзлочинів. Як наголошено вище в законодавстві ЄС введені в дію перелік нормативних актів, що регулюють питання протидії окремим видам злочинів у кіберпросторі, зокрема:

– Пропозиція тимчасового положення про обробку персональних та інших даних з метою боротьби з сексуальним насильством над дітьми, оновлена у 2020 році [40].

– Директива щодо шахрайства з безготівковими платежами, оновлена у 2019 році [41].

– Пропозиції щодо Регламенту й Директиви, що сприяють транскордонному доступу до електронних доказів для кримінальних розслідувань.

– Директива про боротьбу з сексуальною експлуатацією дітей в Інтернеті та дитячою порнографією [42].

Інституційне забезпечення протидії кіберзлочинам. Крім законодавчої підтримки процесів подолання кіберзлочинності Єврокомісія забезпечила створення кількох важливих органів із загальносоюзними повноваженнями.

Координаційним органом із багатьох питань кібербезпеки, в т.ч. подолання кіберзлочинності, є Агентство ЄС з мережевої та інформаційної безпеки ENISA [43], засноване в 2004 році. ENISA займається забезпеченням високого загального рівня кібербезпеки в Європі, зокрема співпрацює з державами-членами та органами ЄС, сприяє обміну інформацією і знаннями, підвищенню обізнаності з кібербезпеки тощо.

Спеціалізовані повноваження щодо боротьби з кіберзлочинністю має Європейський центр боротьби з кіберзлочинністю (EC3), який був створений у 2013 році у складі Європейського поліцейського управління (Європол), щоб посилити реагування правоохоронних органів на кіберзлочинність у ЄС і допомогти захистити європейських громадян, підприємства та уряди [44].

EC3 здійснює аналіз і розвідку кіберзагроз, підтримує розслідування, забезпечує криміналістику високого рівня, сприяє співпраці і створює канали для обміну інформацією між компетентними органами держав-членів, приватним сектором та іншими зацікавленими сторонами.

Щороку EC3 публікує Оцінку загрози організованої злочинності в Інтернеті (IOCTA) [45], яка встановлює пріоритети для Оперативного плану дій EMPACT у сфері кіберзлочинності [46].

Агентство Європейського Союзу з питань співробітництва у сфері кримінальної юстиції (Євроюст), визначає основні перешкоди судовому співробітництву щодо розслідувань кіберзлочинів і координації між державами-членами та третіми країнами, підтримує розслідування кіберзлочинів як на оперативному, так і на стратегічному рівнях [47]. ·

Європейський поліцейський коледж (CEPOL) відповідає за координацію процесів розробки і планування навчальних курсів для правоохоронних органів з питань ефективної боротьби з кіберзлочинністю.

Завдяки впровадженню цих інституційних механізмів ЄС досяг помітних успіхів на операційному рівні, зокрема налагодження ефективної координації між інституціями ЄС, держав-членів та партнерами з приватного сектору для проведення багатьох успішних операцій проти широкомасштабних атак ботнетів і зловмисного ПЗ, великого форуму кіберзлочинців, а також розслідування серйозних кіберзлочинів.

2.4 Наближення законодавства України до нормативно-правової бази ЄС

Україна перебуває на черговому етапі імплементації до національного законодавства положень права ЄС щодо кібербезпеки та захисту об'єктів критичної інфраструктури. Законодавство щодо державного регулювання в зазначених сферах потребує суттєвого доопрацювання і корекції з огляду на необхідність тіснішої співпраці і взаємодії із ЄС, а в частині захисту об'єктів критичної інфраструктури - розробки повноцінної державної політики.

Узгодження процедур і протоколів взаємодії між Україною та ЄС може посилити загальну спільну безпеку кіберпростору не тільки в геополітичному вимірі, але й практичному - для уможливлення інтеграції України до цифрового ринку ЄС. Відповідно до Національного індексу кібербезпеки, за яким Естонська академія електронного врядування вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами, Україна посідає в рейтингу 25 місце з-поміж 152 країн [48].

Ключовими завданнями в рамках наближення законодавства України до законодавства ЄС задля поширення режиму внутрішнього ринку ЄС на базову

для цифрової економіки сферу комунікацій є імплементація актів ЄС у законодавство України. Інтеграція України до Єдиного цифрового ринку ЄС є одним із пріоритетних завдань для України.

Угода про асоціацію між Україною та ЄС [49] закладає чітке юридичне підґрунтя для досягнення цієї мети. Угода про асоціацію передбачає перспективу взаємного надання режиму внутрішнього ринку в секторі телекомунікаційних послуг. Відповідно до статті 4 Додатку XVII до Угоди про асоціацію, такий режим означає, що в цьому секторі не має бути обмежень щодо надання послуг українською юридичною особою на території ЄС і навпаки. Режим можна отримати за умови позитивного оцінювання Європейським Союзом кроків України з наближення нормативно-правових актів України до права ЄС.

Зближення ринків можливе за умови:

1) наближення нормативно-правового регулювання;

2) наявності тотожних регуляторів ринку та чіткого розподілу повноважень між органами, якщо регуляторів сфери, що належить до певного ринку, більш ніж один;

3) однакового або зрозумілого технічного регулювання і стандартизації сфери. Таким чином, інтеграція України до Єдиного цифрового ринку ЄС можлива за умови наближення усіх трьох складових до європейських норм, правил і стандартів.

У рамках виконання завдань забезпечення кібербезпеки України та створення можливостей для участі в Єдиному цифровому ринку ЄС Верховна Рада України ухвалила Закон України «Про основні засади забезпечення кібербезпеки України» [6] яким, зокрема, визначено сферу застосування закону, понятійний апарат, базові принципи, об'єкти та суб'єкти кібербезпеки й кіберзахисту, їхні завдання, способи державно-приватного партнерства, у тому числі й щодо формування і розвитку системи кіберзахисту об'єктів критичної інфраструктури.

На підставі зазначеного закону суб'єкти кібербезпеки та кіберзахисту

розробили низку під законних актів, якими затверджено порядок формування переліку об'єктів критичної інформаційної інфраструктури, порядок внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування; загальні вимоги щодо кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури; критерії формування переліку об'єктів критично інформаційної інфраструктури. Але більшість із них досі залишаються у статусі проєктів.

З огляду на важливість та актуальність завдань щодо захисту об'єктів критичної інфраструктури, зокрема критичної інформаційної інфраструктури, уряд ухвалив Концепцію створення державної системи захисту критичної інфраструктури [50], якою визначено шляхи і способи розв'язання проблем забезпечення захисту критичної інфраструктури.

Реалізація Концепції сприятиме:

– створенню державної системи захисту критичної інфраструктури, здатної забезпечувати належний рівень захисту такої інфраструктури від усіх видів загроз;

– виробленню механізмів ефективного реагування у разі виникнення кризових ситуацій та ліквідації їх наслідків, а також швидкому відновленню функціонування об’єктів критичної інфраструктури;

– налагодженню ефективної взаємодії між усіма суб’єктами державної системи захисту критичної інфраструктури за активної підтримки суспільства, місцевих громад, засобів масової інформації та недержавних дослідних інституцій, що вивчають проблеми безпеки та оборони;

– гармонізації законодавства України у сфері захисту критичної інфраструктури із законодавством ЄС;

– міжнародному співробітництву у сфері захисту критичної інфраструктури та інтеграції України до міжнародних систем захисту критичної інфраструктури.

