ПОНЯТТЯ ТА КЛАСИФІКАЦІЯ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ

ЧОВГАН Ігор - аспірант кафедри адміністративного права, інтелектуальної власності та цивільно-правових дисциплін Київського університету інтелектуальної власності та права Національного університету «Одеська юридична академія»

УДК 343.98

ORCID: https://orcid.org/0009-0006-4797-9318

DOI: https://doi.org/10.32782/LAW.UA.2024.1.5

Стаття присвячена дослідженню сутності поняття «шкідливі програмні засоби» та їх видовій характеристиці. Сучасні комп'ютерні технології стають ідеальним засобом для вчинення кіберзлочинів, які створюють загрозу для всього людства, що виводить питання інформаційної безпеки за національні межі, і воно набуває міжнародного значення.

Автор зазначає, що при дослідженні сутності шкідливого програмного забезпечення варто виділяти технічну та кримінально-правову сторони.

У статті аналізуються критерії віднесення технічних засобів, що можуть використовуватися при вчиненні злочинів у сфері інформаційних технологій, до різних груп, визначається різниця між шкідливими технічними засобами та технічними засобами негласного отримання інформації.

Ключові слова: шкідливі програмні засоби, шкідливі технічні засоби, засоби негласного отримання інформації, кіберзлочинність.

Постановка проблеми

Бурхливий розвиток засобів зв'язку та інформаційних технологій визначає тенденції розвитку шкідливих програмних чи технічних засобів. 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, але і до появи нових, раніше невідомих джерел небезпеки для нього [12, с. 4]. У такий період розвитку людства та держав світу загальновідомим є той факт, що несанкціонований та протиправний доступ до інформаційних ресурсів є можливим у тому випадку, коли такі ресурси є недостатньо захищеними. Адже такий доступ до інформаційних ресурсів може спричинити глобальні катастрофи та заподіяти суттєву шкоду суспільним та державним інтересам.

Однак альтернативи розвитку інформаційно-телекомунікаційних систем і, як наслідок, систем інформаційної безпеки не існує, оскільки кіберзлочинці на сьогодні мають змогу здійснити несанкціонований доступ до інформаційних ресурсів державних установ, організацій та фізичних осіб за допомогою шкідливих програмних чи технічних засобів та анонімності, що дозволяє обійти існуючі заходи інформаційної безпеки. Їх атаки стають регулярнішими, складнішими і витонченішими. Дедалі частіше ці атаки виявляють після їх здійснення (якщо взагалі виявляють). Наявні системи виявлення проникнень, бази даних шкідливих програмних засобів та антивірусні програми не в змозі забезпечити потрібний рівень захисту і занадто швидко втрачають актуальність [10, с. 78].

Актуальність цього дослідження полягає в тому, що у випадку вчинення кіберзлочинів можна дестабілізувати економіку країни, окремі її стратегічні об'єкти та інші галузі господарства. Сучасні комп'ютерні технології стають ідеальним засобом для вчинення кіберзлочинів, які створюють загрозу для

всього людства, що виводить питання інформаційної безпеки за національні межі, і воно набуває міжнародного значення.

Одним із прикладів можна назвати кібератаку на компанію мобільного зв'язку «Київстар». Яскравим прикладом є масштабні хакерські атаки на стратегічні об'єкти життєзабезпечення нашої країни. Так, кібератака на мобільний оператор «Київстар» була «однією з найдеструктивніших подібних операцій від початку повномасштабного вторгнення РФ в Україну», йдеться в повідомленні розвідки Британії. У Міністерстві оборони Британії нагадали, що 12 грудня найбільший оператор мобільного зв'язку в Україні «Київстар», який забезпечує мобільним зв'язком та домашнім інтернетом понад половину населення, зазнав кібератаки. Її наслідки тривали щонайменше дві доби. Розвідники кажуть, що серед іншого користувачі залишились без мобільного зв'язку та можливості користуватися інтернетом. Кібератака також вивела з ладу сирени повітряної тривоги, деякі банки, банкомати й торгові термінали [9].

