цей законопроєкт «грою», адже одночасно пропонується і доповнити і виключити вищезазначене словосполучення.

Список використаних джерел

1. Про внесення змін до статті 149 Кримінального кодексу України (щодо приведення у відповідність до міжнародних стандартів) : проєкт Закону України № 6243 від 27.03.2017 // ВР України : офіційний вебпортал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=61428 (дата звернення: 30.04.2021).

2. Про внесення змін до Кримінального кодексу України щодо посилення кримінальної відповідальності за торгівлю людьми : проєкт Закону № 5134 від 22.01.2021 / ВР України : офіційний вебпортал. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=71204 (дата звернення: 30.04.2021).

3. Про протидію торгівлі людьми : Закон України від 20.09.2011 № 3739-VI // БД «Законодавство України» / ВР України : офіційний вебпортал. URL: https://zakon.rada.gov.ua/laws/show/3739-17 (дата звернення: 30.04.2021).

Одержано 30.04.2021

УДК [004;343.6]

САЄНКО Денис Леонідович,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ОНИЩЕНКО Юрій Миколайович,
кандидат наук з державного управління, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-7755-3071

ВИДИ КІБЕРЗЛОЧИНІВ ТА СПОСОБИ ЗАХИСТУ ВІД НИХ

Зловмисна прив’язка до злому вперше була задокументована в 1970-х роках, коли ранні комп’ютеризовані телефони ставали мішенню. Підковані в техніці люди, відомі як «фрікери», знайшли спосіб оплати міжміських дзвінків за допомогою ряду кодів. Вони були першими хакерами, які навчились використовувати систему, модифікуючи апаратне та програмне забезпечення для крадіжки телефонного часу на великій відстані. Це змусило людей усвідомити, що комп’ютерні системи вразливі до злочинної діяльності, і чим складніші системи ставали, тим більш сприйнятливими вони були до вчинення кіберзлочинів.

Відомий випадок стався 1990 року, коли був викритий великий проект під назвою «Операція Сандевіл». Агенти ФБР вилучили 42 комп'ютери та понад 20000 дискет, які використовувались злочинцями для незаконного використання кредитних карток та телефонних послуг. У цій операції взяли участь понад 100 агентів ФБР, і знадобилося два роки, щоб розшукати лише кількох підозрюваних. Це був наочний спосіб показати хакерам, що за ними слідкуватимуть і будуть переслідувати.

Кіберзлочинність зростає такими ж швидкими темпами, як і кількість нових користувачів, які підключаються до цифрового світу. Подібно до того, як у реальному світі є хороші і погані люди, є користувачі інтернету, які використовують свої знання з кібербезпеки, щоб допомогти іншим (також відомі як білі капелюхи або етичні хакери). Є й ті, хто використовує свої цифрові навички для поширення страху та створення хаосу.

Кіберзлочинність в інтернеті щорічно завдає збитків організаціям, компаніям та урядам на мільярди доларів. Нажаль незаконна діяльність в інтернеті не має тенденцій уповільнення, навпаки – дедалі більше зростає. Дослідження Gallup доводить, що громадян більше турбує кіберзлочинність, аніж безпосередньо небезпечні для життя злочини, такі як вбивство чи тероризм.

Що таке кіберзлочинність? Якщо говорити просто, кіберзлочинність – це злочин, вчинений в інтернеті, в локальних мережах або навіть проти ізольованих комп’ютерів, може

впливати на будь-які цифрові пристрої (включаючи ПК, ноутбуки, смарт-телевізори, планшети, смартфони, електронні системи тощо). Кіберзлочинці загальновідомі як хакери, хоча цей термін технічно неточний, правильний термін – «зломщик».

Класифікація кіберзлочинів поділяється на чотири основні категорії, які базуються на тому, хто постраждав від цифрової злочинності.

Кіберзлочини проти фізичних осіб – злочини, що безпосередньо впливають на людину (соціальна інженерія, фішинг, переслідування електронною поштою, кіберсталінг та розповсюдження незаконних матеріалів).

Кіберзлочини проти юридичних осіб компаній (організацій): порушення даних, кібервимагання та розповсюдження warez (програм, які розповсюджується незаконним шляхом з порушенням прав правовласника) тощо.

Кіберзлочини проти суспільства: фінансові злочини проти громадських організацій, продаж нелегальної продукції, незаконна торгівля, азартні ігри в інтернеті, підробка тощо.

Кіберзлочини проти уряду, зокрема кібертероризм, проникнення в урядові системи та мережі, поширення пропаганди, розміщення у мережі контенту, що має на меті дезінформацію, залякування тощо.

Важливість кібербезпеки зростає. Принципово, що наше суспільство більш технологічно залежне, ніж будь-коли раніше, і немає жодних ознак того, що ця тенденція сповільниться. Витоки даних, які можуть призвести до крадіжки особистих даних, тепер публічно публікуються в акаунтах соціальних мереж. Конфіденційна інформація (номери соціального страхування, дані кредитної картки та реквізити банківських рахунків) тепер зберігаються в хмарних сховищах, таких як Dropbox, Google Drive тощо.

Незалежно від статусу (фізична особа, малий бізнес, велика компанія) користувачі щодня покладаються на інформаційно-телекомунікаційні та комп'ютерні системи. Зі зростанням темпів та обсягів використання хмарних сервісів, їхнім недосконалим рівнем безпеки, уразливостями операційних систем та іншого програмного забезпечення смартфонів та інтернет-сервісів маємо безліч загроз в мережі.

Більшість користувачів інтернету не усвідомлює реальність реалізації та наслідки потенційних загроз мережі (можливість зламу їх акаунтів, компрометації банківських платіжних інструментів, заволодіння персональними даними тощо) та навіть рідко змінює свої облікові дані або оновлює паролі.

Тому, актуальним залишається питання поінформованості населення щодо елементарних правил кібергігієни: необхідність проявляти пильність під час перегляду вебсайтів; ніколи не натискати на незнайомі посилання чи оголошення у листах електронної пошти, що надходять від незнайомців; за можливості використовувати VPN; перш ніж вводити облікові дані, слід переконатися, що вебсайт безпечний; оновлювати антивірусне програмне забезпечення; використовувати надійні паролі з восьми та більше символів різних типів (цифри, літери верхнього та нижнього регістрів, спеціальні символи); не встановлювати однакові паролі на різні облікові акаунти, облікові записи до інтернет-сервісів та системи дистанційного банківського обслуговування тощо.

Одержано 20.04.2021