Угодою про асоціацію прямо не передбачено зобов'язань щодо імплементації актів ЄС з кібербезпеки та захисту об'єктів критичної інфраструктури. Але оскільки вони є фундаментальними засадами Єдиного цифрового ринку ЄС, а Україна має на меті приєднатися до нього, постала необхідність визначити механізми й процедури імплементації актів.

Формування та розвиток національної системи заходів протидії кіберзлочинності та кібертероризму в Україні з урахуванням міжнародно-правових документів, стратегій кібербезпеки інших країн ЄС розпочалося у 2011 році з прийняттям Рішення РНБО України «Про виклики та загрози національній безпеці України у 2011 році» та відповідного Указу Президента України № 1119/2010 від 10 грудня 2010 року (обидва документи наразі не є чинними), за участю СБУ передбачалася підготовка пропозицій щодо створення єдиної національної системи боротьби з кіберзлочинністю та переліку об'єктів, які мають важливе значення для забезпечення національної безпеки і оборони України і потребують першочергового захисту від кібератак.

Окреме місце в процесі вдосконалення вітчизняного законодавства займає Стратегія кібербезпеки України 2016 року. Метою цієї стратегії було визначено створення необхідних умов для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави. Стратегія спрямовувалася на розвиток спроможностей сектору безпеки і оборони для боротьби з кіберзлочинністю, протидії кібератакам на електронні інформаційні ресурси держави та об'єкти критичної інфраструктури, протидії розвідувально-підривній діяльності, спрямованій проти України з боку іноземних спеціальних служб, організацій, груп та окремих осіб у кіберпросторі. Документ передбачав необхідність підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кіберзлочинності [51]. Зазначена стратегія втратила чинність із прийняттям нової стратегії кібербезпеки України 2021 року.

Стратегія кібербезпеки України 2021 року [52] окреслила загрози й виклики кібербезпеці у глобальному контексті, визначила здобутки і недоліки

реалізації попередньої стратегії. Серед основних загроз кібербезпеці України поряд з гібридною агресією РФ проти України у кіберпросторі, кібертероризмом, кібершпигунством документ виділяє кіберзлочинність, що завдає шкоди інтересам держави і суспільства, призводить до значних матеріальних втрат.

Відповідно до Стратегії з метою протидії кіберзлочинності необхідним є досягнення таких цілей:

– забезпечення набуття органами правопорядку та спецпризначення спроможностей для мінімізації загроз кіберзлочинності, посилення їх кадрового і технологічного потенціалу для запобігання і розслідування кіберзлочинів;

– запровадження заходів щодо національної кіберготовності й кіберстійкості в умовах кібератак в інтересах забезпечення економічного добробуту та захисту прав і свобод кожного громадянина України;

– підготовка висококваліфікованих фахівців у сфері кібербезпеки, які забезпечать ефективне запобігання і протидію кіберзлочинності;

– сприяння розвитку кіберобізнаності громадян щодо сучасних кіберзагроз та їх протидії;

– розвиток партнерських відносин з іншими державами й міжнародними організаціями у сфері кібербезпеки, в тому числі обмін інформацією, проведення спільних кібероперацій і розслідування кіберзлочинів тощо.

Водночас, варто наголосити на особливій важливості Закону України «Про основні засади забезпечення кібербезпеки України» [6], який закладає основи створення й розвитку національної системи протидії кібертероризму в Україні, в якому зазначено, що кібербезпека є важливим для України інтересом людини і громадянина, суспільним, державним та національним інтересом.

Закон встановлює правові й організаційні засади забезпечення захисту інтересів, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій та інших суб'єктів, а, отже, є комплексним спеціальним законодавчим актом у сфері кібербезпеки.

Українське законодавство гарантує демократичний цивільний контроль над національними збройними силами та правоохоронними органами, що діють у сфері кібербезпеки, зазначаючи що розвиток і захист кіберпростору має бути складовою державної політики у сфері впровадження електронного урядування, забезпечення безпеки та сталого функціонування електронних комунікацій і національних електронних інформаційних ресурсів, розвитку інформаційного простору та інформаційної інфраструктури. Відповідно до законодавства України, обов’язковим є забезпечення демократичного цивільного контролю над національними збройними силами та правоохоронними органами, що діють у сфері кібербезпеки.

Висновки до розділу 2

Аналіз нормативно-правового забезпечення кібербезпеки ЄС засвідчив наявність п'яти стратегічних пріоритетів кібербезпеки: досягнення кіберстійкості; зменшення кіберзлочинності; розробка політики та можливостей кібероборони; розвиток промислових і технологічних ресурсів для кібербезпеки; встановлення послідовної міжнародної політики щодо кіберпростору для ЄС.

З’ясовано, що проблема запобігання і протидії кіберзлочинності займає одне із центральних місць у політиці кібербезпеки ЄС, про що свідчить, зокрема, велика кількість нормативних актів, які регламентують питання протидії кіберзлочинності, зокрема: Конвенція Ради Європи про кіберзлочинність, Директива про атаки на інформаційні системи, стратегії кібербезпеки 2013, 2017 та 2020 років, нормативні акти щодо окремих видів злочинів у кіберпросторі.

Також на рівні ЄС діють кілька важливих органів із повноваженнями у сфері протидії кіберзлочинності: Агентство ЄС з мережевої та інформаційної

безпеки (ENISA), Європейський центр боротьби з кіберзлочинністю (ЕС3), Євроюст, Європейський поліцейський коледж (CEPOL), завдяки скоординованим діям яких досягнуто помітних успіхів у боротьбі з кіберзлочинністю.

Як показало дослідження, основними напрямками адаптації кращих практик ЄС щодо боротьби з кіберзлочинністю у вітчизняну систему забезпечення кібербезпеки є гармонізації законодавства України із законодавством ЄС; інтеграція України до Єдиного цифрового ринку ЄС; розробка і впровадження комплексу заходів протидії кіберзлочинності в Україні з урахуванням нормативно-правових актів ЄС; узгодження процедур і протоколів взаємодії між Україною та ЄС у сфері кібербезпеки, зокрема забезпечення обміну інформацією, проведення спільних кібероперацій, розслідування кіберзлочинів тощо.

Розділ 3
ЗАСАДИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ КІБЕРЛОЧИНОСТІ В УКРАЇНІ НА ОСНОВІ МІЖНАРОДНОГО ДОСВІДУ

3.1 Державна політика у сфері протидії кіберзлочинності в Україні та міжнародні практики

Нормативно-правова база України у сфері кіберзлочинності має ряд протиріч, що суттєво заважає в ефективній боротьбі проти такого роду злочинів. Проблеми забезпечення кібербезпеки вирішуються прийняттям Законів України та нормативних документів, що охоплюють регулювання кібербезпеки держави. На сьогодні діючими є правові та концептуальні засади, що закладені в таких нормативно-правових актах:

1. Закон України «Про інформацію», 1992 [53].
2. Закон України «Про державну таємницю», 1994 [54].
3. Закон України «Про захист інформації в інформаційно-комунікаційних системах», 1994 [55].
4. Закон України «Про електронні довірчі послуги», 2017 [56].
5. Закон України «Про національну безпеку України», 2018 [57].
6. Закон України «Про основні засади забезпечення кібербезпеки України», 2017 [6].
7. Закон України «Про електронні комунікації», 2020 [58].
8. Постанова Кабінету Міністрів України «Про затвердження загальних вимог щодо забезпечення кіберзахисту об'єктів критичної інфраструктури», 2019 [59].
9. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України», 2017 [60].
10. Указ Президента України «Про рішення Ради національної безпеки і

оборони України «Про Стратегію національної безпеки України», 2020 [61];

11. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», 2021 [62];

12. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію інформаційної безпеки», 2021 [63];

13. Кримінальний кодекс України (стаття 15. Контроль за законністю заходів кібербезпеки в Україні) [64] тощо.

