УДК 347.77:(007:004.056)

В. Бойко,
кандидат технічних наук,
доцент кафедри кібербезпеки
Національного університету «Одеська юридична академія»

М. Василенко,
доктор фізико-математичних наук, доктор юридичних наук, професор,
в. о. завідувача кафедри кібербезпеки
Національного університету «Одеська юридична академія»

Д. Золотоверх,
студент 2 курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»

БЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ У КОНТЕКСТІ ЗАКОНОДАВСТВА ТА ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ

Загальновідомо, що для функціонування комп'ютерів необхідна наявність певної системи, яка забезпечує існування можливості взаємодії з інформацією. Такою системою є комп'ютерна система, якою вважають інформаційно-технічний комплекс. Його метою стало отримання, збереження й оброблення інформації з можливістю її вводу та виводу. Обмін інформацією здійснюється за допомогою локальної або глобальної систем передач даних (комп'ютерної мережі). Комп'ютерну систему можна поділити на два аспекти – програмне й апаратне забезпечення. Апаратним забезпеченням є електронні та механічні частини обчислювального пристрою. У свою чергу, програмним забезпеченням є сукупність програм (набір інструкцій), що використовується для виконання конкретних завдань апаратним забезпеченням і потребує захисту. Саме інформаційна безпека розцінює інформацію як певний актив, що має цінність, і потребує захисту, спрямованого на забезпечення збереження тріади властивостей інформації – конфіденційності, доступності та цілісності [1, с. 2]. Зазначимо, що протягом останніх часів виникла стійка тенденція до збільшення проявів комп'ютерних атак на важливі об'єкти інфраструктури різних держав, що призводить до завдання їм шкоди через спотворення важливої інформації, блокування виробничих процесів на об'єктах промисловості, житлово-комунального господарства, транспорту, енергетики тощо.

Дослідження деяких проблем кібарбезпеки, зокрема законодавчих, а також запобігання кіберзагрозам розглядаються у працях низки вітчизняних дослідників (В. Бурячок, В. Ліпкан, І. Тімкін, Н. Новіков, І. Діордіца, С. Мельник, В. Кащук, В. Шеломенцев та інших). Зазначимо також роботи співавтора цієї статті (див. [2; 3]).

Метою статті є дослідження системи гарантування кібербезпеки комп'ютерних систем, включаючи систему законодавства, запобігання загрозам, що виникають.

Основу законодавства становить Закон України «Про основні засади забезпечення кібербезпеки України» (далі – Закон № 2163), який набув чинності 9 травня 2018 р. і став центральним у розвитку державної системи захисту від мережевих загроз [4]. У ньому визначено правові й організаційні засади забезпечення захисту наці-

ональних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, також повноваження й обов'язки державних органів у цій сфері, основні принципи координації їхньої діяльності щодо кібербезпеки. Варто зазначити, що Закон № 2163 не поширюється на: відносини та послуги, пов'язані зі змістом інформації, що обробляється (передається, зберігається) у комунікаційних та/або технологічних системах; діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення; соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (зокрема, блог-платформи, відеохостинги, інші вебресурси), якщо такі інформаційні ресурси не містять інформації, необхідність захисту якої встановлено законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів; комунікаційні системи, які не взаємодіють із публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем). Закон № 2163 вводить важливі базові поняття у сфері кіберзахисту та кібербезпеки і визначає права й обов'язки державних органів щодо кібербезпеки, хоча й дублює положення Стратегії кібербезпеки України, затвердженої Указом Президента від 15 березня 2016 р. № 96/2016. Гарнатує безпеку в кіберпросторі відповідно до ст. 5 Закону № 2163 сам Президент через: очолювану ним Раду національної безпеки і оборони (далі – РНБО); Національний координаційний центр кібербезпеки як робочий орган РНБО; Кабмін і міністерства. Зокрема, Кабмін забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів країни в кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури в банківській системі України). Згідно із Законом № 2163, основними суб'єктами національної системи кібербезпеки є Держспецзв'язку та захисту інформації, Нацполіція, Служба безпеки України (далі – СБУ), Міноборони та Генштаб Збройних сил України (далі – ЗСУ), розвідувальні органи, Національний банк України (НБУ). Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи з гарантування кібербезпеки, є: міністерства й інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; ЗСУ, інші військові формування, утворені відповідно до закону; НБУ; підприємства, установи й організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України й об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Законом № 2163 визначено, що суб'єкти гарантування кібербезпеки в межах своєї компетенції здійснюють: заходи щодо запобігання використання кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; виявлення і реагування на кіберінциденти та кібератаки, усунення їхніх наслідків; інформаційний обмін щодо реалізованих і потенційних кіберзагроз; розроблення та реалізацію запобіжних, організаційних, освітніх та інших заходів у сфері

