ТИПИ СУЧАСНОГО ОСОБЛИВО НЕБЕЗПЕЧНОГО (ШКІДЛИВОГО) ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: ПРАВОВІ ТА ТЕХНІЧНІ АСПЕКТИ

Б.В. Кузьменко
доктор технічних наук, професор,
професор кафедри управління інформаційною безпекою ВНЗ «Державний університет інформаційно-комунікаційних технологій»
Ю.О. Заїка
доктор юридичних наук, професор,
начальник кафедри цивільного права і процесу ВНЗ «Національна академія внутрішніх справ»

Постановка проблеми. XXI ст., яке вже стало століттям інформаційних технологій, внесло колосальні зміни в життя окремих людей та всього суспільства в цілому. Зросла роль інформації, чисельність людей, задіяних у сфері інформаційних технологій, посилилась загальна інформатизація суспільства, зросла роль телекомунікаційних мереж і персональних комп'ютерів. Усе це привносить позитиви у розвиток комп'ютерних технологій, забезпечує особистості свободу вибору, можливість створювати та використовувати необхідні для життєдіяльності електронні комунікації, кругло добова доступність щодо можливості отримання та відправки інформації. Разом з тим, технічний прогрес надає можливість здійснювати злочини у новий спосіб, з використанням нових знарядь [2; 3].

Аналіз останніх досліджень та публікацій. Питання інформаційного права та правових засад інформаційної безпеки останніми роками вивчали К.І. Бєляков, В.Я. Настюк, Д.Й. Никифорчук, В.Г. Пилипчук, Є.Д. Скулиш та ін. Отримані значні результати у напрямку фундаментальних правових досліджень в інформаційній сфері. Проте динаміка інформаційних систем і технологій набула нових темпів зростання та якостей. Шаленими темпами зростає інформаційна злочинність, створено сучасне, особливо небезпечне програмне забезпечення, яке використано в економічній, терористичній, військовій, розвідувальній та в інших сферах. Перебіг подій потребує правового та технічного аналізу їх динаміки та тенденцій.

Мета статті полягає в аналізі сучасного шкідливого програмного забезпечення та визначенні правових засад протидії та попередження.

Основні результати дослідження. Бурхливий розвиток засобів зв'язку та інформаційних технологій визначає тенденції розвитку шкідливих програм.

Людство вступило в еру цифрових та інформаційних технологій, інформації відводиться велика роль, вона розглядається, як стратегічно важливий ресурс.

Удосконалення технології приводить не тільки до зміцнення індустріального суспільства, а і до появи нових, раніше невідомих джерел небезпеки для нього [1; 4].

Історично одним із перших, найпростіших типів шкідливого програмного забезпечення є класичні комп'ютерні віруси. Нині комп'ютерні віруси зустрічаються вкрай рідко, їх повністю витіснили будь-які мережеві хробаки та шпигунські програми. Наразі можна нарахувати з десяток активних файлових вірусів з достатньо рідкими сплесками їх активності, які пов'язані з здатністю інфікувати виконувані файли поштових хробаків. Часто з'являються варіанти поштових хробаків типу Mydoom, NetSky чи Bagle, заражені файловими вірусами Funlove, Xorala, Parite чи Spaces. Основні зусилля вірусодописувачів спрямовані, окрім використання вразливості мережевих технологій, ще й на людський фактор. Кваліфіковане використання соціального інжинірингу часто сприяє поширенню комп'ютерних вірусів. У троянських програмах сьогодні можна прослідкувати наступні тенденції: значне зростання чисельності програм-шпигунів, які «викрадають конфіденційну інформацію; прагнення отримати тотальний контроль над інфікованими комп'ютерами (їх об'єднання у зомбі-мережі, які управляються з єдиного центру). Використання інфікованих комп'ютерів задля розсилання через них спаму чи організації DDoS-атак. Більшість установ і організацій використовують мережеві технології, доступ до конфіденційної інформації отримується шляхом використання Інтернет, а особи, зацікавлені у такій інформації, наймають хакерів, чи своїми зусиллями отримують доступ до інформації своїх конкурентів.