Невідповідність термінів в законодавчих актах ускладнює нейтралізацію та понесення відповідальності за здійснене в правовому полі. Так у Законі України «Про національну безпеку України» використовуються терміни «комп'ютерна злочинність» та «комп'ютерний тероризм». Проблема полягає у тому, що ані в вищезгаданому документі, ані в інших нормативних актах не має чіткого визначення цих термінів. Навіть якщо звернутися до тексту Закону України «Про боротьбу з тероризмом», ми взагалі не побачимо визначення поняття «комп'ютерний тероризм» [65].

Закон України «Про захист інформації в інформаційно-комунікаційних системах» та документи, що супроводжують цей документ, мають застарілу інформацію і не відповідають сучасності. Адже усім відомо, що ІТ-прогрес не стоїть на місці, а розвивається семимильними кроками. Згідно з цим Законом, на державних підприємствах, у приватних компаніях Інтернет-провайдери мають застосовувати комплексну систему захисту інформації, яка вже багато років є неефективною і застарілою.

Такий стан речей призводить до проблем у координації діяльності правових структур і нейтралізації злочинів на правовому рівні, що впливає на комплекс процедур із запобігання і протидії кіберзлочинам.

Наступною проблемою державної політики в сфері кібербезпеки, на наш погляд, є неефективна робота системи кіберрозвідки. Адже, є приклади, коли приватний сектор попереджував державні органи про зовнішні кібератаки, однак влада належним чином не прореагувала. В умовах війни на високому фаховому рівні має працювати кіберрозвідка.

Основними перспективами державної політики в сфері кіберзахисту є визначення ключових принципів і напрямків покращення кібербезпеки в Україні. Основна ідея - дозволити приватному сектору процес саморегуляції, тобто самостійно виявляти й визначати стандарти кібербезпеки суто для тієї галузі, яка цього потребує. В даному випадку, держава буде виступати не як регулятор, а як вищий орган, що надає допомогу у вирішенні проблем кібербезпеки на законодавчому рівні.

Таким чином, з вказаного вище можна узагальнити проблеми державної політики у сфері кіберзахисту:

1. неузгодженість у визначенні термінів у законодавчих актах;

2. відсутність роз'яснень щодо повноважень державних структур, які вирішують питання кібератак;

3. використання застарілих систем захисту Інтернет-провайдерами, які підпорядковані державі.

Виходячи з аналізу основних проблем, впровадження державної політики у сфері кібербезпеки вимагатиме дотриманням таких вимог:

– вдосконалити нормативну правову базу;

– оновити систему захисту;

– дозволити приватному сектору самостійно регулювати свій кіберзахист і запровадити галузеві стандарти кібербезпеки;

– для мінімізації збитків від кібератак потрібно не лише захищати, алей належним чином прогнозувати кібератаки й інциденти безпеки;

– формувати культуру кібербезпеки і забезпечити дотримання правил кібергігієни;

– мотивувати молодь отримувати спеціальності в галузі ІТ та кібербезпеки. Це завдання має виконувати саме держава.

Міжнародне середовище відіграє важливу роль у протидії кіберзлочинності в Україні. Основними партнерами України є Європейський Союз і Сполучені Штати Америки, а їх нормативно-правове та інституційне

забезпечення кібербезпеки є для нашої держави зразком передового досвіду і основою для гармонізації законодавства у цій сфері.

Загальні положення про кібербезпеку ЄС викладені в таких документах:

- Конвенція Ради Європи про кіберзлочинність, 2001 [9].

- Директива Європейського Парламенту та Ради «Про обробку персональних даних і захист приватності у сфері електронних комунікацій» (Директива про захист приватності й електронні комунікації), 2002.

- Спільне звернення Європейського Парламенту і Ради «Стратегія кібербезпеки ЄС: відкритий, безпечний і надійний кіберпростір», 2013 [15].

- Директива ЄС «Про заходи щодо забезпечення високого рівня безпеки спільних мереж та інформаційних систем в ЄС», 2016.

- Загальний регламент захисту даних (GDPR), 2016 [26].

- Повідомлення Єврокомісії і Ради «Зміцнення європейської системи кіберстійкості та розвиток конкурентоспроможної та інноваційної індустрії кібербезпеки», 2016 [66].

- Рекомендація Єврокомісії «Про скоординоване реагування на великі інциденти та кризи у сфері кібербезпеки», 2017.

- Спільне звернення Європейського Парламенту і Ради «Стійкість, стримування та оборона: розбудова стійкої кібербезпеки для ЄС», 2017 [31].

- Регламент ЄС «Про ENISA та сертифікацію кібербезпеки інформаційно-комунікаційних технологій (Закон про кібербезпеку), 2019.

- Рекомендація Єврокомісії «Про кібербезпеку в мережах 5G», 2019.

У США галузь кібербезпеки регулюється такими законодавчими актами:

- Акт про конфіденційність електронних комунікацій (Electronic Communications Privacy Act, ECPA), 1986.

- Акт про комп’ютерні шахрайство та зловживання (Computer Fraud & Abuse Act, CFAA), 1986.

- Акт про мобільність та підзвітність медичного страхування (HIPAA), 1996.

- Акт про захист конфіденційності дітей в Інтернеті (Children’s Online

Privacy Protection Act, COPPA, 1998.

- Акт про захист національної кібербезпеки, 2014.
- Закон про обмін інформацією з питань кібербезпеки, 2015.
- Каліфорнійський акт про конфіденційність споживачів (California Consumer Privacy Act, CCPA, 2018.
- Каліфорнійський акт про права на конфіденційність (California Privacy Rights Act, CPRA, 2023.
- Національна стратегія кібербезпеки США, 2023 [67].

Важливу роль у регламентуванні засад кібербезпеки та захисту інформації відіграє Національний інститут стандартів і технологій NIST, який опублікував понад 200 спеціальних публікацій серії 800 (NIST SP 800) з кібербезпеки [68], зокрема NIST SP800-82 Посібник з безпеки промислових систем управління, NIST SP 800-50 Створення програми підвищення обізнаності про IT- безпеку, NIST SP 800-40 Посібник з методів управління вразливостями, NIST 800-53Управління безпекою і конфіденційністю для федеральних інформаційних систем та агентств, NIST 800-53 Рекомендації з цифрової ідентифікації.

Важливу роль у взаємодії євроатлантичного і євразійського просторів у сфері кібербезпеки відіграє діяльність міжнародних і регіональних безпекових інститутів таких як ООН, ОБСЄ, НАТО, ЄС, Рада Європи. Ці органи працюють разом, щоб охопити якомога ширший спектр питань безпеки й уникнути дублювання функцій. ООН відіграє особливу роль у вирішенні питань міжнародного співробітництва в боротьбі з кіберзлочинністю і постійно обговорює питання запобігання та боротьби з комп'ютерними злочинами.

