ПРОТИДІЯ КІБЕРАТАКАМ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЖИТТЕЄЗАБЕЗПЕЧЕННЯ ПІД ЧАС ВІЙСЬКОВОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

Наталія Євгенівна ФІЛІПЕНКО,

доктор юридичних наук, доцент, професор кафедри права (702) гуманітарно-правового факультету Національного аерокосмічного університету ім. М. Є. Жуковського "Харківський авіаційний інститут"
https://orcid.org/0000-0001-9469-3650

В умовах збройної агресії росії проти України особливої уваги набувають питання захисту об'єктів критичної інфраструктури та життєзабезпечення від різноманітних кібератак країни-агресора.

Як зазначається у звітах Служби безпеки України, з початку повномасштабного вторгнення росії виявили та нейтралізували понад 120 потужних кібератак на ресурси органів державної влади та військового управління України, а також ІТ-систем об'єктів критичної інфраструктури, операторів зв'язку та ЗМІ. За даними Державної служби спеціального зв'язку та захисту інформації України, за місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року. Найпопулярнішими видами атак залишаються фішингові розсилання, розповсюдження шкідливого програмного забезпечення, DDoS-атаки. Як зазначає голова Держспецзв'язку Юрій Щиголь, атакують передусім державні установи, фінансовий, оборонний сектор, операторів зв'язку, місцеві органи влади, логістичні компанії, медіа. Ми також бачимо численні спроби хакерів зламати ресурси, які збирають інформацію про військові злочини рф в Україні. Держспецзв'язку докладає зусиль для забезпечення їхнього кіберзахисту [1].

На жаль, мусимо зазначити про певні недоліки у протидії таким загрозам. Адже рівень захисту внутрішньої критичної інфраструктури та авіації не завжди відповідає сучасним світовим вимогам безпеки. Дуже часто це відбувається через корупцію або недоліки в організаційно-господарській діяльності на критичних інфраструктурних та авіаційних об'єктах [2, с. 206].

У цьому зв'язку якісна, своєчасна та ефективна протидія кримінальним правопорушенням, пов'язаним з використанням електронних засобів, у даний час не може бути здійснена без використання спеціальних знань в області новітніх інформаційних технологій. Особливості виявлення і дослідження криміналістично-значимої комп'ютерної інформації пов'язані, перш за все, з тим, що дана область спеціальних знань включає в себе ряд досить різнорідних наукомістких напрямів, таких як електроніка, електротехніка, інформаційні системи і процеси, радіотехніка та зв'язок, обчислювальна техніка (у т.ч. програмування) і автоматизація. Злочини розглянутих категорій носять найчастіше латентний характер, не залишають видимих слідів і складні з точки зору розкриття і збирання доказової

інформації в зв'язку з широким застосуванням засобів віддаленого доступу, захисту даних тощо.

Як і будь-який інший рід судової експертизи, потреба в якому виникла з кінця XX століття з появою нових видів злочинів і вдосконаленням технічних засобів (генетична, лінгвістична), комп'ютерна експертиза пройшла всі стадії розвитку - від формулювання предмета і завдань, визначення термінології до формування сучасної академічної та методичної школи, що відповідає вимогам кримінального процесу, технічним вимогам дослідження об'єктів високих технологій. На різних стадіях формування даного роду експертиз застосовувалися різні найменування (програмно-технічна, інженерно-комп'ютерна, судово-технічна експертиза інформаційно-обчислювальних систем, інформаційно-технічна, інформаційно-технологічна експертиза, судово-кібернетична експертиза). Сьогодні використовується термін "комп'ютерно-технічна експертиза" (далі – КТЕ), який застосовується в судово-експертних установах Міністерства юстиції України. Однак, незалежно від назви, незмінним залишається її висока технократичність і потреба з боку як правоохоронних органів, так і суспільства в цілому.

Основним завданням експертів, при здійсненні ними комп'ютерно-технічної експертизи є відповідь на питання, що вимагають спеціальних знань в області "форензік" (комп'ютерної криміналістики) - знань про методи пошуку, закріплення і дослідження цифрових доказів за злочинами, пов'язаними з комп'ютерною інформацією (кіберзлочинів). Комп'ютерно-технічна експертиза дозволяє сформувати цілісну побудову доказової бази шляхом вирішення більшої частини діагностичних та ідентифікаційних питань, тобто вирішує завдання, пов'язані з пошуком, виявленням, оцінкою і аналізом інформації, що міститься в комп'ютерній системі. В результаті ТКЕ, що проводиться під час розслідування кримінальних правопорушень, пов'язаних з порушенням інформаційної безпеки у відкритих комп'ютерних мережах, розкраданням (руйнуванням, модифікацією) інформації та порушенням інформаційної безпеки, формується інформація про уразливість процесів переробки інформації в інформаційних системах. При цьому результати ТКЕ можуть бути використані фахівцями з інформаційної безпеки для вдосконалення існуючих засобів захисту інформації та забезпечення інформаційної безпеки.