Нові середовища і можливості шкідливих програм можуть свідчити про ймовірне збільшення чисельності програм, написаних на мові програмування NET, її популярність неминуче притягне увагу вірусодописувачів. Linux- платформи залишатимуться у полі уваги програм класу rootkit, та найпростіших файлових вірусів. Основна загроза для них виходитиме від виявляння уразливості у програмних продуктах для цієї платформи, які нададуть вірусодописувачам допомогу у досягненні цілей – тотального контролю за значною чисельністю комп'ютерів у Інтернет. Може зрости кількість шкідливих програм та кількість випадків виявлення вразливості ОС Unix. Стосовно мобільних технологій слід мати на увазі шкідливе програмне забезпечення для КПК, сотових телефонів, старт-фонів та комунікаторів. Стрімке зростання популярності ОС Windows Mobile 2003/05/06 та Symbian широкі можливості мережевої комутації цих засобів та наявність середовища розробки додатків (NET framework) неминуче призведе до появи троянських програм (для PalmOS такі вже існують), але й до значно небезпечніших різновидів, включно з варіантом мережевих хробаків. Найбільшу загрозу безпеці мобільних пристроїв становлять хробаки – віруси, що поширюються самостійно. Хробак здатний викликати надшвидке зараження великої кількості систем, порушити працездатність мобільної мережі, або перетворити її у підконтрольну зловмиснику розподілену мережу.

Стала закономірною поява у 2012 р. мобільних ботнетів на базі мобільних пристроїв з ОС Android. Першою недоброю подією стало виявлення у січні 2012 р. IRC-бота для Android, який працював у спаровуванні з СМС-трояном. Обидві шкідливі програми названі Foncy. У АРК-дроппері містився також root-експлойт. Усі інфіковані IRC-ботом Foncy смартфони залишали потенційний ботнет і були готовими до здійснення будь якої дії за командою «господаря». Того ж року нові шкідливі комп'ютерні програми використовувалися для точкових атак – атаки з використанням ZitMo та SpitMo (Zeus- та SpyEye-in-the-Mobile).

Розвиток інформаційних технологій на сучасному етапі нерозривно пов'язаний з безпекою інформації та захистом інформації, останнє поняття (захист інформації) є складовою частиною першого (захист інформації). У свою чергу, має 2 складові: безпека змістовної частини (смислу) інформації відсутність у ній спонукальних мотивів людини до негативних дій, умисно закладених механізмів негативної дії на людську психіку, або на інший блок інформації; захищеність інформації від зовнішньої дії (спроб неправомірного копіювання, поширення, модифікації, чи знищення). Захист інформації є прийняття правових, організаційних та технічних заходів, спрямованих на забезпечення захисту інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, поширення, та від інших неправомірних дій у відношенні такої інформації, дотримання конфіденційності інформації обмеженого доступу, реалізації права на доступ до інформації. У цілому проблема інформаційної безпеки включає, поряд із задачами забезпечення захищеності інформації та інформаційних систем, ще два аспекти: захист від дії шкідливої інформації, забезпечення прийняття обґрунтованих рішень з максимальним використанням доступної інформації.

Забезпечення інформаційної безпеки має вирішувати наступні основні задачі: виявлення, оцінка та попередження загроз інформаційним системам та ресурсам; захист прав юридичних та фізичних осіб на інтелектуальну власність, та збирання, накопичення та використання інформації; захист державної, службової, комерційної, особистої та інших типів таємниці. Загрози інформаційним системам та ресурсам можна умовно поділити на основні чотири групи: програмні — впровадження «вірусів», апаратних та програмних закладок; знищення та модифікація даних в інформаційних системах; технічні, у тому числі радіоелектронне, перехоплення інформації у лініях зв'язку, радіоелектронне придушення сигналу у лініях зв'язку та системах управління; фізичні — знищення засобів обробки та носіїв інформації; крадіжка носіїв, а також апаратних чи парольних програмних ключів; інформаційні – порушення регламентів інформаційного обміну; незаконне збирання та використання інформації; несанкціонований доступ до інформаційних ресурсів; незаконне копіювання даних в інформаційних системах; дезінформація, укриття чи спотворення інформації; крадіжка інформації з баз даних.

Протистояти цим загрозам можна на основі створення та впровадження ефективних систем захисту інформації.

Останнім часом розглядається й обговорюється питання комп'ютерного протистояння у просторі Інтернету – т.з. кібервійна. Вона спрямована насамперед на дестабілізацію комп'ютерних систем і доступу до Інтернету державних установ, фінансових та ділових центрів, створення безладу та хаосу у державах, які покладаються на Інтернет у повсякденному житті. Міждержавні відношення та політичне протистояння може знаходити своє продовження в Інтернеті у вигляді кібервійни: вандалізму, пропаганді, шпигунстві та безпосередніх атаках на комп'ютерні системи та сервери.