кібербезпеки, кібероборони та кіберзахисту; забезпечення проведення аудиту інформаційної безпеки, зокрема на підпорядкованих об'єктах і об'єктах, що належать до сфери їх управління; інші заходи із забезпечення розвитку та безпеки кіберпростору. Закон № 2163 пропонує такий розподіл функцій і повноважень органів державної влади у сфері кіберзахисту. Держспецзв'язку та захисту інформації виконуватиме такі функції, як: кіберзахист об'єктів критичної інформаційної інфраструктури; координація діяльності інших суб'єктів кібербезпеки; забезпечення створення та функціонування національної телекомунікаційної мережі; запобігання, виявлення та реагування на кіберінциденти і кібератаки й усунення їхніх наслідків; інформування про кіберзагрози і методи захисту від них; забезпечення аудиту інформаційної безпеки на об'єктах критичної інфраструктури, установлення вимог до аудиторів інформаційної безпеки, визначення порядку їх атестації та переатестації. На Нацполіцію покладено відповідальність за попередження, виявлення, припинення й розкриття кіберзлочинів. Міноборони та Генштаб ЗСУ зобов'язані забезпечувати кібероборону військових об'єктів, кіберзахист об'єктів критичної інфраструктури під час війни і надзвичайного стану, а також відбивати військову агресію в кіберпросторі. СБУ в межах своїх повноважень має попереджати, виявляти, припиняти та розкривати злочини проти миру та безпеки людства в кіберпросторі, боротися з кібертероризмом і кібершпигунством. Також СБУ надано повноваження проводити таємні перевірки об'єктів критичної інфраструктури. Нацбанк визначається законом як регулятор з кібербезпеки в банківській сфері. Для цього він має право на встановлення в цій сфері власних стандартів і організацію перевірки їх дотримання. Однак хотілося б підкреслити, що зараз це вже відбувається – банківський сектор давно запровадив міжнародний стандарт захисту інформації ISO-27001. Навіть більше, НБУ має визначати порядок, вимоги та заходи щодо гарантування кіберзахисту й інформаційної безпеки в банківській системі й для суб'єктів переказу коштів. Для цього створено центр кіберзахисту, а також реєстр об'єктів критичної інформаційної інфраструктури в банківській системі. Водночас має проводитися оцінка стану кіберзахисту й аудит інформаційної безпеки банків. Кіберзахисту підлягають комунікаційні системи всіх форм власності, у яких обробляються національні інформаційні ресурси і які використовуються в інтересах органів державної влади та місцевого самоврядування, правоохоронних органів і військових формувань, у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу, а також об'єкти критичної інформаційної інфраструктури. До останніх можуть бути віднесені підприємства, установи й організації незалежно від форми власності: у галузі енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському і фінансовому секторах; у сферах водо-, газо- й електропостачання, водовідведення, виробництва продуктів харчування, сільського господарства, охорони здоров'я. Також до об'єктів критичної інформструктури належать комунальні, аварійні та рятувальні служби, стратегічні підприємства, потенційно небезпечні виробництва. У сфері кібербезпеки передбачено державно-приватну взаємодію. Так, система своєчасного виявлення, попередження та нейтралізації кіберзагроз може бути створена із залученням волонтерських організацій. Передбачено підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі. Заплановано обмін інформацією про кіберзагрози і координацію команд реагування на комп'ютерні надзвичайні події. Для громадян, представників промисловості та бізнесу створять консультаційні пункти. Крім того, ідеться про створення системи підготовки кадрів

та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки.

