УДК 343.98

Ілля Миколайович МЕЛЬНИКОВ,
старший викладач кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ (м. Київ)

СУЧАСНІ ВИКЛИКИ ТА ЗАВДАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

В наш час всі ми є свідками стрімкого прогресу та розвитку інформаційних технологій. Зараз до мережі Інтернет підключено кілька мільярдів комп'ютерів. Одночасно в Мережі розміщено кілька сотень мільярдів сайтів, сторінок і зображень. На інтернет-економіку в світі вже припадає значна частина валового продукту, приблизно 10-15 %. Щокварталу обсяг переданих через Інтернет даних подвоюється і зараз, як зазначалося на міжнародних конференціях, можна говорити про появу реальної залежності розвинених країн від надійності міжнародної інформаційної інфраструктури. Даний процес, природно, торкнувся і України. Через кілька років кожен другий фахівець у нас буде здобувати другу вищу освіту дистанційним шляхом. Особливої популярності та необхідності цей процес набув під час епідемії коронавірусу. Розпочато створення Національної електронної бібліотеки. Однак сьогодні, як відомо, Інтернет став не тільки світової скарбницею, але і, на жаль, «світовим смітником». Спами, неправомірна реклама і порнографія все більш нахабно нав'язуються користувачам. Криміналізація соціуму отримала своє специфічне переломлення і в криміналізації Інтернету, появі якісно нових загроз у вигляді інформаційних воєн і кіберзлочинності [1].

Фахівці називають п'ять основних напрямків (викликів) правового регулювання Інтернет-відносин: захист особистих даних і приватного життя в Мережі; регулювання електронної комерції та інших угод і забезпечення їх безпеки; захист інтелектуальної власності; боротьба проти протиправного змісту інформації і протиправної поведінки в Мережі; правове регулювання електронних повідомлень [2].

В даний час кіберзлочинність розглядається багатьма експертами як бурхливо зростаюча загроза безпеці, як для окремих держав, так і для світової спільноти в цілому. Ця загроза спонукала до пошуку адекватних заходів протидії. Після прийняття в 2000 р. Хартії глобального

інформаційного суспільства і в 2001 р. відомої Конвенції Ради Європи про боротьбу з кіберзлочинністю, в світі проведені спеціальні форуми з цієї проблеми. Так, в грудні 2002 р в Лондоні пройшов перший т. зв. Стратегічний конгрес по боротьбі з електронної злочинністю. У лютому 2003 року за підтримки Інституту вивчення проблем кіберзлочинності в Атланті (США) відбувся Перший міжнародний саміт з проблем кіберзлочинності. Проте, поки проблема загострюється, і так буде тривати ще досить довго.

Лідером за кількістю кібератак сьогодні є США, на рахунку яких 35,4% від світового коефіцієнта кіберзлочинів. Ця цифра постійно зростає. Друге місце в списку кіберзлочинів займає Південна Корея – 12,8%; за нею Китай – 6,9%; Німеччина – 6,7%; Франція – 4%, Великобританія – 2,2% від усього коефіцієнта кібератак. Найпоширенішими серед них є: програмні віруси, комп'ютерні віруси, що саморозмножуються та інші форми збоїв програмного коду. Той факт, що США лідирують в цьому списку, цілком закономірний, оскільки тут, в порівнянні з іншими країнами, спостерігається найбільше число користувачів [3].

Найбільш небезпечним видом кіберзлочинності стає кібертероризм. Головною мішенню кібертерористів в майбутньому можуть стати основні фінансові інститути, бо посягання на них здатні заподіяти дуже тяжка шкода. Так, якщо, наприклад, відключити всі засоби зв'язку Нью-йоркській біржі із зовнішнім світом, то їй буде завдано збитків більше, ніж від вибуху вибухового пристрою в її будинку [4, с. 11].

Також нагадаємо, що за характером використання комп'ютерів або комп'ютерних систем зазвичай виділяють три види кіберзлочинів: діяння, де комп'ютери є предметами злочинів – власне комп'ютерні злочини (викрадення інформації, несанкціонований доступ, знищення або пошкодження файлів і пристроїв тощо.); дії, де комп'ютери використовуються як знаряддя злочину (електронні розкрадання тощо.); злочини, де комп'ютери відіграють роль інтелектуальних засобів (наприклад, розміщення в Інтернет порносайтів) [4].

Примикають до кіберзлочинності і деякі дії, спрямовані на підтримку умов для її існування і розвитку (використання електронної пошти для комунікації, створення власних сайтів, спрямованих на поширення кримінальної та протиправної ідеології, а також обмін кримінальним досвідом і спеціальними знаннями). У всьому світі налічується десятки тисяч орієнтованих на злом і навчальних цим прийомам сайтів. Будь-

який підліток може купити за невеликі гроші книгу, навчальну його елементарним прийомам атаки на інформаційні системи. Ще однією проблемою є те, що комп'ютерна злочинність по-різному криміналізована в законодавстві країн світу. В даний час більше 100 країн, в тому числі 60% членів Інтерполу, не мають законів, призначених для боротьби з кіберзлочинами.

Ефективна боротьба з кіберзлочинністю передбачає адекватне з'ясування специфіки причин її розростання. В цілому злочинні прояви мають єдиний причинний комплекс, в основі якого знаходяться найглибші і гострі деформації в суспільстві у всіх його сферах (політичній, економічній, соціальній і духовній) та на всіх його рівнях, починаючи зі світового глобального і закінчуючи індивідуальним особистісним. Це такі деформації, які, по-перше, перш за все, висловлюють несправедливість соціального устрою, відкривають простір для сваволі одних суб'єктів на шкоду іншим; по-друге, обмежують права і свободи громадян і, по-третє, ведуть до дегуманізації і ущербності соціального статусу і менталітету частини населення. Особливості причинного комплексу кіберзлочинності пов'язані зі специфікою віртуального світу. Тут в не меншому ступені, ніж у світі реальному, потрібно гармонізація відносин.

Кіберзлочинність має специфічні причини, і боротьба з нею також передбачає застосування специфічних засобів. У світі вже накопичено певний позитивний досвід такої боротьби, який треба застосовувати і на Україні.

Список бібліографічних посилань

1. Дремин В. Н. Глобализация информационных систем как фактор глобализации преступности. *Інформаційні технології та безпека*. 2002. Вип. 1. С. 56–59.
2. Номоконов В. Актуальные проблемы борьбы с киберпреступностью // Computer Crime Research Center : сайт. URL: http://www.crime-research.org/library/Nomokon1.html (дата звернення: 07.04.2020).
3. Некоторые проблемы современного кибертерроризма. *Борьба с преступностью за рубежом*. 2001. № 12.
4. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. М. : Юрид. лит., 1991. 160 с.
5. Правовые аспекты борьбы с кибернетическими преступлениями в ЕС. *Борьба с преступностью за рубежом*. 2003. № 2. С. 37.

Одержано 28.04.2020