етапах цивілізації за допомогою різних мов, а також вербальних і невербальних засобів» [1, с. 80].

Як сфера діяльності галузі прикладних соціально-комунікаційних технологій зазначена наука виникла зі стрімким розвитком технічних можливостей та зміною ролей в інформаційно-комунікаційних процесах.

Список використаних джерел:

1. Бацевич Ф. Основи комунікативної лінгвістики : підручник. Київ : Академія, 2004. 342 с.

2. Димитров В. Ю. Комунікативістика в системі суспільних відносин URL : https://core.ac.uk/download/pdf/47225795.pdf

3. Митко А. Досвід сучасної американської комунікативістики для України в сфері дослідження інформаційної демократії. URL : https://evnuir.vnu.edu.ua/bitstream/123456789/13036/1/%d0%9c%d0%b8%d1%82%d0%ba%d0%be_%d0%90.pdf

DOI https://doi.org/10.36059/978-966-397-444-6-57

Дрижакова Д. Ю.,
аспірантка кафедри кримінально-правової політики
та кримінального права
Київського національного університету імені Тараса Шевченка
м. Київ, Україна

ЗАХИСТ КОМП'ЮТЕРНИХ СИСТЕМ, МЕРЕЖ І ДАНИХ ВІД БУДЬ-ЯКИХ ФОРМ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ В КІБЕРПРОСТОРІ

Світ, що стрімко розвивається, де технології є невід'ємною частиною повсякденного життя, стикається з новим видом злочинності – кіберзлочинністю. Комп'ютерні технології, з одного боку, значно спрощують наше життя, а з іншого – створюють нові можливості для вчинення злочинів.

Захист комп'ютерних систем, мереж і даних від кіберзлочинності є одним з найактуальніших питань сучасності. З розвитком технологій зростає і кількість загроз, з якими стикаються як окремі користувачі, так і великі корпорації.

У Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. законодавець визначає *кіберпростір як «середовище (віртуальний простір), яке надає можливості для*

здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [1].

Переваги сучасного кіберпростору обумовили виникнення нових загроз національній і міжнародній безпеці, а саме появу кіберзлочинності. Термін «кіберзлочинність» вжито в американській доктрині на початку 60-х рр., коли було виявлено перші випадки злочинів, здійсне- них із використанням комп'ютерів. Саме тоді з'явилися перші «хакери», ними були студенти Массачусетського технологічного інституту, які маніпулювали з програмами нового університетського комп'ютера [3, с. 294].

На основі аналізу використання кіберпростору маємо змогу визначити певні особливості кіберпростору:

1) віддаленість (дистанційність) доступу;

2) оперативність створення, поширення, модифікації або знищення інформації в кіберпросторі;

3) віртуальність, що забезпечує відносну конфіденційність інформації та можливість впливати на свідомість певної категорії осіб;

4) комунікативність;

5) недосконаліть забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі [2].

На думку експертів ООН, комп'ютерна злочинність тотожна «кіберзлочинності», і її можна визначити так: «...охоплює будь-який злочин, який можна вчинити за допомогою комп'ютерної системи або мережі, в межах комп'ютерної системи або мережі чи проти комп'ютерної системи або мережі» [4, с. 134]. Тому можна зробити висновок, що це поняття, яке охоплює будь-який злочин, який може бути вчинений в електронному середовищі.

На сьогодні **основні загрози кібербезпеки:**

– **Віруси та шкідливе програмне забезпечення.** Програми, які пошкоджують дані, знижують продуктивність системи або отримують несанкціонований доступ до інформації.

– **Хакерські атаки.** Несанкціонований доступ до комп'ютерних систем з метою крадіжки даних, дестабілізації роботи систем або вимагання викупу.

– **Фішинг.** Спроби отримати конфіденційну інформацію (логіни, паролі, номери кредитних карток) шляхом обману користувачів.

– **Соціальна інженерія.** Маніпуляція людьми з метою отримання доступу до конфіденційної інформації або систем.

– **DDoS-атаки.** Спроби зробити сервіс недоступним для законних користувачів шляхом перевантаження сервера великою кількістю запитів.

