безпека виступає як чинник та критерій обмеження прав і свобод людини та громадянина (частина друга статті 32, частина третя статті 34, частина перша статті 36, частина друга статті 39, частина друга статті 44). По-четверте, національна безпека розглядається як застереження для інститутів громадянського суспільства (частина перша статті 37). По-п'яте, безпека як основа діяльності, соціального призначення та завдання органів публічної влади (пункт 12-1 та 22 частини першої статті 85, пункт 1, 14, 17 та 18 частини першої статті 106, частина перша-восьма статті 107, пункт 3 та 7 статті 116, пункт 7 частини першої статті 138). По-шосте, безпека як найважливіше питання, що визначається виключно законом (пункт 17 частини першої статті 92).

Отже, на базі норм Конституції та законів України можна зробити висновок про суттєве місце захисту конституційного ладу у системі забезпечення національної безпеки України.

1. Конституція України : прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року // *Відомості Верховної Ради України*. – 1996. – № 30. – Ст. 141.

2. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018, № 31, ст. 241.

3. Про оборону України : Закон України від 6 грудня 1991 р. № 1932-XII. *Відомості Верховної Ради України*. 1992, № 9, ст. 106.

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

ДО КРИМІНАЛЬНО-ПРАВОВОГО РОЗУМІННЯ СУТНОСТІ ТА ОЗНАК ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ

Бурхливий розвиток засобів зв'язку та інформаційних технологій визначає тенденції розвитку шкідливих програмних чи технічних засобів. Актуальність даного дослідження полягає в тому, що у разі отримання кіберзлочинцями доступу до комп'ютерних мереж у них з'являється можливість доволі ефективно виводити з ладу системи керування та зв'язку державних установ та організацій, дестабілізувати роботу фінансових ринків і стратегічних об'єктів життєзабезпечення. Яскравим прикладом є масштабна хакерська атака на компанію мобільного зв'язку «Київстар» у результаті якої 24 млн. абонентів залишилися без зв'язку. Вона спричинила «катастрофічні»

руйнування та мала на меті завдати психологічного удару й отримати розвідувальну інформацію. За цією атакою стоїть хакерське угруповання Sandworm, яке є штатним підрозділом російської воєнної розвідки і раніше неодноразово здійснювало кібератаки на українські об'єкти, зокрема і на операторів зв'язку та інтернет-провайдерів [1]. Зокрема, вказане угруповання Sandworm у грудні 2015 року через несанкціоноване втручання в роботу об'єктів нашої енергосистеми частково без електропостачання залишило Івано-Франківську область (загалом 230 тисяч місцевих мешканців). А у червні 2017 року шкідливі програмні засоби було виявлено в комп'ютерних мережах аеропорту «Бориспіль», до якої входить і управління повітряним рухом аеропорту, Київського метрополітену, Ощадбанку, «Нової Пошти», компанії «Київенерго» та «Укренерго» [2].

Кримінальне законодавство України містить низку статей, які прямо або опосередковано стосуються незаконного виготовлення, використання, збуту, розповсюдження шкідливих програмних чи технічних засобів, що використовуються для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, – ст. 359 КК (незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації; ст. 361 КК (несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж), ст. 361-1 КК (створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) [3]. Як бачимо, кримінальний закон 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 Кабінету Міністрів України 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 (прийому, обробки, реєстрації та/або передачі) інформації, призначені для використання у скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності [4]. На жаль, визначення понять «шкідливий програмний засіб» чи «шкідливий технічний засіб» у національному законодавстві взагалі відсутні. В такому випадку

спробуємо проаналізувати та надати власні визначення вказаних понять.

Програмні чи технічні засоби стають шкідливими за умови запуску та свого функціонування можуть завдати шкоди пристроям 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 кіберзлочинцями 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 [5, с.141].

Так, на початку квітня 2010 року ОСОБА_2, діючи умисно з корисливих мотивів, перебуваючи у себе вдома, а саме на орендованій квартирі у м. Києві, використовуючи власний ноутбук торгової марки «DELL», моделі «Vostro3700», серійний номер № 2FH87L1, можливість доступу до мережі Інтернет, а також власний досвід у сфері створення програмного забезпечення, на мові програмування «С++» шляхом написання вихідних кодів розпочав створення шкідливого програмного засобу – шкідливої комп'ютерної програми під назвою «ІНФОРМАЦІЯ_11», призначеної для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), якій у подальшому ним було надано умовну назву «ІНФОРМАЦІЯ_12», з метою його збуту через мережу Інтернет [6].

Отже, створення шкідливих програмних чи технічних засобів полягає у виготовленні будь-яким способом відповідного пристрою, обладнання чи устаткування. Причому, зважаючи на специфічність такого устаткування, виготовлення може полягати не лише у його фізичному збиранні, а й, наприклад, у розробці чи налагодженні устаткування відповідним чином або його програмуванні (перепрограмуванні), після чого пристрій набуватиме ознак шкідливості.

Наступною ознакою шкідливих програмних чи технічних засобів, виступає «призначення для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», вказує на їх спеціальне призначення – несанкціоноване втручання в роботу комп'ютерної техніки чи мереж електрозв'язку. Як зазначає М.В. Карчевський, на відміну від будь-яких інших комп'ютерних програм та обладнання шкідливі програмні та технічні засоби спеціально розробляються для несанкціонованого втручання, тобто порушення режиму роботи інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [7, с.135].

Характеризуючи ознаку «призначення для несанкціонованого втручання», необхідно виходити із наступного. У Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» наводиться дефініція такої категорії як «несанкціоновані дії щодо інформації в системі», до яких відносяться такі, що провадяться з порушенням порядку доступу до

цієї інформації, установленого відповідно до законодавства. Згідно зі ст. 1 зазначеного Закону доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі. Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації. Обробка інформації в системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів [8]. Виходячи з аналізу наведених категорій, можна зробити висновок, що несанкціоноване втручання в роботу – це порушення користувачем умов та правил отримання і обробки інформації. Такі умови та правила отримання і обробки інформації встановлюються володільцем інформації [9, с. 246].

Виходячи з аналізу диспозиції ст. ст. 361, 361-1 КК України можна виділити низку ознак, якими наділені програмні чи технічні засоби. Такими ознаками є: 1) шкідливість, 2) призначеність для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Відсутність вказаних ознак виключає можливість визнати вказані програмні чи технічні засоби як предмет злочину, передбаченого ст. 361-1 КК України.

---

1. Російські хакери перебували у системі телекомоператора «Київстар» щонайменше з травня 2023 року. Про це сказав в інтерв'ю Reuters голова департаменту кібербезпеки СБУ Ілля Вітюк. URL: https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307

2. Через хакерську атаку у Борисполі можуть затримувати рейси. URL: https://www.bbc.com/ukrainian/news-40417148

3. Кримінальний кодекс України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

4. 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 Кабінету Міністрів України від 22.09.2016 р. № 669. URL: https://zakon.rada.gov.ua/laws/show/669-2016-%D0%BF#Text

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

6. Вирок Дарницького районного суду м. Києва від 28 груд. 2015 р. Справа № 753/23764/15-к. Єдиний державний реєстр судових рішень : сайт. URL: http://reyestr.court.gov.ua/Review/54799070

7. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.

8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

9. Курман О. В. Способи несанкціонованого втручання в роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Право і суспільство.2017. № 4. С. 245-249.