Пізніше до розслідування кібератаки підключилися експерти урядових установ США (Держдепартамент, Міністерство енергетики, Міністерство національної безпеки та ФБР) встановили, що для атаки застосовували шкідливе програмне забезпечення «BlackEnergy», а саму атаку здійснювала російська хакерська група під назвою «Sandworm». Кібератака складалася з п'яти елементів: 1) зараження мереж за допомогою підроблених листів; 2) захоплення управління автоматизованою системою диспетчерського управління з вимиканнями на підстанціях; 3) виведення з ладу мереж безперебійного живлення, модемів, комутаторів та іншої ІТ-інфраструктури; 4) знищення інформації на серверах і робочих станціях (утилітою «KillDisk»); 5)атака на телефонні номери колл-центрів (з російських номерів) з метою відмови від обслуговування знеструмлених абонентів [10, с. 79]. Ці атаки здійснювалися системно та періодично.

Отже, як свідчить сучасна практика, вчинення кіберзлочинів, у переважній більшості випадків вони вчиняються шляхом віддаленого несанкціонованого доступу до комп'ютерів, комп'ютерних систем, комп'ютерних мереж та мереж електрозв'язку за допомогою комп'ютерної техніки загального використання, на яку встановлюється спеціальне програмне забезпечення, наприклад, Dugu, Wiper, Flame, Gauss, Madi, Narilam [5, с. 100].

Стан опрацювання цієї проблематики

Різним аспектам боротьби з кіберзлочинністю, а також частково і дослідженню сутності шкідливих програмних чи технічних засобів, присвятили свої праці І.А. Білан, М.Д. Василенко, О.О. Волков, Б.Д. Леонов, Ю.Ю. Нізовцев, О.А. Парфило, В.О. Рачук, Д.О. Ричка, В.М. Слатвінська, В.С. Серьогін та інші науковці. Однак проблема визначення понятійного апарату та класифікації шкідливих програмних чи технічних засобів досліджена не повною мірою.

Метою статті є дослідження сутності поняття «шкідливі програмні засоби» та їх видова характеристика.

Виклад основного матеріалу

На підставі аналізу ст. ст. 359, 361 та ст. 361-1 можна зробити висновок, що кримінальне законодавство виділяє три види засобів, які потенційно можуть бути використані (використовуються) для вчинення кіберзлочинів. По-перше, це спеціальні технічні засоби отримання інформації, по-друге, – шкідливі технічні засоби, а по-третє, це шкідливі програмні засоби. Якщо у першому випадку ще можна знайти нормативне визначення спеціальних технічних засобів. Так, у п. 2 Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, затверджених Постановою КМУ від 22.09.2016 р. № 669 закріплене наступне визначення поняття «спеціальних технічних засобів» – це технічні, апаратно-програмні, програмні та інші засоби, які відповідають критеріям належності технічних засобів негласного отримання інформації, що мають технічну забезпеченість для негласного отримання (при-

йому, обробки, реєстрації та/або передачі) інформації, призначені для використання у скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності [6]. Оскільки у законодавстві України відсутнє нормативне визначення такого поняття, як «шкідливий програмний засіб», то варто його проаналізувати та з'ясувати сутність.

У відповідності до ст. 1 Закону України «Про авторське право і суміжні права» комп'ютерні програми виступають у вигляді набору інструкцій, слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером (настільним комп'ютером, ноутбуком, смартфоном, ігровою приставкою, смарт телевізором тощо), які приводять його у дію для досягнення певної мети або результату, зокрема операційна система, прикладна програма, виражені у вихідному або об'єктному кодах [13].

У науці кримінального права існують різноманітні підходи до розуміння такого поняття, як «шкідливий програмний засіб. Так, М.Д. Василенко, В.О. Рачук та В.М. Слатвінська назву «шкідливі програми» пояснюють терміном «malware», утвореним від двох англійських слів: «malicious» («зловмисний») і «software» («програмне забезпечення») [2, с. 29]. За результатами аналізу шляхів еволюції їх застосування Ю.Ю. Нізовцев дійшов висновку, що сучасні шкідливе програмне забезпечення – це високотехнологічні програмні засоби, що спеціально розробляються для застосування іноземними спецслужбами, як кіберзброї, при проведенні спецоперацій за конкретними об'єктами посягання [8, с. 232].