Розвиток правових засад організації кібербезпеки в Україні, а саме захист відносин, що виникають під час одержання, використання, поширення та зберігання інформації, регулюються положеннями Конституції України, законами України: «Про інформацію», який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [5]; «Про доступ до публічної інформації», що визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [6]; «Про Національну програму інформатизації», який визначає загальні засади формування, виконання та коригування Національної програми інформатизації [7]; «Про захист інформації в інформаційно-телекомунікаційних системах», що регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [8]; «Про телекомунікації», який визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у такій діяльності або користуються телекомунікаційними послугами [9]: «Про електронні документи та електронний документообіг», що встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів [10]; «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом й обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини та громадянина, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних [11]; «Про **електронну ідентифікацію та** електронні довірчі послуги», що визначає правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації [12].

Найбільшим «проривом» вітчизняного законодавства у сфері забезпечення кібербезпеки стала ратифікація в 2005 році Конвенції про кіберзлочинність, прийнятої Радою Європи. Відповідно до Преамбули, метою створення документа стала необхідність зупинення дій, спрямованих проти конфіденційності, цілісності й доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними

правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, та укладення домовленостей щодо швидкого й надійного міжнародного співробітництва [1].

У січні 2016 року Радою національної безпеки та оборони України було прийнято за основу Стратегію кібербезпеки України з урахуванням викликів, які стоять перед нашою державою: агресивних дій Російської Федерації, посилення тенденцій використання кіберпростору розвідувальними і спеціальними військовими структурами, терористами, криміналітетом [13].

Попри наявність чинних нормативно-правових актів, вітчизняне законодавство лише частково задовольняє потреби сьогодення. Законодавство України про кримінальну відповідальність не містить у повному обсязі понять, що розкривають кіберзлочинність. Загалом у КК України немає термінів із префіксом «кібер-», є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку. Уважаємо за доцільне стверджувати або висловити думку, що Кримінальний кодекс України повинен бути оновлений відповідно до сучасних термінів, які б розкривали суть кіберзлочинів, у розділі, що передбачає відповідальність за них.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса, 2020. 112 с.
3. Ричка Д. О. Історичні аспекти кіберзлочинності. *Сучасний стан і перспективи розвитку держави і права* : матеріали VII Міжнародної наукової конференції студентів, аспірантів та молодих вчених, м. Дніпропетровськ, 4–5 груд. 2015 р. Дніпропетровськ : Дніпропетровський національний університет імені Олеся Гончара, 2015. С. 293–295.
4. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України.* 2010. № 3. С. 129–136.
5. Закон України: «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
6. Закон України «Про доступ до публічної інформації». URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text
7. Закон України «Про Національну програму інформатизації». URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text
8. Закон Украине «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

9. Закон України «Про телекомунікації». URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text
10. Закон України «Про електронні документи та електронний документообіг». URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
11. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
12. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text
13. Указ Президента «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні». URL: https://zakon.rada.gov.ua/laws/show/928/2000#Text

DOI https://doi.org/10.36059/978-966-397-444-6-58

Омецинська Н. В.,
кандидат технічних наук, доцент,
завідувачка кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

Дроменко В. Б.,
кандидат технічних наук, доцент,
доцент кафедри інженерних систем та технологій
Таврійського національного університету імені В. І. Вернадського
м. Київ, Україна

КІБЕРЗАХИСТ В ІНФОРМАЦІЙНИХ СИСТЕМАХ: ПРИНЦИПИ ТА ПІДХОДИ

Від початку військових дій, які розпочалися після 2014 року, і значно загострилися з повномасштабним вторгненням Росії в 2022 році Україна зіткнулася з безпрецедентною хвилею кібератак. Кібератаки стали невід'ємною частиною російської агресії, націленої на критичні інфраструктури: енергетичний сектор, телекомунікації, банківську систему, державні сайти та сервіси.

Основними загрозами кібербезпеки під час війни стають: *кібератаки на критичну інфраструктуру*, які можуть виводити з ладу електромережі, телекомунікаційні системи або банківські сервіси, що паралізує економіку та управління державою; *фішингові атаки*, коли противник використовує кампанії для отримання доступу до