Роль ОБСЄ І НАТО полягає в регулюванні й запобіганні конфліктам, недопущення кризового становища, а також реагування на безпекові виклики. ОБСЄ виступає регулятором в обговоренні питань світового рівня, які є важливими для загальної безпеки. Країни-члени НАТО та ОБСЄ обмінюються

інформацією з питань кібербезпеки, співпрацюють у виявленні та реагуванні на кіберінциденти. Тісна співпраця між НАТО, ЄС і ОБСЄ є одним з елементів комплексного підходу до врегулювання криз, який вимагає ефективного використання як військових, так і цивільних інструментів [69].

На підставі ст. 14 Закону України «Про основні засади кібербезпеки в Україні» регламентовано такі засади міжнародного співробітництва:

1. Україна відповідно до укладених міжнародних договорів здійснює співпрацю з іноземними державами;

2. Україна, відповідно до міжнародних договорів, може приймати участь у спільних міжнародних заходах з обговорення питань захисту в сфері кібербезпеки в рамках дозволеного з боку Верховної ради України;

3. Відповідно да законодавства України, держава може приймати участь в міжнародній співпраці з іноземними державами в рамках своїх повноважень;

4. На підставі запиту з боку міжнародного співтовариства надавати інформацію щодо кібербезпеки державам, які цього потребують [6].

Для реалізації таких заходів важливо вивчити міжнародний досвід міжнародних організацій у цій сфері, вжиті ними заходи та ефективність їх впровадження.

Держави-члени НАТО акцентують увагу на налагодженні сталого діалогу між країнами та запровадження дієвих механізмів протидії викликами, якими супроводжується їх діяльність у кіберпросторі. Відкрита інформаційна сфера, відповідальна поведінка держав в сфері кібербезпеки, довіра в обміні інформацією, заходи нарощування потенціалу безпеки в кіберпросторі - це пріоритетні напрямки країн НАТО.

3.2 Особливості реалізації міжнародних практик у запобіганні та протидії кіберзлочинності в Україні

Кіберстійкість вимагає від суб’єктів кібербезпеки ефективно та вчасно реагувати на кібератаки, забезпечувати в режимі реального часу готовність до реагування на поточні та потенційні кіберзагрози. За таких умов важливою є організація управління реагуванням на інциденти інформаційної безпеки в рамках роботи відповідних груп. На сьогодні прикладами таких груп можуть слугувати:

Security Operations Center (SOC) - операційний центр безпеки, централізований підрозділ установи, який вирішує питання інформаційної та кібербезпеки на організаційному й технічному рівні. SOC - це об'єкт, де корпоративні інформаційні системи (веб-сайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп'ютери й інше кінцеве обладнання) контролюється, оцінюється та захищається.

Computer Emergency Response Team (CERT) - комп'ютерна група реагування на надзвичайні ситуації - назва груп експертів з комп'ютерної безпеки, що займаються збором інформації про інциденти, їх класифікацією і нейтралізацією [70].

Information Security Incident Response Team (CSIRT) - група IT-фахівців, яка надає організації послуги й підтримку щодо оцінки, управління та запобігання надзвичайним ситуаціям, пов’язаним з кібербезпекою, а також координації зусиль щодо реагування на інциденти [71].

Державні органи влади можуть використовувати один або більше з трьох основних типів команд реагування на інциденти: SOC, CERT і CSIRT. Іноді ці терміни використовуються синонімічно, хоча різниця залежить від того, як використовуються ці терміни.

Найбільш унікальною з цих трьох команд є SOC, який є спеціальний об'єктом, що контролює і захищає технології та обладнання, а також виконує

функції командно-адміністративного центру для організації, регіону чи країни. SOC захищає мережі, сервери, програми та кінцеві точки. Однак обов'язки SOC виходять за рамки реагування на інциденти.

CERT - це зареєстрована торгова марка, для використання якої необхідно отримувати офіційний дозвіл від Університету Карнегі-Меллона, без якого будь-яке використання буде незаконним. У той час, як у абревіатури CSIRT (вона ж CIRT, SIRT, CIRC, IRT, IRC, SERT) ніяких обмежень на використання немає.

CSIRT зазвичай є невеликою і формалізованою групою, яка нерідко формується для виконання певних завдань на певний період часу. Натомість CERT діє постійно і часто його співробітники займаються тільки завданнями, пов'язаними з реагуванням на інциденти.

Члени CSIRT можуть працювати в різних підрозділах організації (IT, ІБ, СБ, PR тощо), збиратися за потребою і працювати на ентузіазмі або не отримуючи за свою роботу жодної винагороди. Часто CSIRT працює тільки з внутрішніми інцидентами або інцидентами, спрямованими на внутрішні інформаційні активи організації. CERT не мають таких обмежень, працюючи з різними організаціями.

Ще однією відмінністю CERT від CSIRT є джерела інформації. CERT оперує тільки тим, що йому надсилають його клієнти: описи інцидентів, підозрілі файли, дампи пам'яті й мережевого трафіку. У CSIRT, яка зазвичай діє всередині конкретної компанії, більше можливостей отримувати дані безпосередньо від розкиданих мережею засобів захисту, мережевого устаткування, операційних і прикладних систем, СУБД та інших джерел інформації.

Державний центр кіберзахисту та протидії кіберзагрозам. На основі зазначених груп реагування в Україні з 2007 року розпочав свою діяльність спеціалізований структурний підрозділ Державної служби спеціального зв'язку та захисту інформації України - Державний центр кіберзахисту та протидії кіберзагрозам, який можна віднести до категорії SOC.

Основними завданнями Центру є:

– впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки;

– забезпечення створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет;

– забезпечення створення та функціонування системи антивірусного захисту національних інформаційних ресурсів;

– аудит інформаційної безпеки та стану кіберзахисту об’єктів критичної інформаційної інфраструктури;

– забезпечення створення та функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту;

– забезпечення створення та функціонування системи взаємодії команд реагування на комп’ютерні надзвичайні події;

– розробка сценаріїв реагування на кіберзагрози, заходів щодо протидії таким загрозам, програм і методик проведення кібернавчань у взаємодії з іншими суб’єктами забезпечення кібербезпеки;

– створення та забезпечення функціонування Національного центру резервування державних інформаційних ресурсів [72].

На базі Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку створений тренінговий кіберцентр. У тренінговому кіберцентрі проводяться кібернавчання і кібертренінги для фахівців із кібербезпеки та кіберзахисту, що працюють у складі команд (центрів) реагування на кіберінциденти основних суб’єктів забезпечення кібербезпеки, секторальних команд реагування та персоналу, відповідального за забезпечення кібербезпеки на об’єктах критичної інфраструктури держави.

Кібернавчання проводяться у навчальному мережевому середовищі для фахівців різного рівня кваліфікації. Одночасно в кібернавчаннях можуть брати участь до двох команд із максимальною кількістю учасників – 10 осіб у

кожній. Тренінги проводять у форматах «Кіберзахист», «Тестування на проникнення» та «War Game».

Формат «Кіберзахист» (англ. Cyber Defence Excercises, CDX, blueteaming – активний кіберзахист, навчання щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі) – це формат тренінгу, під час якого учасники здійснюють оборонні кібероперації: запобігають, виявляють та усувають наслідки кіберінцидентів / кібератак на умовний об'єкт критичної інформаційної інфраструктури.