О.О. Волков зазначає, що шкідливий програмний засіб – це програмний засіб у вигляді коду, скрипта, активного контенту, програмного забезпечення, який існує в кібернетичному середовищі, спеціально створений і конструктивно призначений та технічно придатний для несанкціонованого втручання в роботу електронно-обчислювальної техніки, який не має будь-якого іншого програмного, технічного, господарського, а також прикладного призначення, що призводить до зміни, модифікації, блокування, копіювання або знищення інформації, споживання технічних ресурсів ЕОТ. Таке визначення, на його думку, буде найбільш точно відповідати вимогам сьогодення та актуальності заходам протидії кіберзлочинності [3, с. 54].

І.А. Білан під шкідливим програмним забезпеченням розуміє програмне забезпечення, яке за умови запуску може завдати шкоди пристрою різними способами, зокрема – призвести до блокування пристрою та його непридатності для використання; крадіжки, видалення або шифрування даних; використання пристрою для атак на інші пристрої; отримання кіберзловмисниками інформації щодо облікових даних, які дозволяють отримати доступ до систем або служб, які використовуються; застосування з метою незаконного майнингу криптовалюти на вашому пристрої; використання платних послуг на основі ваших даних (наприклад, телефонні дзвінки на платні номери) тощо [1, с. 141].

О.А. Гритенко та Г.С. Резніченко Г.С. зазначають, що програмні засоби (комп'ютерні програми) – це певний набір інструкцій у вигляді слів, цифр, кодів, схем, символів, виражених у формі, придатній для зчитування комп'ютером, який приводить цю програму в дію для досягнення певної мети [4, с. 11].

У такому випадку варто розрізняти шкідливе програмне забезпечення з технічної та кримінально-правової сторін.

Традиційний підхід до виявлення шкідливих програм заснований на зіставленні сигнатур досліджуваних файлів [16]. Процедура полягає в наступному: новий вірус / шкідливе програмне забезпечення починає поширюватися; експерти антивірусних компаній отримують зразки для дослідження поведінки вірусу; експерти привласнюють вірусу унікальну сигнатуру, що представляє собою послідовність інструкцій; сигнатура додається в базу даних сигнатур шкідливих програм; клієнти повідомляються про оновлення бази сигнатур; клієнти оновлюють їх бази сигнатур, таким чином стають захищеними від цього виду шкідливого програмного забезпечення. Це технічна сторона розуміння сутності шкідливого програмного забезпечення. А коли ми виходимо із аналізу

диспозиції ст. ст. 361, 361-1 КК України, де вказується на шкідливість та призначеність для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, то таке розуміння шкідливого програмного забезпечення вже виступає, з точки зору кримінально-правової сторони, розуміння його як предмету злочину.

Тепер перейдемо до класифікації шкідливого програмного забезпечення, адже в побуті всі шкідливі програми часто називають комп'ютерними вірусами, хоча це термінологічно некоректно. Так, М.Д. Василенко, В.О. Рачук, В.М. Слатвінська залежно від механізму дії шкідливих програм їх поділяють на чотири класи: комп'ютерні віруси, логічні бомби, хробаки, троянські коні. Найбільш відомими серед знаних «шкідників» є комп'ютерні віруси [2, с. 29]. При чому, такої думку дотримується абсолютна більшість дослідників у сфері кіберзлочинності [1, с. 141-142; 4, с. 11; 5, с. 101; 7, с. 1135].

Дещо подібну позицію у науці кримінального права висловив Д.О. Ричка, який вважає, що найбільш розповсюдженими видами шкідливих програмних засобів є: 1) комп'ютерні віруси – комп'ютерні програми, здатні після проникнення до операційної системи ЕОМ чи до АС порушити нормальну роботу комп'ютера, АС чи комп'ютерної мережі, а також знищити, пошкодити чи змінити комп'ютерну інформацію; 2) програми, призначені для нейтралізації паролів та інших засобів захисту комп'ютерних програм чи комп'ютерної інформації від несанкціонованого доступу; 3) програми-шпигуни, які після їх проникнення до певної АС, комп'ютерної мережі, операційної системи ЕОМ чи окремої комп'ютерної програми забезпечують несанкціонований доступ сторонньої особи до інформації, яка зберігається у ЕОМ, АС, мережі чи програмі або ж непомітно для власника чи законного користувача здійснюють несанкціоновану передачу такої інформації сторонній особі [14, с. 86].