На сьогодні створено команду реагування на комп'ютерні надзвичайні події України (англ. Computer Emergency Response Team of Ukraine, CERT-UA) – спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України. Мета діяльності підрозділу визначена законодавчо та полягає в захисті державних інформаційних ресурсів і телекомунікаційних інформаційних систем від несанкціонованого доступу, неправомірного використання, а також порушення цілісності конфіденційності та доступності інформації [4]. Створення та функціонування урядової команди пов'язане із забезпеченням Стратегії кібербезпеки України [5], а також є однією з форм електронного урядування, тобто вона відкрита для звернень громадян із метою надання допомоги з питань протидії кіберзагрозам. Водночас система має забезпечувати конфіденційність, цілісність і доступність інформації. Конфіденційність полягає в неможливості отримання інформації неуповноваженою особою, тобто особою, яка не має права на дану інформацію. Цілісність полягає в неможливості будь-якої трансформації інформації неуповноваженою особою або ж уповноваженою, але без обґрунтованої на те мети. Такою трансформацію є зміна, спотворення або взагалі знищення інформації. Доступність реально являє собою властивість інформації, що може бути отримана уповноваженою особою за розумну кількість часу.

Для забезпечення стану кібербезпеки, а саме захищеності інформації, існують відповідні засоби захисту інформації. Існує умовний поділ таких засобів на технічні, інженерні, криптографічні й організаційні.

Технічні засоби спрямовані на обмеження доступу до носія інформації, завдяки апаратно-технічних засобів. Вираженням може бути програмне, апаратне забезпечення або ж їх сукупність. Інженерні засоби покликані забезпечити захист від руйнування носія навмисними діями чи впливом чинників природного характеру. Криптографічні засоби використовують математичні перетворення для ускладнення використання інформації в разі несанкціонованого доступу до неї. Організаційні заходи полягають у зменшені впливу людського чинника на комп'ютерну системи (ретельний добір та підвищення кваліфікації персоналу).

Кожне підприємство, установа, організація мають використовувати вищевказані заходи для мінімізації збитків або інших негативних явищ як наслідку прояву кіберзагроз.

Усі дії, пов'язані із забезпеченням стану захищеності комп'ютерних систем, водночас мають бути спрямовані на захист конфіденційності, цілісності та доступності інформації.

Розуміння загроз визначено і не викликає сумнівів. У широкому сенсі загрозою стає потенційно можлива дія або подія, що може завдати майнової шкоди інтересам осіб. У вузькому – загрозою є будь-яке несанкціоноване посягання на порушення конфіденційності, цілісності, доступності інформації [6, с. 420].

На сьогодні існує великий перелік інформаційних загроз, тому виникає необхідність у їх класифікації. Різні типи загроз за низкою ознак розподілено так.

Загрози, пов'язані з порушенням доступності інформації, спрямовані на блокування доступу до деяких ресурсів комп'ютерної системи або на зниження її працездатності. Тобто якщо один користувач відсилає запит на одержання певної інформації, а водночас відбувається блокування доступу, користувач відмову в доступі відчуває – втрачає можливість взаємодії з інформацією.

Загрози, пов'язані з порушенням цілісності інформації, що зберігається в комп'ютерній системі, що спрямовані

на її зміну чи спотворення, що призводить до зменшення її цінності або ж взагалі знищення. Така загроза може бути пов'язана як з діями злочинців, так і із впливом навколишнього середовища. Загрози такого виду є найбільш актуальною проблемою для безпеки комп'ютерних систем.

Загрози, пов'язані з порушенням конфіденційності, спрямовані на розголошення конфіденційної або ж секретної інформації. Такі дії призводять до того, що така інформація стає відомою особам, які не повинні мати до неї доступ. Конфіденційною є інформація, яка зберігається в комп'ютерній системі або передається від однієї системи іншій.

Загрози можна класифікувати на такі, що виникли через подію або дію. Подією може бути наслідок взаємодії об'єктивних фізичних процесів або ж стихійного лиха. Дія є штучною загрозою, що спричиняється діяльністю людини.

