УДК 343.3/.7:343.85

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: ТЕОРЕТИЧНІ АСПЕКТИ І ШЛЯХИ ЗАХИСТУ

Точілов В.О.
Національний юридичний університет імені Ярослава Мудрого

У статті автор досліджує явище кіберзлочинності; аналізує положення українського законодавства в частині, що стосується інформаційних злочинів. Також автор розглядає питання кібербезпеки в Україні; надає загальні рекомендації щодо підвищення особистої інформаційної безпеки. Крім того, автор пропонує шляхи підвищення кібербезпеки в Україні в цілому.
Ключові слова: злочини в сфері інформаційних технологій, кіберзлочини, кібербезпека, кібератака, кіберпростір, програмне забезпечення, інформація.

Постановка проблеми. Дуже часто виходить так, що науковий і технічний прогрес, який надає людям нові блага та можливості, тягне за собою негативні явища, що являють собою іншу, невідривну, сторону прогресу.

Яскравим приладом є інформаційна революція, внаслідок якої в кожній сфері суспільного життя, таких як, наприклад, виробництво товарів, надання послуг і дозвілля, виник якісний переворот в їх існуванні за допомогою інформаційних і комп'ютерних технологій. На сьогоднішній день життя людей майже повністю комп'ютеризувалось, і майже всі дані мають електронну форму.

В даному випадку іншою, негативною стороною є інформаційні злочини або кіберзлочини. Єдиного підходу до визначення цього поняття не існує, але можна сказати, що кіберзлочини – це злочини, які вчиняються в процесі автоматизованої обробки інформації за допомогою електронно-обчислювальних машин або через комп'ютерні системи, об'єктом посягання яких є суспільні відносини у сфері обігу електронної інформації та інші суспільних відносин, у яких комп'ютер виступає кваліфікуючою ознакою вчинення злочину [1, с. 417].

Кіберзлочини є одним з тих видів злочинів, що мають найбільшу динаміку росту в світі. Це на пряму пов'язано зі стрімким розвитком інформаційних технологій (або ІТ) і зі все більшою їх інтеграцією в людське життя. Тобто, чим більше життя людей залежить від новітніх технологій, тим більше їхні права та інтереси знаходяться під загрозою з боку кіберзлочинців.

Як свідчать дані Генеральної прокуратури України, упродовж 2017 року на території України було зареєстровано 3178 кіберзлочинів, і 1076 проваджень за такими правопорушеннями направлені до суду [2]. При цьому дані Генпрокуратури за 2016 рік говорять, що протягом позаминулого року було зареєстровано лише 705 кіберзлочинів, і тільки 185 проваджень направлені до суду [3].

Отже, статистика показує, що рівень інформаційних злочинів в Україні дійсно зростає найшвидшими темпами. Це робить всі дослідження в цій «перспективній» сфері надзвичайно актуальними, а діяльність кожного дослідника – надзвичайно важливою і корисною.

Така ситуація надає змогу зробити кілька висновків. По-перше, кіберзлочинці з кожним роком «нарощують» свою суспільну небезпечність, по-друге – рівень безпеки у сфері інформаційних технологій серед громадян України є досить низьким. Причиною останнього можна назвати малу освіченість широких мас населення у питаннях кібербезпеки.

Аналіз останніх досліджень і публікацій. Тема кіберзлочинності і кібербезпеки є досить «популярною» у наукових дослідженнях. Увагу можна приділити публікаціям О. Гладуна, В. Голубєва, А. Гребенькова, О. Григорьєва, Г. Долженкова, М. Журби, І. Карася, В. Кіютіна, І. Клепицького, О. Книженко, О. Користіна, Л. Краснова, В. Крачевського, М. Литвинова, Ю. Ляпунова, С. Максимова, А. Музики, А. Новікова, Л. Нундича, П. Смагіна, М. Погорецького, В. Шеломенцева, В. Хахановського, І. Юрченка та ін.

Оскільки кіберзлочинність є явищем, що швидко розвивається, і з кожним роком є все більш суспільно небезпечним, варто зауважити, що дослідження на цю тему мають тенденцію втрати актуальності, застарілості. Тому, важливим є регулярне оновлення «бази знань» на цю тему шляхом проведення нових досліджень і їх публікацій.

Виділення не вирішених раніше частин загальної проблеми. На мою думку, в питанні досліджень кіберзлочинності варто приділяти більше уваги темі захисту від кіберзлочинів, тобто кібербезпеці. Важливим є розбір теоретичних питань у даній сфері, але при цьому, я вважаю, що дана проблема потребує більше досліджень, що мали б дійсне практичне використання.

Мета статті. Однією з цілей цієї статті є висвітлення проблеми кіберзлочинності шляхом аналізу основних кіберзлочинів, передбачених українським кримінальним законодавством.