Однак, з метою визначення більш чітких критеріїв належності програмного забезпечення до шкідливого доцільно створити класифікацію програмних засобів, які можна використовувати для тих чи інших шкідливих цілей, залежно від їх початкового призначення. У такому випадку найбільш прийнятною є класифікація, яку запропонували О.А. Парфило та Ю.Ю. Нізовцев, де шкідливе програмне забезпечення поділяється умовно на три групи [10, с. 80].

До першої класифікаційної групи мають належати програмні засоби, спеціально призначені для несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем. Це, так би мовити, класичні шкідливі програмні засоби: віруси, шпигунські програми, блокувачі комп'ютера чи браузера тощо.

Друга група складається з програм подвійного призначення – програм, створених для проведення тих самих дій, що й шкідливе програмне забезпечення, але санкціоновано. Найяскравішим прикладом таких програм є програми для тестів на проникнення (т.зв. пентестів, від англ. penetration test, pentest) [11].

Ще одним типом програм, які можна віднести до другої класифікаційної групи програмних засобів, є програми контролю роботи співробітників. Такі програми забезпечують віддалений контроль дій співробітників, аналіз ефективності їхньої праці та захист інформації від витоків. Зазвичай цього досягають такими шляхами: зняття знімків екрану (скриншотів); перехоплення натискання клавіш; моніторинг запущених процесів; контроль корпоративної пошти; відслідковування месенджерів (Skype, ICQ, MSN тощо); моніторинг веб-сайтів; відслідковування пошукових запитів; контроль соціальних мереж; моніторинг файлів і папок; моніторинг буфера обміну; моніторинг шифрованого трафіка.

Третю класифікаційну групу становлять програми, створені тільки для благонадійних цілей, але які за умови певних налаштувань можна використовувати як шкідливі програмні засоби. Однією з таких програм є Punto Switcher – програма, яка автоматично переключає розкладку клавіатури. Основне призначення програми – збільшення продуктивності та зручності під час роботи з комп'ютером. Працюючи у фоновому режимі, Punto Switcher проводить ста-

тистичний аналіз послідовностей символів, що складають слова, і, якщо поєднання букв виявляється нетиповим для мови, якою вводяться символи, Punto Switcher перемикає мову введення, стирає надруковане, імітуючи натискання клавіші Backspace, і повторно вводить текст уже з правильною розкладкою клавіатури. За певних налаштувань ця, на перший погляд, зовсім невинна програма стає повноцінним клавіатурним шпигуном [17].

Ще одним прикладом третьої групи програм є утиліта ping, яка за замовченням вбудована майже в усі сучасні операційні системи та є доволі корисною для перевірки мережевого з'єднання у мережах TCP/IP. Вона надсилає запити (англ. Echo-Request) протоколу ICMP зазначеному вузлу мережі та фіксує відповіді (англ. Echo-Reply). Час між надсиланням запиту та одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки у маршруті та частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв. Налаштування цієї утиліти на максимальне та безперервне надсилання запитів фактично розпочне атаку на відмову в обслуговуванні [15].

Висновки

Отже, у науці кримінального права та у сфері кібербезпеки також не існує єдиного підходу до визначення поняття «шкідливе програмне забезпечення» та їх класифікації. Аналізуючи різні погляди різноманітних науковців, слід зазначити, що вони досить часто застосовують поняття «шкідливий програмний засіб», не розкриваючи його суті та змісту, чи надають визначення окремих різновидів шкідливого програмного забезпечення, уникаючи загального визначення цього поняття.

Саме тому можна погодитися із запропонованим О.А. Парфило та Ю.Ю. Нізовцевим визначенням поняття «шкідливий програмний засіб», під яким вони розуміють програму або комплекс програм, призначених для несанкціонованої (з порушенням встановленої політики безпеки) зміни режиму роботи атакованої інформаційно-телекомунікаційної системи, спрямованої на порушення порядку обробки інформації або спричинення їй збитків [10, с. 82-83].

Література

1. Білан І.А. Особливості застосування шкідливого програмного забезпечення спецслужбами країни-агресора. Інформація і право. № 2 (45). 2023. С.139-152.

2. Василенко М.Д., Рачук В.О., Слатвінська В.М. Шкідливі програми в контексті розуміння комп'ютерної вірусології та техніко-правової змагальності: міждисциплінарне дослідження. Наукові праці Національного університету «Одеська юридична академія». 2021. Том 29. С. 28-36.