Формат «Тестування на проникнення» (англ. pentesting, redteaming – тестування на проникнення, етичний хакінг, оцінка стану захищеності) – це формат тренінгу, під час якого учасники здійснюють наступальні кібероперації: виявляють вразливості умовного об'єкту критичної інформаційної інфраструктури та здійснюють кібератаки на нього.

Формат «WarGame» (англ. Red&Blue Team) – це формат тренінгу, учасники якого поділяються на дві команди суперників (агресор і жертва), що здійснюють наступальні та оборонні кібероперації на кіберполігоні [73].

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA. З 2009 року в Україні працює урядова команда реагування на комп'ютерні надзвичайні події CERT-UA. Підрозділ є акредитованим членом форуму команд реагування на інциденти безпеки FIRST, який об'єднує широкий спектр груп безпеки та реагування на інциденти, зокрема команди безпеки продуктів з урядового, комерційного та академічного секторів, у багатьох країнах світу. Це дає можливість звернутися за підтримкою щодо протидії кіберзагрозам у будь-яку з 326 команд у 73 країнах. З 2012 року CERT-UA також приєдналась до IMPACT (Міжнародне багатостороннє партнерство проти кібернетичних загроз).

Метою діяльності CERT-UA є забезпечення захисту державних інформаційних ресурсів, інформаційних і комунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності.

Завданнями урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA українським законодавством визначено:

– накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення й усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки і власників об'єктів кіберзахисту;

– підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту і протидії кіберзагрозам [74].

Усі зазначені підрозділи належать до структури управління Державної служби спеціального зв'язку та захисту інформації України.

Національна система кібербезпеки України. Агресія РФ, що триває й досі, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України, зокрема отримання безвізового режиму, що є знаковою подією для стратегічного розвитку України, вимагало невідкладного створення національної системи кібербезпеки як складової частини системи забезпечення національної безпеки України.

Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Рис. 3.1. Основні суб'єкти національної системи кібербезпеки України

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

1) Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, 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;

2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє

кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

4) Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;

5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний

банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг.

Координація діяльності національної системи кібербезпеки та у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

Національний координаційний центр кібербезпеки 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 [6].

Національна система кібербезпеки забезпечує взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Системи кібербезпеки провідних країн світу. Аналізуючи системи кібербезпеки провідних країн світу, доходимо висновку, що на сьогодні не існує уніфікованої моделі побудови національної системи кібербезпеки. Наприклад, відповідно до комплексного нормативно-правового акту США «Про внутрішню безпеку» 2002 року урядові структури, які займались забезпеченням комп'ютерної безпеки, перейшли під контроль цього новоствореного відомства.

Вказаний закон також посилив відповідальність за комп'ютерні злочини (включаючи довічне ув'язнення), зобов'язав Інтернет-провайдерів надавати інформацію про клієнтів за вимогою правоохоронних органів, розширив їх права щодо можливості перехоплення інформації (прослуховування телефонних переговорів і перлюстрацію електронних повідомлень) без дозволу

суду, визначив основні напрями діяльності федеральних органів із підвищення ефективності захисту критичної інфраструктури США від кібератак, зокрема об'єктів стратегічного значення, що перебувають у приватній власності [75].

Стратегія кібербезпеки Канади визначає кібертероризм і ворожі дії в кіберпросторі з боку інших країн (кібершпигунство і кібервійну) основними загрозами кібернетичній безпеці держави, а ключовим органом, на який покладена координація та контроль за імплементацією вказаної Стратегії, реалізація державної політики та координація заходів у сфері кібербезпеки та протидії кіберзагрозам, визначене Міністерство громадської безпеки Канади (Public Safety Canada).

Законом ФРН «Про посилення безпеки інформаційних систем» завдання попередження, реагування на інциденти, викликані кібернетичними загрозами, управління й координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема у взаємодії з приватним сектором, покладене на Федеральне відомство безпеки інформаційних систем (BSI) ФРН.

Головним державним органом Великої Британії, на який покладено завдання захисту критичної інфраструктури, мінімізації загроз її сталому функціонуванню, насамперед, від загроз тероризму, є Центр захисту національної інфраструктури (Centre for the Protection of National Infrastructure, CPNI). Крім того, у Великобританії наприкінці березня 2013 р. було створено Центр із протидії кібернетичним загрозам із метою попередження та нейтралізації кібернетичних атак на об'єкти критичної інфраструктури, а також швидкого реагування на скоєні правопорушення у цій сфері.

Стратегією кібернетичної безпеки Австрії національним координатором і центральним органом у сфері кібербезпеки визначено Центр боротьби з кіберзлочинністю Федерального міністерства внутрішніх справ Австрії (Cyber Crime Competence Center (C4) of the Federal Ministry of the Interior). Крім того, на нього покладено головні функції щодо здійснення правоохоронної діяльності у сфері кібербезпеки та боротьби з кіберзлочинністю.

Ключову роль у забезпеченні кібернетичної безпеки Польщі відіграє Агентство внутрішньої безпеки (АВБ) – польський контррозвідувальний орган. Так, у 2013 р. АВБ розробило Стратегію кібербезпеки Польщі та ініціювало створення Центру криптології при Міністерстві національної оборони Польщі, на який покладено завдання із захисту інформації, кібероборони та проведення наступальних кібероперацій (активний кіберзахист).

Ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації (РСІ) [75].

Враховуючи зазначене, варто відзначити, що наша національна система кібербезпеки є багатокомпонентною, а її мета полягає у забезпеченні функціонування та розвитку комплексу заходів і засобів кіберзахисту, і, як наслідок, забезпечення належного рівня кібербезпеки держави.

Аналіз нормативно-правових та організаційних основ системи кібербезпеки провідних країн світу свідчить про домінантну роль спецслужб у забезпеченні кібербезпеки держави, що пов’язано із характером кіберзагроз сьогодення, протидія яким потребує інструментарію (повноважень, форм і методів), притаманного виключно спеціальним, насамперед контррозвідувальним органам держави.

3.3 Методи запобігання та протидії кіберзлочинності в Україні

В умовах всеохоплюючої цифровізації всіх сфер життєдіяльності суспільства, яка несе як переваги широкого доступу й обміну інформацією, так і загрози кібератак та онлайн-шахрайства, запобігання і протидія кіберзлочинності стає важливою і обов’язковою складовою забезпечення національних інтересів України. Кіберзлочинність уже стала великою проблемою для всього світу, і її масштаби нестримно зростають. Україна також

намагається йти в ногу з часом. Законодавці ухвалюють нові закони, регулюючи проблеми, пов'язані з розвитком і безпекою кіберпростору, правоохоронні органи намагаються вчасно реагувати на кіберзагрози, формуються спеціальні підрозділи по боротьбі з кіберзлочинністю, посилюється міжнародна співпраця у сфері запобігання і розслідування комп'ютерних злочинів. Водночас варто пам'ятати, що кіберзлочин, як і будь-який інший, є не лише правовою, але і соціальною проблемою.

На сьогодні для нашої держави важливо створити уніфіковану класифікацію і формальну модель кіберзлочинів, які полегшать протидію і розслідування правопорушень з використанням ІКС. Організація і впровадження комплексу заходів забезпечення кібербезпеки повинна носити комплексний характер і ґрунтуватися на глибокому аналізі можливих негативних наслідків.