Але головною метою є позначення існуючої проблеми державної і, в особливості, особистої кібербезпеки в України та надання загальних відомостей, що можуть допомогти її підвищити.

Виклад основного матеріалу. У п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 р. з попередження злочинності і поводження з правопорушниками зазначено, що існує дві категорії інформаційних злочинів: 1) кіберзлочини у вузькому розумінні («комп'ютерні» злочини) – будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних; 2) кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) – будь-яке протиправне діяння, що вчинюється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [4, с. 129].

Що стосується конкретно українського законодавства, то у Кримінальному Кодексі України (далі – ККУ), у розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» кіберзлочинами визнано такі діяння [5]:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2);

4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст. 363);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363^1)

Злочин, визначений статтею 361 ККУ, це «класичне» зламування комп'ютерної системи, тобто самочинне, без належного дозволу проникнення у комп'ютерні системи чи мережі з протиправним умислом, що спричинило певні негативні наслідки (витік, втрату, підробку, блокування ін-формації тощо). Зазвичай злом супроводжує інше суспільно небезпечне діяння, таке як, наприклад, крадіжка, тобто є допоміжним засобом у вчиненні багатьох інших злочинів.

Стаття 361^1 ККУ передбачає дії, що полягають у створенні, розповсюдженні чи збуті шкідливого програмного забезпечення (далі – ПЗ) – певної програми або сукупності програм, що перешкоджає функціонуванню комп'ютера, пошкоджує дані на ньому або призводить до інших небажаних наслідків в комп'ютерній системі [6]. Шкідливе ПЗ може мати різноманітну форму (віруси (програми, здатні до самокопіювання з одночасним завдаванням шкоди комп'ютеру), троянська програма (шкідлива програма, що видає себе за безпечну, яка заважає роботі, шпигує за ним, використовує ресурси комп'ютера для якої-небудь незаконної діяльності і т. д.,) тощо), і може застосовуватись як допоміжний засіб у зломі та інших кіберзлочинах.

Відповідно до статті 361^2 ККУ, злочином є несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах або інших носіях інформації. При цьому не обов'язково, щоб збут і розповсюдження такої інформації стали наслідком вчинення злочинів, зазначених вище.

«Комп'ютерна» інформація з обмеженим доступом поділяється на конфіденційну і таємну [7]. Конфіденційна інформація містить відомості, які перебувають у володінні, користуванні або розпорядженні окремих осіб, поширюється за їх бажанням згідно з передбаченими ними умовами. До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Згідно зі статтею 362 ККУ кіберзлочином є несанкціоновані зміна, знищення або блокування комп'ютерної інформації. Також карається за цією статтею несанкціоновані перехоплення або копіювання комп'ютерної інформації, якщо це призвело до її витоку. При чому, суб'єктом цього злочину є тільки особи, що мають право доступу до такої інформації.

Статтею 363 ККУ передбачено такі злочинні діяння, як порушення правил експлуатації комп'ютерів (що може виражатися у невиконанні або неналежному виконанні обов'язків із виконання правил експлуатації комп'ютерів (наприклад, правил апаратного забезпечення або правил експлуатації їх програмного забезпечення)) і порушення порядку чи правил захисту інформації (невиконання або неналежне виконання встановлених нормативно-правовими актами вимог (організаційних чи технічних) захисту інформації), якщо це заподіяло значну шкоду, вчинені особами, які відповідають за таку експлуатацію чи захист.

У ст. 363^1 КК передбачено відповідальність за умисне масове розповсюдження повідомлень, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютеру. Повідомлення, про які йде мова – це так званий «спам», тобто масове розповсюдження попередньо не обумовлених електронних листів. Через масовий характер спамових повідомлень останні утруднюють роботу інформаційних систем і ресурсів, створюючи для них зайве перевантаження, що може бути причиною їх виходу з ладу. «Спам» також може стати носієм згаданих раніше шкідливих програм і вірусів [8].

Ми бачимо, що інформаційні злочини, відповідно до українського законодавства, можуть мати різноманітну форму та способи вчинення. Крім того, можна сказати, що вчинювані кіберзлочинцями дії можуть мати комплексний характер, тобто становити сукупність кіберзлочинів, що супроводжують і забезпечують один одного.

Суспільну небезпечність кіберзлочинів та актуальність цієї проблеми ілюструє таке явище, як кібератака. Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення 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 елек-

тронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [9].

Кібератаки, в силу своєї специфіки, дуже часто спрямовані на автоматизовані та інформаційні системи, що мають державне значення. Прикладом цього можуть слугувати відомі кібератаки на енергетичні компанії України 23 грудня 2015 року, коли зловмисникам вдалось успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній України, або кібератака 17-18 грудня 2016 року, коли була виведена з ладу підстанція «Північна» енергокомпанії «Укренерго», що мало наслідком залишення без струму споживачів певних районів Києва [10].