З огляду на розробки вчених [3, с. 296-298], сучасний рівень розвитку науки і техніки, практичний досвід здійснення комп'ютерно-технічної експертизи, зрозуміло, що в якості основних областей досліджень фахівців у царині КТЕ є інтегровані та вбудовані системи, відкриті системи, системи зв'язку, а також мультимедійні об'єкти. У більшості випадків метою подібних досліджень є вирішення діагностичних та ідентифікаційних завдань при дослідженнях інформаційної системи, отримання доступу до електронного обладнання й інформації. Так, особлива увага при дослідженнях мобільних терміналів приділяється телекомунікаційним сервісів SMS, EMS, MMS, тому що вони можуть надавати відомості про осіб, причетних до вчинення кримінальних дій, в тому числі і в мережах мобільного зв'язку.

Великий обсяг роботи експертів вітчизняних судово-експертних установ та їх закордонних колег (наприклад, в Нідерландах, Чехії, Італії), пов'язаний із дослідженням *відкритих систем*, які охоплюють різні операційні системи, їх

архітектури, апаратно-програмні комплекси. Апаратними об'єктами експертизи в цих випадках є різні комп'ютерні системи: від мініатюрних персональних комп'ютерів до надзвичайно великих суперкомп'ютерів. Для цих систем характерна наявність різноманітних електронних накопичувачів даних: від жорстких і флоппі-дисків, стрічок, CD-ROM, DVD, магнітооптичних накопичувачів до RAID-масивів, тобто здійснюється аналіз комп'ютерного середовища. В цілому експертами успішно застосовуються при розслідуванні злочинів та отриманні інформації з електронних носіїв, такі операції як: злом захистів під паролем; моделювання пам'яті вилучених електронних апаратів в пам'яті комп'ютера (органайзерів, стільникових телефонів, сім-карт, смарт-карт і модулів, смартфонів та фнших носіїв інформації, за допомогою апаратного програмного інструментарію (Cardreader CardLabs) тощо.

Географічні інформаційні системи та *комунікаційні інформаційні системи* є наступним перспективним напрямом експертів, що спеціалізуються у мережевих відкритих системах. Основними завданнями тут є аналіз різних інформаційних потоків з метою їх виявлення, інтерпретації повідомлень, відновлення інформації, розкодування даних, виявлення використаних різних алгоритмів тощо. Головне місце в експертному дослідженні займає вивчення протоколів передачі даних, в тому числі повного стека протоколів за рівнями OSI. Ця модель включає до себе маршрутизовані і транспортні протоколи. Окремим видом є проведення досліджень телекомунікаційних мереж забезпечення стільникового зв'язку GSM, GPS, GPRS - комунікацій. Однак дії фахівців з перехвату сигналів зв'язку, їх аналізу, ідентифікації систем локального і глобального зв'язку, географічної області, локалізації користувача/ адресата, найчастіше пов'язані з проведенням оперативно-розшукової діяльності та використовуються експертами лише у прикладних цілях для вирішення окремих завдань. Подібна ситуація спостерігається і в дослідженнях, пов'язаних із розслідуванням різноманітних злочинів у глобальних мережах. Ця область спеціальних знань включає до себе як завдання ідентифікації та діагностики користувачів мережі, їх ресурсів, так і аналіз роботи провайдерів, характеристик досліджуваних трафіків та інформаційних систем Internet, активне використання різних програм-браузерів тощо. Сучасні Інтернет технології, технології розробки програмного забезпечення (OLE, ActiveX), різні plug-ins, Java-аплети значно розширюють список можливих форматів даних та об'єктів програмного забезпечення, що потрапляють до уваги експертів. Даний перелік напрямів комп'ютерно-технічної експертизи не є вичерпним, і може бути змінений та доповнений з урахуванням сучасного розвитку комп'ютерної техніки, високих технологій та програмного забезпечення, а також розробок нових методик дослідження технічних і програмних засобів.

Підсумовуючи викладене зазначимо, що кіберпростір має стати інструментом нашої негайної та потужної відповіді на агресію; створювати й удосконалювати інтелектуальний потенціал країни (адже навіть за два місяці війни росія не змогла суттєво нашкодити об'єктам критичної інфраструктури України завдяки злагодженій роботі усіх військових та цивільних структур; розгорнути багаторівневий захист об'єктів критичної інфраструктури та

життєзабезпечення від різноманітних кібератак країни-агресора, залучаючи можливості країн-партнерів (США, Великої Британії та країн Євросоюзу).

Список використаних джерел:

1. За час війни кількість хакерських атак в Україні зросла втричі. URL: https://www.ukrinform.ua/rubric-technology/3447656-za-cas-vijni-kilkist-hakerskih-atak-v-ukraini-zrosla-vtrici.html

2. Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko (2020) Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Integrated Computer Technologies in Mechanical Engineering – 2020. Synergetic Engineering P. 206-220. ISBN 978-3-030-66716-0 ISBN 978-3-030-66717-7 (eBook). https://doi.org/10.1007/978-3-030-66717-7

3. Можаєв О. О., Логвиненко М. О., Чорний С. В. Автоматизована система накопичення емпіричних даних у сфері комп'ютерно-технічних експертиз // Актуальні питання протидії кіберзлочинності та торгівлі людьми : збірник матеріалів Всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2018.С. 296-298.