3. Волков О.О. Початковий етап розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів: Дис... канд. юрид. наук: 12.00.08. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 198 с.

4. Гритенко О.А., Резніченко Г.С. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: Лекція з кримінального права. ОДУВС., 2018. 24 с.

5. Леонов Б.Д., Серьогін В.С. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. Інформація і право. № 4 (31). 2019. С.98-106.

6. Ліцензійні умови провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, затверджені Постановою КМУ від 22.09.2016 р. № 669. URL: https://zakon.rada.gov.ua/laws/show/669-2016-%D0%BF#Text.

7. Науково-практичний коментар Кримінального кодексу України / за ред. М.І. Мельника, М.І. Хавронюка. 11-те вид., переробл. та допов. Київ: ВД «Дакор», 2019. 1384 с.

8. Нізовцев Ю.Ю. Еволюція шкідливих програмних засобів та аналіз тенденцій не-

безпеки їх застосування: зб. наукових праць Національної академії СБ України. 2017. № 65. С. 230-238.

9. Одна з наймасштабніших»: розвідка Британії щодо кібератаки на «Київстар. URL: https://www.radiosvoboda.org/a/news-kyyivstar-kiberataka-rozvidka-brytaniya/32733498.html.

10. Парфило О.А., Нізовцев Ю.Ю. Актуальні питання судово-експертного дослідження шкідливих програмних засобів у межах протидії кібертероризму. Криміналістичний вісник. № 1 (25), 2016. С.78-84.

11. Пентест – спосіб реально перевірити ефективність кібербезпеки бізнесу. URL: https://my-itspecialist.com/pentest-is-a-way-to-check.

12. Попередження та розкриття кіберзлочинів: Курс лекцій / За ред. Д.Й. Никифорчука. К.: НАВСУ, 2013. 300 с.

13. Про авторське право і суміжні права: Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

14. Ричка Д.О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: Дис... канд. юрид. наук: 12.00.08. Дніпровський національний університет імені Олеся Гончара, Дніпро; Університет державної фіскальної служби України, Ірпінь, 2019. 212 с.

15. Як перевірити пінг через командний рядок? URL: https://hostiq.ua/wiki/ukr/ping/.

16. Jinrong Bai, Junfeng Wang, Guozhong Zou. A Malware Detection Scheme Based on Mining Format Information / Jinrong Bai – The Scientific World Journal. 2014, Vol. 2014. URL: https://www.researchgate.net/publication/263712293_A_Malware_Detection_Scheme_Based_on_Mining_Format_Information.

17. Punto Switcher – що це за програма і чи потрібна вона? URL: https://hi-news.pp.ua/tehnka-tehnologyi/print:page,1,3069-punto-switcher-scho-ce-za-programa-chi-potrbna-vona.html.

Chovgan I.

CONCEPT AND CLASSIFICATION OF MALICIOUS SOFTWARE OR TECHNICAL MEANS

The article is devoted to the study of the essence of the concept of "malicious software" and their specific characteristics. Modern computer technologies are becoming an ideal tool for committing cybercrimes, which pose a threat to all of humanity, which takes the issue of information security beyond national borders, and it acquires international importance.

The author notes that based on the analysis of Art. Art. 359, 361 and Art. 361-1, it can be concluded that criminal legislation distinguishes three types of means that can potentially be used (used) to commit cybercrimes: special technical means of obtaining information, malicious technical means and malicious software means.

The article indicates that when investigating the essence of malicious software, it is worth highlighting the technical and criminal legal aspects.

On the technical side, malware is starting to spread; experts from antivirus companies receive samples to study virus behavior; experts assign a unique signature to malicious software, which is a sequence of instructions; the signature is added to the malware signature database; clients are notified of updates to the signature database; clients update their signature databases, thus becoming protected against this type of malware. Based on the analysis of the disposition of Art. Art. 361, 361-1 of the Criminal Code of Ukraine, which indicates harmfulness and purpose for unauthorized interference in the work of information (automated), electronic communication, information and communication systems, electronic communication networks, then this understanding of malicious software comes from the point of view of criminal law.

The article analyzes the criteria for assigning technical means that can be used in the commission of crimes in the field of information technologies to different groups, and defines the difference between harmful technical means and technical means of secretly obtaining information.

Keywords: malicious software, malicious technical means, means of secretly obtaining information, cybercrime.