Атакою (кібератакою, хакерською атакою) уважають реалізацію загрози, якщо загроза – явище ймовірнісне (є вірогідність того, що воно відбудеться), то атакою виступає дія, що вже відбулась або відбувається. Тобто це дії кіберзловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу. На практиці це послідовність взаємозв'язаних дій порушника, які призводять до реалізації загроз інформаційним ресурсам шляхом використання вразливостей цієї інформаційної системи.

Зазвичай законодавство відстає від нових технологічних рішень і спонукає розвиток вірусних технологій для використання в кібератаках. Під час здійснення атаки використовується вразливість інформаційної системи. Вразливість комп'ютерної системи – це досить слабке місце, що може бути використане для здійснення несанкціонованих дій у межах комп'ютерної системи [1, с. 14]. Нездатність системи протистояти здійсненню загрози або сукупності загроз характеризує певні недоліки комп'ютерної системи, які можуть бути використані для порушення її цілісності, завдання шкоди, порушення властивостей інформації, що перебуває в обігу. Найпопулярнішим і найефективнішим видом атак на комп'ютерні системи є атаки з використанням комп'ютерного вірусу або ж вимагальної програми. Сьогодні можна вже говорити про «технічну вірусологію». Майже кожного року вірусні атаки набирають розмах справжніх вірусних епідемій та спричиняють збитки на мільярди доларів США. Прикладами таких вірусних програм стали програми, що генерують відомі однойменні віруси, як-от CryptoLocker, WannaCry, Petya. Саме такий вид програм називають шкідливим програмним забезпеченням.

Шкідливе програмне забезпечення (далі – ШПЗ) являє собою будь-яке програмне забезпечення, яке розроблене для того, щоби завдати шкоди комп'ютеру, серверу, клієнту або комп'ютерній мережі. ШПЗ завдає шкоди після того, як воно було певним чином внесено в комп'ютер цільового призначення, і може мати форму активного вмісту (виконуваного коду чи скрипту) та іншого програмного забезпечення. Цей код відомий як комп'ютерні віруси, вимагальні програми, шпигунські програми, рекламні програми та програми для сканування. ШПЗ має шкідливий намір, який діє проти інтересів користувача комп'ютера, тому не належить ПЗ, яке спричиняє шкоду через певний недолік, який зазвичай описується як помилка програмного забезпечення [7].

ШПЗ посягає на всі три ланки тріади комп'ютерної безпеки, адже воно має можливість передачі повного контролю над комп'ютерною системою особі чи групі осіб, що здійснюють атаку.

Використання соціальної інженерії базується на експлуатації людських чинників у комп'ютерних системах.

Унаслідок успішного психологічного впливу на жертву досвідчений зловмисник може виявити багато базових моментів у роботі організації для планування злому, викрадення інформації. Прикладами такої діяльності є використання графіка роботи охорони чи прибиральниць, оцінка кваліфікації персоналу тощо. І хоча такий метод безпосередньо не посягає на безпеку комп'ютерних систем, він використовується в більшості кіберзлочинів.

Багато атак пов'язані з витоком інформації, джерелом якої є власні співробітники. Таке явище поширене в організаціях, де відсутній контроль за наданням прав доступу високого рівня, а також відсутні розмежування щодо прав доступу до інформаційних ресурсів.

DoS (від англ. Denial of Service – відмова в обслуговуванні) називають атаку, що спрямована на те, щоб змусити комп'ютерну систему не відповідати на санкціоновані запити, знизити її продуктивність. Такий вид атаки не передбачає отримання деякої секретної інформації, але іноді буває підмогою для інших атак. Підтипом такої атаки є DDoS (від англ. Distributed Denial of Service – розподілена DoS). Атака характеризується тим, що вона відбувається з використанням не одного комп'ютера, а декількох.

Атака типу «Людина посередині» являє собою атаку, що відбувається завдяки перехопленню сигналу, який передається між двома системами, тобто передача відбувається через посередника. Такий посередник не тільки отримує доступ до всієї інформації, що передається таким каналом, а й має можливість модифікації. Метод, що використовує електронну пошту, називають фішинг, а його суть полягає в надсиланні листа, що має вигляд офіційного листа організації. Одержувач має враження, що має справу з листом банку, податкової служби чи популярного інтернет-магазину, надсилає свої дані зловмиснику.