З оглядом на все вище сказане, можна зробити висновок, що кіберзлочини дійсно мають високу ступінь суспільної небезпечності, тому що дії, які складають такі злочини, є досить складними для реалізації, оскільки потребують спеціальних знань в сфері комп'ютерних технологій. Це означає, що і використання існуючих способів захисту від них також потребує певного рівня обізнаності в даній сфері.

Отже, одна з проблемних сторін явища кіберзлочинності полягає у низькому рівні ІТ-освіченості населення різних країн, зокрема, України. Складність полягає в тому, що комп'ютерні технології є досить складними в освоєнні. Тому дуже важливо для пересічного громадянина знати хоча б найпростіші способи захисту, що не потребують глибоких специфічних знань. Є багато джерел інформації, де визначені поради з безпеки в Інтернеті, і рекомендованим є використання всієї наявної інформації, для захисту себе та свої діяльність.

Ось декілька порад щодо того, як залишатись в безпеці [11].

1) При користуванні електронною поштою, соціальними мережами, месенджерами тощо необхідно зменшити кількість спаму, що надходить до користувача.

Як вже раніше зазначалося, спам може містити небезпечні для системи програми, а також може бути використаний для фішингу (злочинної діяльності по викраденню особистої інформації користувача шляхом надсилання підробленого листа якоїсь фінансової установи з проханням оновити особисті данні, які потім викрадаються [12]).

Для зазначених цілей рекомендується: використовувати спам-фільтр (програму, що виявляє і блокує небажані повідомлення); бути обережним з всією рекламою та пропозиціями в Інтернеті, а також з повідомленнями від невідомих відправників; якнайшвидше видаляти підозрілий спам і не відкривати будь-які вкладення в таких повідомленнях. Що стосується фішингу, необхідно пам'ятати, що офіційні веб-сайти певних організацій, онлайн-обробників платежів і т. п. ніколи не просять користувачів підтверджувати конфіденційну інформацію, такі як паролі чи реквізити.

2) При роботі в Інтернеті через інтернет-браузер (програму для перегляду веб-сторінок) дотримуватись таких правил: використовувати всі доступні програми та налаштування безпеки, що пропонуються браузером (якщо це браузер, якому користувач довіряє); блокувати спливаючі вікна браузера; не переходити по підозрілим посиланням, не заходити на неперевірені вебсайти, не завантажувати файли, що знаходяться за цими посиланнями чи на цих сайтах.

3) Для забезпеченнях належної роботи комп'ютера та захисту його від шкідливого програмного забезпечення необхідно застосовувати низку спеціально розроблених для цього програм. Такими програмами є: брандмауер, антивірусне програмне забезпечення, різноманітні анти-шпигунські інструменти тощо.

Брандмауер (або фаєрвол) – програмне забезпечення, що діє як фільтр, який пропускає, відмовляє, шифрує дані між областями різної безпеки (зазвичай між персональним комп'ютером та мережею Інтернет) згідно з набором правил та інших критеріїв [13]. У найпопулярнішій операційній системі Windows є вбудований брандмауер, що функціонує автономно, тобто без втручання користувача, що робить захист комп'ютера від небажаних даних значно простішим.

Антивірус – спеціалізована програма для знаходження комп'ютерних вірусів та інших шкідливих програм та відновлення заражених (модифікованих) такими програмами файлів, а також для запобігання зараження (модифікації) файлів чи операційної системи шкідливим кодом.

3) Необхідно виконувати такі загальні рекомендації, як: регулярне оновлення операційної системи комп'ютера (оскільки часто таким чином збільшується загальний рівень безпеки ПК шляхом усунення розробниками помилок у програмному коді ОС чи додаванням до неї нових захисних елементів); надійне шифрування бездротових мереж; створення надійних паролів всюди, де вони необхідні – щонайменше вісім символів у довжину і включаючи суміші прописних та літерних букв, цифр, знаків пунктуації або символів; збереження паролів в таємниці тощо.

Висновки і пропозиції. Отже, проаналізувавши все вище сказане, можна зробити висновок, що явище кіберзлочинності має досить велику суспільну небезпечність. Про це говорять такі фактори як: стрімке зростання кількості вчинюваних кіберзлочинів; можливість завдання шкоди як фізичним, так і юридичним особам, і навіть державним структурам; досить складні способи захисту, і, часто, неможливість застосування найпростіших з них пересічним громадянином через низьку освіченість в даній сфері тощо.

Але при цьому є способи підвищити кібербезпеку, як країни в цілому, так і кожної конкретної людини.