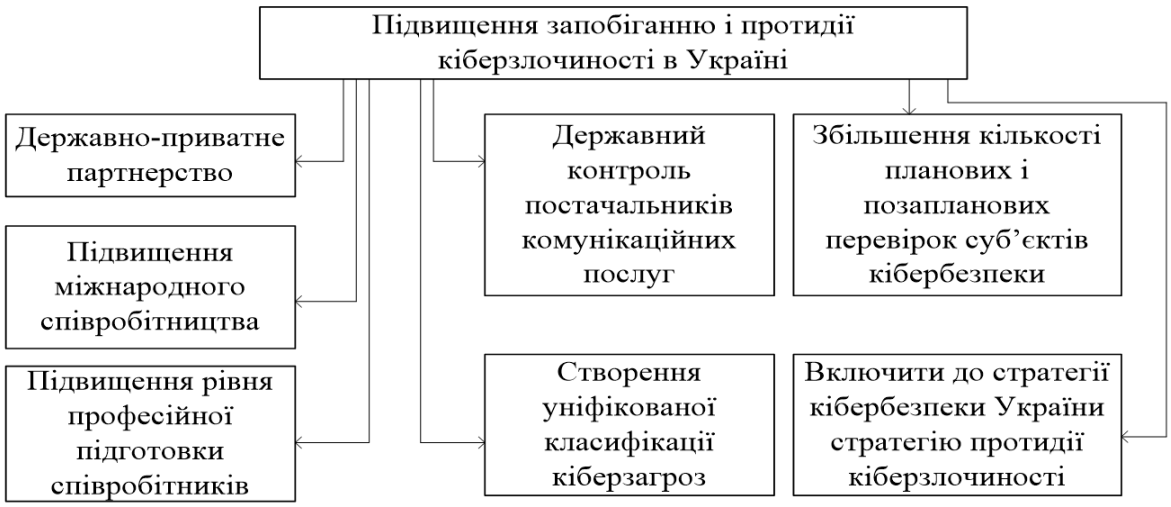

Рис. 3.2. Напрями запобігання та протидія кіберзлочинності в Україні

Запобігання кіберзлочинності складається зі стратегій і заходів, спрямованих на зниження ризику вчинення злочинів і нейтралізацію потенційно шкідливих наслідків для приватних осіб і суспільства загалом. У багатьох випадках стратегії протидії кіберзлочинності є невід'ємною частиною стратегій забезпечення кібербезпеки.

Дослідження, в тому числі проведені в країнах, що розвиваються, показують, що більшість індивідуальних користувачів Інтернету нині вживають

основні запобіжні заходи. У ході опитування представники урядів, організацій приватного сектора і наукових установ підкреслили значення інформаційно-просвітницьких кампаній з питань кібербезпеки, у тому числі щодо нових загроз. Респонденти також наголосили на необхідності орієнтувати інформаційні заходи на конкретні цільові групи, наприклад дітей. Організації приватного сектора також повідомляють, що обізнаність користувачів і співробітників має бути частиною комплексного підходу до забезпечення корпоративної безпеки.

Найбільша ефективність навчання користувачів досягається в разі поєднання навчання із системами, які допомагають користувачам безпечним чином досягти своїх цілей. Якщо витрати користувачів перевищують безпосередню отриману ними вигоду, у них зникає стимул застосовувати заходи безпеки. Відзначено такі принципи й оптимальні види практики:

– встановлення відповідальності за підвищення обізнаності;
– політика і практичні заходи у сфері управління ризиками;
– настанови на рівні вищого керівництва, зокрема рад директорів;
– професійна підготовка співробітників.

Дві третини респондентів з організацій приватного сектора провели оцінку ризику кіберзлочинності, і більшість повідомили про використання таких технологій забезпечення кібербезпеки, як:

– міжмережевий захист;
– збереження цифрових доказів;
– ідентифікація змісту даних;
– виявлення вторгнень;
– контроль і моніторинг системи.

У той же час було зазначено, що малі і середні підприємства або не впроваджують достатніх заходів для захисту систем від атак, або помилково вважають, що вони не стануть мішенню злочинців.

Важливу роль у запобіганні кіберзлочинності відіграє нормативно-правова база – як відносно приватного сектора в цілому, так і відносно постачальників послуг зокрема. Майже в половині країн ухвалені закони про захист інформації, які передбачають вимоги щодо захисту і використання персональних даних. Деякі з них містять конкретні вимоги до постачальників послуг Інтернету й інших постачальників електронних засобів зв'язку.

Хоча закони про захист інформації вимагають видаляти персональні дані, якщо немає потреби їх більше використовувати, в деяких країнах зроблені винятки для цілей карних розслідувань, згідно з якими постачальники Інтернет-послуг зобов'язані зберігати певні види даних упродовж певного терміну.

У багатьох розвинених країнах є також правила, що вимагають від організацій у разі витоку даних повідомляти приватних осіб і регулюючі органи. Постачальники Інтернет-послуг зазвичай несуть обмежену відповідальність як прості канали передачі даних. Модифікація переданого змісту даних підвищує міру відповідальності, так само як і фактичне або передбачуване знання про незаконну діяльність. З іншого боку, оперативне вжиття заходів після отримання повідомлення знижує міру відповідальності [76].

Незважаючи на наявність технічних можливостей, що дозволяють постачальникам послуг фільтрувати онлайн-контент, при обмеженні доступу до Інтернету їм необхідно дотримуватися критеріїв передбачуваності і співмірності, що передбачаються міжнародним правом у сфері прав людини, яке захищає право шукати, отримувати і передавати інформацію.

Центральним елементом у запобіганні кіберзлочинності є державно-приватне партнерство. Про наявність такого партнерства повідомляють респонденти з понад половини всіх країн. Це партнерство рівною мірою створюється як на підставі неофіційних домовленостей, так і на юридичній основі. Найчастіше партнерські відносини встановлюються з організаціями приватного сектора, за ними йдуть наукові установи, міжнародні й регіональні організації.

Партнерські відносини використовуються переважно для полегшення обміну інформацією про загрози і тенденції, а також для діяльності із

запобігання кіберзлочинності і вжиття заходів у конкретних випадках. У контексті деяких видів державно-приватного партнерства організації приватного сектора застосовують запобіжний підхід до проведення розслідувань і звернення в судові органи для боротьби з кіберзлочинністю. Такі заходи доповнюють зусилля правоохоронних органів і можуть допомогти понизити заподіюваний жертвам збиток.

Наукові організації виконують різноманітні функції у справі запобігання кіберзлочинності, у тому числі за допомогою навчання і професійної підготовки фахівців, розробки законодавчої бази і політики, а також підготовки технічних стандартів і пошуку рішень. В університетах працюють і використовують наявні можливості експерти з кіберзлочинності, різні групи реагування на комп'ютерні інциденти і спеціалізовані науково-дослідні центри.

У зв'язку зі зростаючою кількістю злочинів, пов'язаних з використанням комп'ютерів, чому сприяє створення глобальних міжнародних і публічних електронних мереж, великого значення набуває міжнародна співпраця і координація дій у цій сфері. Просвіта і підвищення обізнаності громадськості, без сумніву, сприяє скороченню кількості злочинів в електронному середовищі завдяки безпечній поведінці користувачів.

Транснаціональний характер кіберзлочинності дає підстави вважати, що розробка загальної політики з основних питань має бути частиною будь-якої стратегії боротьби зі злочинністю. Для розслідування кіберзлочинів потрібен персонал, що має конкретний судовий і технічний досвід і знання, а також наявність конкретних процедур.