Отже, кібербезпека комп'ютерних систем фактично визначається станом захищеності комп'ютерних систем – комплексу апаратного та програмного забезпечення та допомогою локальної або глобальної системи передач даних (комп'ютерної мережі), якою здійснюється передача інформації між комп'ютерними системами.

Інформація потребує захисту від випливу навмисних дій зловмисників та природних чинників. Захист спрямований на збереження трьох ознак інформації, а саме: конфіденційності (неможливість отримання інформації неуповноваженою особою, тобто особою, яка не має права на дану інформацію), цілісності (неможливість будь-якої трансформації інформації неуповноваженою особою або ж уповноваженою, але без обґрунтованої на те мети. Такою трансформацію є зміна, спотворення або взагалі знищення), доступності (являє собою властивість інформації, що може бути отримана уповноваженою особою за розумну кількість часу). Законодавство в такому разі залишається важливим, але не визначальним чинником через відставання від стрімкому технологічного прогресу у галузі розробки комп'ютерних систем і швидкого вдосконалення вірусних технологій. Основу законодавства у сфері кібербезпеки становить Закон України «Про основні засади забезпечення кібербезпеки України», що визначає правові й організаційні засади забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, також повноваження й обов'язки державних органів у цій сфері й основні принципи координації їх діяльності щодо гарантування кібербезпеки. Команда реагування на комп'ютерні надзвичайні події України (CERT-UA) захищає державні інформаційні ресурси та телекомунікаційні інформаційні системи від несанкціонованого доступу, неправомірного використання інформації. Будь-які проєкти, пов'язані з фінансовою або іншою системою, повинні передбачати можливі загрози і захищати своїх користувачів від їх негативних дій.

Ключові слова: кібербезпека, комп'ютерні системи, інформаційні технології, законодавство, кіберзагрози, вірусні програми.

Стаття висвітлює аспекти безпеки комп'ютерної системи як виду інформаційної системи. Досліджено законодавство у сфері кібернетичної безпеки. Визначено поняття та проведено класифікацію загроз, пов'язаних із комп'ютерною безпекою. Надано рекомендації щодо підвищення безпечності використання комп'ютерних систем і комп'ютера як їхнього елементу.

Статья освещает аспекты безопасности компьютерной системы как вида информационной системы. Исследовано законодательство в сфере кибернетической безопасности. Определено понятие и проведена классификация угроз, связанных с компьютерной безопасностью. Даны рекомендации по повышению безопасности использования компьютерных систем и компьютера как их элемента.

The article highlights the security aspects of a computer system as a type of information system. The legislation in the sphere of cybernetic security is investigated. The concept and classification of threats related to computer security are defined. Recommendations for improving the safety of computer systems and computer as its element are given.

Література

1. ISO / IEC Стандарт 27000. Інформаційні технології. Методи і засоби забезпечення безпеки. Системи менеджменту інформаційної безпеки. Загальні відомості і словник : вебсайт. URL: https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27000-2016.pdf (дата звернення: 10.05.2019)

2. Василенко М. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства. Юридичний вісник. Одеса : ВД «Гельветика», 2018. № 3.

3. Василенко М. Якість кібербезпеки інформаційно-комунікаційних систем (ІКС) та деякі законодавчі питання щодо її підвищення для суспільства. Юридичний вісник. Одеса : ВД «Гельветика», 2018. № 4.

4. Про основні засади забезпечення кібербезпеки України : Закон України № 2163 від 5 жовтня 2017 р. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

5. Указ Президента України про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 р. URL: http://zakon.rada.gov.ua/laws/show/96/2016.

6. Богуш В., Кривуца В., Кудін А. Інформаційна безпека : термінологічний навчальний довідник / за ред. В. Кривуци. Київ, 2004. 508 с.

7. Actions to be performed on infected objects. Лабораторія Касперського : вебсайт. URL: https://web.archive.org/web/20150809113716/.