З поширенням інформаційних технологій громадяни, підприємства, державні установи у прямому розумінні стали залежними від мережі Інтернет у повсякденному житті, його використання для атак комп'ютерних систем іншої держави здатне нанести значні збитки економіці, створити розлад у повсякденне життя держави. На відміну від кібератак минулого нині кібервійна є загрозою для національної безпеки і сприймається як серйозна загроза національній безпеці. Розвідувальні установи багатьох країн займаються шпигунством в Інтернеті, збирають інформацію, зламують комп'ютерні системи та мережі інших держав, займаються диверсійною діяльністю та економічним шпигунством. Згідно з висновками західних спеціалістів, лідерами у веденні кібервійни нині є Китай та Росія, представники яких категорично заперечують причетність державних установ до організації атак. Подальший розвиток нових технологій, рівень кібервійни постійно вдосконалюється і підвищує її небезпечність. Певні держави приділяють належну увагу захисту від кібервійни, і виділяють необхідні ресурси для організації систем захисту, підтримують спеціальні підрозділи, задачею яких є підвищення і вдосконалення інформаційної безпеки. Контроль над Інтернетом у наш час визначає стан національної безпеки держави. У грудні 2012 р. у Дубаї (Об'єднані Арабські Емірати) відбувся Міжнародний саміт з питань кіберпростору, на якому дійшли висновку про те, що суперечності, пов'язані з міжнародними телекомунікаціями посилюються. Зокрема, США відмовилися підписати договір, що регламентує право усіх держав здійснювати управлінням Інтернетом, у цьому їх підтримали більше 50 держав світу, зокрема Франція, Велика Британія, Канада. На іншому боці виявилися Російська Федерація, Китай, Індія та інші держави наполягають на рівноправності у глобальній мережі, результатом чого стали досить невтішні висновки цього Саміту.

Нині основним документом, який регулює питання міжнародного співробітництва у боротьбі з кіберзлочинністю є «Конвенція про злочинність у сфері комп'ютерної інформації». У ньому сформульовано принципи із забезпечення заходів до боротьби і кіберзлочинністю на національному та міжнародному рівнях. Міжнародне співробітництво сприяє розв'язанню питань у відношенні видачі осіб, які здійснили кібернетичні злочини, загальних принципів взаємної допомоги, конфіденційності та забезпечення збереження інформації, транскордонного доступу до неї тощо [4]. У відповідності з даною Конвенцією, видача осіб іншій стороні можлива за такі типи здійснених кібернетичних злочинів: протизаконний доступ, неправомірне перехоплення, дія на дані функціонування системи, протизаконне використання пристроїв, фаль-

шування та шахрайство з використанням комп'ютерних технологій, правопорушення, пов'язані з дитячою порнографією, порушення авторських та суміжних прав. Допускається також видача осіб іншим державам, у випадку замаху співучасті чи підбурювання до здійснення вищевказаних злочинів. Видача осіб, які здійснили злочини, можлива за наявності у двох сторін передбаченого покарання у вигляді позбавлення волі на максимальний термін не менше одного року.

Важливим документом, у рамках країн-учасниць ООН є Резолюція «з боротьби із злочинним використанням інформаційних технологій», прийнята у 2001 р., у якій вказано на необхідність співробітництва між державами та приватним сектором у боротьба із злочинним використанням інформаційних технологій. Співробітництво у боротьбі із злочинами у сфері інформаційних технологій повинно досягатися шляхом уведення до законодавства відповідальності за інформаційні злочини, транснаціонального співробітництва правоохоронних органів, міжнародного обміну інформацією про проблеми злочинного використання інформаційних технологій, навчання співробітників правоохоронних органів за умови інформаційного суспільства, захисту комп'ютерних систем від несанкціонованого втручання, забезпечення зберігання інформаційних даних та своєчасний збір доказів при розслідуванні злочинів. У п. 1 Резолюції вказано, що інформаційні технології мають розроблятися таким чином, щоб сприяти попередженню та виявленню випадків злочинного використання, відстежуванню злочинців та збиранню доказів [5]. Цей пункт надає правоохоронним органам окремої країни здійснити виявлення та піймання злочинців у короткий термін з більшою ефективністю. Але існує можливість неправомірного доступу злочинців до вищевказаних технологій з використанням скритих можливостей систем з метою здійснення інформаційних злочинів, наприклад, крадіжка персональних даних.

У 1996 р. країнами Великої Вісімки було прийнято рішення про створення спеціальної підгрупи по боротьбі з міжнародними злочинами у сфері високих технологій — «Ліонська група» [6]. В цей же час глави країн схвалили прийняття плану, що складається з десяти пунктів, по протидії кіберзлочинам. З найбільш важливих пунктів документу, варто відмітити: створення в кожній країні контактного центру, працюючого 24 години в добу, для співпраці у боротьбі з інформаційними злочинами, надання допомоги кваліфікованими співробітниками правоохоронних органів іншим державам, розробку і використання сумісних стандартів для отримання і перевірки достовірності електронних даних у ході судового розслідування, ознайомлення із законодавчими методами боротьби з комп'ютерними правопорушеннями країн-учасниць [7].