Для ефективного розслідування таких злочинів держави можуть потребувати допомоги з боку інших держав. Така допомога охоплює як співпрацю персоналу правоохоронних органів у робочому порядку, так і офіційну взаємну правову допомогу через центральні органи влади. Необхідно, щоб реалізація викладених пропозицій на практиці сприяла підвищенню ефективності діяльності державних організацій, силових структур і спецслужб з метою запобігання і протидії злочинам, що здійснюються у кіберпросторі.

Висновки до розділу 3

Аналіз нормативно-правової бази України у сфері кібербезпеки засвідчив наявність низки проблем, серед яких неузгодженість у визначенні термінів, відсутність роз'яснень щодо повноважень державних структур, які протидіють кібератакам, відставання законодавства від практики кіберзахисту.

Виходячи з виявлених проблем, державна політика у сфері кібербезпеки та протидії кіберзлочинності має базуватися на дотриманні таких основних вимог: удосконалення нормативно-правової бази; оновлення систем захисту; надання приватному сектору можливості саморегулювання кіберзахисту і впровадження стандартів кібербезпеки; розвиток механізмів прогнозування кіберінцидентів; формування культури кібербезпеки у суспільстві; державна підтримка освітніх програм у галузі ІТ та кібербезпеки, їх пропагування серед молоді.

В умовах постійного збільшення кількості та видів кіберзагроз державні суб'єкти кібербезпеки мають ефективно та вчасно реагувати на кібератаки. З цією метою у 2007 році був створений Державний центр кіберзахисту та протидії кіберзагрозам Держспецзв'язку України, який відповідає за організаційно-технічне забезпечення національної системи кібербезпеки. На базі Центру діє тренінговий кіберцентр для підготовки фахівців з кібербезпеки. Також в Україні діє урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, метою якої є забезпечення захисту державних інформаційних ресурсів, ІКС від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності.

Встановлено, що національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і

технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури.

За підсумками дослідження окреслено основні напрями запобігання та протидії кіберзлочинності в Україні, зокрема посилення державного контролю щодо суб’єктів кібербезпеки; створення уніфікованої класифікації кіберзагроз; розробка стратегії протидії кіберзлочинності і включення її до стратегії кібербезпеки України; підвищення рівня підготовки фахівців з кібербезпеки та захисту інформації; налагодження державно-приватного партнерства і посилення міжнародної співпраці з питань подолання кіберзлочинності.

Вказані заходи потребують подальших наукових розробок для створення дієвих інструментів протидії сучасним викликам кіберзлочинності.

ВИСНОВКИ

У результаті аналізу законодавства й наукових джерел запропоновано розуміти під кіберзлочином (комп’ютерним злочином) будь-яке протиправне діяння, яке вчиняється завдяки електронним операціям, метою яких є подолання систем захисту комп'ютерних систем і даних, а під кіберзлочинністю - сукупність кіберзлочинів. Кіберзлочинності притаманні такі ознаки: відсутність кордонів; прихований характер; великі обсяги збитків у порівнянні з іншими кримінальними діями; складність вчасного виявлення й ідентифікації порушників; використання новітніх ІТ; взаємозв'язок з організованою злочинністю.

Встановлено, що наразі найпоширенішими є класифікації кіберзлочинів провідних міжнародних та європейських організацій, зокрема ООН, ОЕСР, Ради Європи (Конвенція про кіберзлочинність) та інших. У науковій літературі кіберзлочини поділяють на окремі види за такими критеріями як мета і мотиви правопорушення, роль комп’ютерних систем і мереж у їх здійсненні тощо.

Аналіз нормативно-правового забезпечення кібербезпеки ЄС показав, що проблема запобігання і протидії кіберзлочинності займає одне із центральних місць у політиці кібербезпеки ЄС. На основі вивчення нормативно-правових актів ЄС зроблено висновок про наявність стратегічних пріоритетів у галузі кібербезпеки: досягнення кіберстійкості; забезпечення кібероборони; зменшення кіберзлочинності; підтримка міжнародної співпраці щодо безпеки кіберпростору.

Інституційне забезпечення діяльності з кібербезпеки й подолання кіберзлочинності здійснюють такі інституції ЄС: Агентство ЄС з мережевої та інформаційної безпеки (ENISA), Європейський центр боротьби з кіберзлочинністю (ЕС3), Євроюст, Європейський поліцейський коледж (CEPOL).

Як показало дослідження, основними напрямками адаптації кращих практик ЄС щодо боротьби з кіберзлочинністю у вітчизняну систему забезпечення кібербезпеки є гармонізації законодавства України із законодавством ЄС; інтеграція України до Єдиного цифрового ринку ЄС; розробка і впровадження

комплексу заходів протидії кіберзлочинності в Україні з урахуванням норм законодавства ЄС; узгодження взаємодії між Україною та ЄС сфері кібербезпеки.

Встановлено, що національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, криптографічних, технічних та інших заходів з метою захисту національних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Аналіз нормативно-правової бази України у сфері кібербезпеки засвідчив наявність низки проблем, серед яких неузгодженість у визначенні термінів, відсутність роз'яснень щодо повноважень державних структур, які протидіють кібератакам, відставання законодавства від практики кіберзахисту.

Виходячи з цього, державна політика у сфері кібербезпеки та протидії кіберзлочинності має охоплювати: удосконалення нормативно-правової бази; оновлення систем захисту; надання приватному сектору можливості саморегулювання кіберзахисту і впровадження стандартів кібербезпеки; розвиток механізмів прогнозування кіберінцидентів; формування культури кібербезпеки у суспільстві; державна підтримка освітніх програм у галузі ІТ та кібербезпеки, їх пропагування серед молоді.

Ключову роль у запобіганні та протидії кіберзлочинності в Україні відіграють такі суб'єкти: Державний центр кіберзахисту та протидії кіберзагрозам Держспецзв'язку України, урядова команда реагування на комп'ютерні надзвичайні події CERT-UA.

За підсумками дослідження окреслено основні напрями подолання кіберзлочинності в Україні: посилення державного контролю щодо суб'єктів кібербезпеки; створення уніфікованої класифікації кіберзагроз; розробка стратегії протидії кіберзлочинності і включення її до стратегії кібербезпеки України; підвищення рівня підготовки фахівців з кібербезпеки та захисту інформації; налагодження державно-приватного партнерства і посилення міжнародної співпраці з питань подолання кіберзлочинності.

ПЕРЕЛІК ПОСИЛАНЬ

1. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. Комп'ютерна злочинність: Навч. посіб. К.: Атіка, 2002. 240 с.

2. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : Монографія / За заг. ред. д-ра юрид. наук Р. А. Калюжного. Запоріжжя: Просвіта, 2001. 252 с.

3. Правове регулювання відповідальності за кіберзлочини в Україні. URL: https://legalitgroup.com/pravove-regulyuvannya-vidpovidalnosti-za-kiberzlochini-v-ukrayini/

4. Максименко Ю.Є. Інформаційні правопорушення: поняття та ознаки. URL: https://goal-int.org/informacijni-pravoporushennya-ponyattya-ta-oznaki/

5. Латиш К.В. Криміналістична характеристика кібервандалізму. Науковий вісник публічного та приватного права. 2018. Випуск 5. том 3. С. 117-121. URL: http://www.nvppp.in.ua/vip/2018/5/tom_3/25.pdf

6. Про основні засади забезпечення кібербезпеки : Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради. 2017. № 45. Ст.403.

