Сверба Ю.І.
Національний університет «Одеська юридична академія»,
студент 6-го курсу Інституту кримінальної юстиції

ІСТОРИЧНИЙ РОЗВИТОК ТА СУЧАСНИЙ СТАН ЗАХИСТУ КІБЕРПРОСТОРУ

Інформаційна революція ХХстоліття ознаменувалась створенням «цифрового простору», який часто залишається недосяжним для кримінально-правових заходів впливу. Масштабний розвиток технологій посилює негативну тенденцію нездатності імперативних норм захистити кіберпростір, а як наслідок - різке зростання кіберзлочинів, що спричиняють мільярдні збитки.

Не менш актуальне це питання і для українських реалій. Так, зазначається, що побудова в Україні інформаційного суспільства можлива за умови широкої інтеграції сучасних технологій автоматизованої обробки даних у всі сфери економіки, державного управління та суспільної діяльності. Це різко збільшує залежність реалізації життєво важливих інтересів осіб, суспільства та держави від належного функціонування інформаційно-телекомунікаційних систем, за допомогою яких й забезпечується така реалізація.

За таких умов питання захисту життєво важливих інтересів людини, суспільства та держави у кіберпросторі набуває особливого значення. Потребує подальшого розвитку механізм захисту приватного життя особи при користуванні кіберпростором, при автоматизованій обробці персональних даних [Пояснювальна записка доПроекту Закону про кібернетичну безпеку України № 2207а від 04.06.2013. [Електронний ресурс] - Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=47240].

Ретроспективне дослідження«цифрового простору» значно ускладнюється термінологічною неоднорідністю. Також, часто вживані

дефініції як «кіберпростір», «кіберзлочин», «кібербезпека» є досить умовними і не відображають всього лексичного спектру. Більше того, сам термін «кіберпростір» (англ. - cyberspace) вперше застосував письменник- фантаст Вільям Гібсон в п'єсі «LeNeuromancer», що ще раз відображає ефемерне, а не наукове чи технічне значення.

Досить обґрунтованим та змістовним є визначення кіберпростору надане В.А. Голубевим. Останній визначає його як модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі [Голубев В.А. Кибертерроризм - миф или реальность? [Електронний ресурс] - Режим доступу: http://www.cnme- research.org/library/terror3 .htm].

Виходячи з вищевказаного, вдалим, на нашу думку, є визначення кібербезпеки, запропоноване Д.В. Дубовим та М.А. Ожеваном, а саме: стан захищеності кіберпростору в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу (кібератак), за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз особистим, корпоративним та/або національним інтересам [Дубови Д.В., Ожеван М.А. Кібербезпека: світові тенденції та виклики для України. - К.: НІСД. - 2011. - 30 с. [Електронний ресурс]. - Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab 17 .pdf].

Зрозуміло, що первинним в кібербезпеці є сам кіберпростір, оскільки не можливо застосовувати охоронні засоби до неіснуючого об'єкту. Крім того, кіберзлочини виникли не так давно, лише після появи мережі Інтернет, в той час як традиційні злочини мають багатовікову історію. Висловлюються думки

науковців про теоретичну можливість існування кіберпростору до моменту створення мережі Інтернет. Обґрунтовуються такі тези наявністю електронно-обчислювальних машин (комп'ютерів) та інших систем, проте вони не ставали об'єктом незаконних посягань кіберзлочинців, тому істотного значення для дослідження не мають.

Оскільки кіберпростір невід'ємний від інформаційної революції, то початок його існування слід датувати з 60-х років минулого століття. У 1962 р. професор Джон Ліклайдер опублікував свою концепцію широкого розповсюдження комп'ютерної мережі «GalacticNetwork». Дана концепція припускала, що в майбутньому з'явиться глобальна мережа, підключитися до якої зможе будь-хто, і що дана мережа з'єднає комп'ютерні системи всього світу.

Першим кроком власне до появи Інтернет стало створення комунікаційної мережі комп'ютерів ARPANet, створеної за замовленням Міністерства оборони США. Ідея даної розробки полягала в тому, щоб створити розподілену комп'ютерну систему без одного чітко вираженого центру, який можна було б вивести з ладу у разі ядерної війни, і яка складається з взаємозамінних сегментів.

І вже у 1970-х роках з'являються перші комп'ютерні злочинці, яких почали називати «хакерами». Важко точно сказати, хто був першим кіберзлочинцем, але в більшості джерел згадується Джон Дрейпер, який вперше незаконно проник в телекомунікаційну мережу [Дзюндзюк В. Б. Поява і розвиток кіберзлочинності / В. Б. Дзюндзюк, Б. В. Дзюндзюк. // Державне будівництво. - 2013. - № 1. - С. 1-7].

Наступні етапи розвитку кіберзлочинності не мають чіткої періодизації, а лише характеризуються набуттям транснаціонального характеру, появою кібертероризму та виникненням інформаційних війн. Сама кіберзлочинність набула рис організованої та такої, що спричиняє серйозні збитки не тільки окремій банківській системі, а й світовій економіці в цілому.

Говорячи про сучасний стан забезпечення кібербезпеки, можливо констатувати існування якісно нової системи протидії кіберзлочинам. Більшість потужних держав світу (США, Росія, ЄС, Китай, Індія та інші) перебувають нині на етапі створення і трансформації власних військових кібернетичних підрозділів з огляду на можливості використання мережі Інтернет проти їх національних інтересів, а також отримання можливості впливати на інші держави. За даними керівника компанії McAfee, оприлюдненими на Всесвітньому економічному форумі в Давосі ще у 2010 р. , вже у 2009-2010 рр. понад 20 країн планували або здійснювали різноманітні інформаційні операції [Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. - К.: НІСД. - 2014. - С. 50].

Ще більшого загострення питання кібербезпеки отримало в контексті інформаційного протистояння США та Росії. Взаємні звинувачення у застосуванні кібератак, а також викрадення особистої інформації у високопоставлених чиновників переформатувало геополітичне протистояння. Існують думки про настання нової холодної війни інформаційного плану.

Таким чином, за останні півстоліття можна спостерігати різку еволюцію кіберзлочинів від дрібних правопорушень до транснаціональних злочинів. Прогнозуємо, що подальша інформатизація суспільства спричинить ще більшу потребу у кібербезпеці, і як наслідок, прирівняє кіберзлочини до злочинів міжнародного характеру з більш жорсткими кримінальними санкціями.

Науковий керівник: Березовська Н.Л. - к.ю.н., доцент кафедри кримінального права Національного університету «Одеська юридична академія».