По-перше, вбачаю необхідність у приділенні уваги державою до підготовки більшої кількості кваліфікованих спеціалістів у сфері кібербезпеки. Не можна сказати, що в України немає таких спеціалістів, але не можна також сказати, що збільшення їх кількості та підвищення їх кваліфікації будуть зайвими.

По-друге, цілком можливим для центральних органів державної влади є прийняття загальних і спеціальних рекомендацій у сфері кібербезпеки у різноманітних областях життя суспільства, по прикладу правил пожежної безпеки.

Позитивним аспектом у даному питанні є набрання чинності 9 травня 2018 року Закон України «Про основні засади забезпечення кібербезпеки України», що визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, осно-

вні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [9].

По-третє, необхідно підвищити освіченість громадян України у сфері кібербезпеки. Це можна зробити на рівні державної пропаганди через ЗМІ, інформуючи населення про загальний стан справ в сфері кібербезпеки держави, стимулюючи населення до самоосвіти. Але перш за все, потрібно здійснити якісні зміни у системі освіти щодо цього питання, оскільки всім відомо, що у непрофільних навчальних закладах, таких як загальноосвітні школи, такі предмети, як інформатика (яка і дає базові знання учням у сфері інформаційних технологій, зокрема, щодо кібербезпеки) має низький рівень якості викладання [14].

Список літератури:

1. Щодо визначення поняття кіберзлочину / Ю. Бельський // Юридичний вісник. – 2014. – № 6. – С. 414–418. – Режим доступу: http://nbuv.gov.ua/UJRN/urid_2014_6_71.
2. Статистика кіберзлочинності в Україні (2017) [Електронний ресурс]. – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v_2.
3. Статистика кіберзлочинності в Україні (2016) [Електронний ресурс]. – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v#outgoing-23042.
4. Європіна І.В. Види протиправних діянь у сфері новітніх інформаційних технологій // Вісник Академії адвокатури України. – 2010. – № 3. – С. 129–136.
5. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. – Відомості Верховної Ради України. – 2001. – № 25–26 – Ст. 131.
6. Malware Definition [Електронний ресурс]. – Режим доступу: https://techterms.com/definition/malware.
7. «Про інформацію»: Закон України від 02.10.1992 № 2657-XII. – Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
8. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку [Електронний ресурс]. – Режим доступу:http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02.
9. «Про основні засади забезпечення кібербезпеки України»: Закон України від 05.10.2017 № 2163-VIII. – Відомості Верховної Ради України. – 2017. – № 45 – Ст. 403.
10. The Ukrainian Power Grid Was Hacked Again [Електронний ресурс] // MOTHERBOARD. – 2017. – Режим доступу: https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report.
11. Online safety [Електронний ресурс]. – Режим доступу: https://www.interpol.int/Crime-areas/Cybercrime/Online-safety.
12. Phishing Definition [Електронний ресурс]. – Режим доступу: https://techterms.com/definition/phishing.
13. Firewall Definition [Електронний ресурс]. – Режим доступу: https://techterms.com/definition/firewall.
14. Изучение IT в школе: почему украинские выпускники не умеют пользоваться Excel [Електронний ресурс] // Сегодня. – 2018. – Режим доступу до ресурсу: https://www.segodnya.ua/ukraine/izuchenie-it-v-shkole-pochemu-ukrainskie-vypuskniki-ne-umeyut-polzovatsya-excel-1120328.html.

Точилов В.О.
Национальный юридический университет имени Ярослава Мудрого

КИБЕРПРЕСТУПНОСТЬ В УКРАИНЕ: ТЕОРИТИЧЕСКИЕ АСПЕКТЫ И ПУТИ ЗАЩИТЫ

Аннотация
В статье автор исследует явление киберпреступности; анализирует положение украинского законодательства в части, касающейся информационных преступлений. Также автор рассматривает вопрос кибербезопасности в Украине; предоставляет общие рекомендации по повышению личной информационной безопасности. Кроме того, автор предлагает пути повышения кибербезопасности в Украине в целом.
Ключевые слова: преступления в сфере информационных технологий, киберпреступления, кибербезопасность, кибератака, киберпространство, программное обеспечение, информация.

Tochilov V.O.
Yaroslav Mudryi National Law University

CYBERCRIMES IN UKRAINE: THEORETICAL ASPECTS AND WAYS OF PROTECTION

Summary
In the article the author investigates the phenomenon of cybercrime; analyzes the provisions of Ukrainian legislation in the part concerning information crimes. The author also considers cybersecurity in Ukraine; provides general recommendations for improving personal information security. In addition, the author suggests ways to increase cyber security in Ukraine as a whole.
Keywords: information crimes, cybercrime, cyber security, cyberattack, cyberspace, software, information.