7. Cyber Criminals and its types. URL: https://www.geeksforgeeks.org/cyber-criminals-and-its-types/

8. Карчевський М. В. Злочини у сфері використання комп’ютерної техніки : навч. посібник. Київ : Атіка, 2010. с. 60

9. Конвенція Ради Європи щодо кіберзлочинності від 23.11.2001 р. URL: http://zakon2.rada.gov.ua/laws/show/994_575

10. M. Edwards, E. Williams, C Peersman, A. Rashid. Characterising Cybercriminals: A Review. URL: https://arxiv.org/pdf/2202.07419.pdf

11. A. Maskun, M. H. Naswar. Qualifying Cyber Crime as a Crime of Aggression in International Law. URL: https://www.researchgate.net/ figure/The-Classification-of-Cybercrime-13_fig1_347143188

12. K Vadza. Cyber Crime & its Categories. URL: https://www.researchgate.net/publication/274652160_Cyber_Crime_its_Categories

13. F. Zandt. The Most Prevalent Forms of Cyber Crime. URL: https://www.statista.com/chart/30870/share-of-worldwide-cyber-attacks-by-type/

14. Crime doesn’t pay, but Cybercrime does. What motivates Cybercrime, URL: https://stage2data.com/crime-doesnt-pay-but-cybercrime-does-what-motivates-cybercrime/

15. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001

16. Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, 2016. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0410

17. Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1701413743859

18. Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cyber security certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1701413940571

19. Global Cyber Security Ecosystem. ETSI TR 103 306 V1.4.1 2020. URL: https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.04.01_60 /tr_103306v010401.pdf

20. Regulation (EC) No 460/2004 of the European Parliament and of the Council of establishing the European Network and Information Security Agency, 2004. URL:https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

21. State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks (19 September 2017) URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm

22. Кузнєцов О.М., Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. Інформація і право. № 1(36) 2021. С.106-113.

23. Wessel RA (2015) Towards EU cybersecurity law: regulating a new policy field. In: Tsagourias N, Buchan R Research handbook on international law and cyberspace. Edward Elgar Publishing

24. European Court of Auditors (2019) Challenges to effective EU cybersecurity policy. URL: https://www.eca.europa.eu/Lists/ECADocuments/BRP_ CYBERSECURITY/BRP_ CYBERSECURITY_EN.pdf Last access 7 July 2019

25. Directive 2013/40/EU of the European Parliament and ofthe Council of 12 August 2013 on attack sagainst information systems and replacing Council Framework Decision 2005/222/JHA, 2013. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040&qid=1701416096796

26. General Data Protection Regulation. GDPR, 2016. URL: https://gdpr-info.eu/

27. Communication from the Commissionto the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 2001. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF

28. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. A strategy for a Secure Information Society – «Dialogue, partner ship and empowerment», 2006. URL: https://ec.europa.eu/information_society/doc/ com2006251.pdf

29. Communication from the Commission to the Council, the European Parliament. Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attack sand disruptions: enhancing preparedness, security and resilience", 2009. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN: PDF

30. A Global Strategy for the European Union’s Foreign and Security Policy, 2016. URL:https://www.coe-civ.eu/kh/a-global-strategy-for-the-european-unions-foreign-and-security-policy

31. Permanent Structured Cooperation (PESCO). https://www.pesco.europa.eu/

32. Joint Communication to the European Parliament and the Council.Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017JC0450

33. European Cybercrime Centre. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

34. European Cybersecurity Competence Centre and Network. URL: https://cybersecurity-centre.europa.eu/about-us_en

35. Public Private Partner ships (PPPs). ENISA. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps

36. Малахов Г.Б. Шляхи удосконалення державно-приватного партнерства у сфері кібербезпеки України. Інформація і право. № 4(47). 2023. С. 197-206.

37. Joint communication to the European Parliamentand the Council. The EU's Cybersecurity Strategy for the Digital Decade (2020). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

38. Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text

39. Cybercrime. URL: https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

40. Proposal for a Regulation of the European Parliament and of the Councilon a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council a sregards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, 2002. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0568

41. Directive (EU) 2019/713 of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing

Council Framework Decision 2001/413/JHA. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG

42. Directive 2013/40/EU of the European Parliament and of the Councilon attack sagainst information system sandreplacing Council Framework Decision 2005/222/JHA, 2013. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

43. ENISA. URL: https://www.enisa.europa.eu/

44. European Cybercrime Centre - EC3. Combating crime in a digital age. URL:https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

45. Internet Organised Crime Threat Assessment. URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report

46. EU Policy Cycle – EMPACT. URL: https://www.europol.europa.eu/crime-areas-and-statistics/empact

47. Euro just. URL:https://www.eurojust.europa.eu/

48. Міжнародний рейтинг із кіберебезпеки. 2020. URL: https://logincasino.ua/news/mijnarodnii-reiting-iz-kiberbezpeki-ukraiyna-posila-25-te-misce-sered-160-kraiyn64865.html

49. Угода про асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами. 2014. URL: https://zakon.rada.gov.ua/ laws/show/984_011#Text

50. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

51. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року №96/2016. URL: https://www.president.gov.ua/documents/962016-19836

52. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

53. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 651.

54. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. Відомості Верховної Ради України. 1994. № 16. Ст. 93.

55. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 31.05.2005 р. № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31, Ст. 286

56. Про електронні довірчі послуги : Закон України від 5 жовтня 2017 року № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19

57. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.

58. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. Офіційний вісник України. 26.01.2021. № 6, стор. 10, стаття 306

59. Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова КМУ від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text;

60. Про рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47. URL: http://www.president.gov.ua/documents/472017-21374

61. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 р. №392/2020. URL: https://www.president.gov.ua/ documents/3922020-35037

62. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/ documents/4472021-40013

63. Про рішення Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 р. URL : https://zakon.rada.gov.ua/laws/show/685/2021#n14

64. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

65. Доронін І. М. Правові проблеми визначення компетенції суб'єктів забезпечення кібербезпеки України. Актуальні проблеми управління інформаційною безпекою держави. Київ, 2018. С. 62–64. URL: http://academy.ssu.gov.ua/upload/file

66. Communication «Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry» (2016) URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0410

67. National Cyber Security Strategy, March 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

68. NIST SP 800. URL: https://csrc.nist.gov/publications/sp800

69. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ : КНТ, 2020. 280 с.

70. Операційний центр безпеки. URL: http://surl.li/ommkv

71. Security Incident Response Teams. URL: https://www.techtarget.com/searchsecurity/definition/incident-response-team#:~:text=This%20is%20a%20team%20of,or%20communicating%20with%20the%20;

72. Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів. URL: https://zakon.rada.gov.ua/laws/show/311-2023-%D0%BF#Text

73. Сайт ДЦКЗ. URL: https://scpc.gov.ua/uk/cyber-trainer

74. Сайт CERT-UA. URL: https://cert.gov.ua/about-us

75. Климчук О.О., Ткачук Н.А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. Інформаційна безпека людини, суспільства, держави. 2015. № 3. С. 75–83

76. Кіберзлочинність: її детермінація та запобігання. URL: https://oduvs.edu.ua/wp-content/uploads/2016/09/lek-2016-d-z-3-4-kriminologia_ta_profilakt_zloginiv-10.pdf