На щорічній сесії країн НАТО, що проходила у 2009 р., була підготовлена доповідь — «НАТО і Кіберзахист». У доповіді були згадані засадничі принципи, сприяючі ефективному захисту від можливих кібернетичних загроз. Так, на міжнародному рівні, було запропоновано ввести в законодавства країн, такі терміни: «кібервійна», «кібератака», «кібертероризм». Відзначалася необхідність щільнішої співпраці країн з приватними організаціями й Інтернет-

провайдерами для забезпечення захисту. Крім того, у рамках розвитку заходів по кіберзахисту країн НАТО, було рекомендовано сприяти Росії, Китаю, Бразилії і Індії, до швидкого їх приєднання до «Конвенції про злочинність у сфері комп'ютерної інформації» [7]. Блоком країн НАТО, в Талліні, у 2008 р. був відкритий сучасний центр по проведенню досліджень і навчань в області кіберзахисту і веденню військових дій у кіберпросторі [8].

У рамках співпраці держав-учасників СНД, у 2001 р., було вироблено угоду по боротьбі із злочинами у сфері комп'ютерної інформації, за якою, сторони здійснюють співпрацю у формах обміну інформацією, проведенню розслідувань в області комп'ютерної інформації, сприяння в підготовці кадрів, проведення спільних наукових досліджень, створення інформаційних систем, обміну нормативно-правовими актами і науково-технічної літератури по боротьбі з комп'ютерними злочинами [9]. У документі також вказувалося, що співпраця між країнами СНД здійснюється на підставі запитів компетентних органів про сприяння. Час виконання запиту не повинен перевищувати 30 діб з дня його отримання. Відмова в його виконанні допустима, у разі, якщо його виконання суперечить національному законодавству запрошеної сторони. Російська Федерація прийняла Угоду з обмовкою — відмова у виконанні запиту допустима, якщо його виконання може завдати збитку суверенітету або безпеці РФ [10].

Міжнародне законодавство грає дуже важливу роль у боротьбі з кіберзлочинами. Створення 24/7 контактних центрів, законодавче визначення понять «кіберзлочини», видача осіб, що їх вчинили, міжнародна взаємодія співробітників компетентних органів, проведення навчань та обмін інформацією сприяють здійсненню ефективних методів реагування і боротьби з міжнародними злочинами, що здійснюються в кіберпросторі.

Висновки. Розвиток сучасних інформаційних технологій має тенденції до все більшого прискорення, тому нормативно-правова база має не тільки встигати за ним, але й змінюватися, задовольняючи у цьому всі нагальні проблеми людини, суспільства і міжнародного співтовариства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Попередження та розкриття кіберзлочинів: Курс лекцій / За ред. Д.Й. Никифорчука. – К. : НАВС, 2013 – 300 с.

2. *Кривогин М.С.* Международно-правовые аспекты борьбы с кибернетическими преступлениями/ М.С. Кривогин // Государство и право: теория и практика: материалы междунар. заоч. науч. конф. (г. Чита, март 2013 г.). – Чита : Изд-во «Молодой ученый», 2013. — С. 77-79.

3. *Федотов Н.Н.* Форензика – компьютерная криминалистика. – М. : Юридический Мир, 2007. – 432 с.

4. http://pravo.ru/interpravo/legislative/viev/27/7page=20

5. Резолюція, прийнята Генеральною Асамблеєю 55/63 Боротьба із злочинним використанням інформаційних технологій

6. http://www.g8.utoronto.ca/justice_uk2005.htm

7. http://news.bbc.co/uk/2/hi/science/nature/38671.stm

8. http://www.nato.int/cps/en/natolive/topics_78170.htm?

9. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации.

10. Федеральный закон РФ от 01.10.2008 № 164-ФЗ «О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерных технологий.

Кузьменко Б.В., Заїка Ю.О. Типи сучасного особливо небезпечного (шкідливого) програмного забезпечення: правові та технічні аспекти

У статті досліджені технічні та правові питання програмного забезпечення різних типів програмного забезпечення, у тому числі шкідливого (небезпечного).

Ключові слова: *інформаційні технології, шкідливе (небезпечне) програмне забезпечення.*

Кузьменко Б.В., Заика Ю.А. Типы современного особо опасного (вредного) программного обеспечения: правовые и технические аспекты

В статье исследованы технические и правовые вопросы программного обеспечения разных типов, в том числе опасного (вредного).

Ключевые слова: *информационные технологии, опасное (вредное) программное обеспечение.*

Kuzmenko B.V., Zaika Y.A. Types of modern highly dangerous (harmful) software: legal and technical aspects of

The technical and legal questions of software of different types are investigational in the article, including dangerous(harmful).

Keywords: *information technologies, dangerous(harmful) software.*

Стаття надійшла до редакції 22.05.2013.