захоплення важливих державних об'єктів або місцевостей, що загрожує безпеці громадян і порушує нормальну діяльність органів державної влади та органів місцевого самоврядування; участь у підтриманні або відновленні правопорядку в районах виникнення особливо тяжких надзвичайних ситуацій техногенного чи природного характеру (стихійного лиха, катастроф, особливо великих пожеж, застосування засобів ураження, пандемій, панзоотій тощо), що створюють загрозу життю та здоров'ю населення; участь у припиненні групових протиправних дій осіб, узятих під варту, засуджених, а також ліквідації наслідків таких дій в установах попереднього ув'язнення, виконання покарань та ін.

Література

1. Про Національну гвардію України: Закон України від 13 бер. 2014 року № 876-VII. URL: https://zakon.rada.gov.ua/laws/show/876-18#Text.

2. Ковалів М.В., Єсімов С.С., Лозинський Ю.Р. Правове регулювання правоохоронної діяльності: навчальний посібник. Львів: ЛьвДУВС, 2018. 323 с.

3. Терехов В.Ю. Сучасні аспекти теоретико-правового забезпечення реалізації правоохоронної функції держави. *Наукові записки. Серія: Право.* 2021. № 11. С. 91-96.

4. Братель С.Г. Функції правоохоронної сфери. *Право і суспільство*. 2015. № 4. С. 63-66.

5. Тацій В. Поняття та система правоохоронних органів: у контексті системних змін до Конституції України. *Науковий вісник Національної юридичної академії імені Ярослава Мудрого.* Випуск 4 (71). С. 3–17.

6. Шай Р.Я. Правоохоронна функція правової держави: теоретико-практичний аспект: автореф. дисертації на здоб. наук. ступ. к.ю.н. за спеціальністю 12.00.01. Львів, 2012. 20 с.

УДК 342.9(043.2)

Грекова Л.Ю., старший викладач
кафедри кримінального права і процесу
Павроз Д.О., здобувач вищої освіти
першого (бакалаврського) рівня,
Національний авіаційний університет, м. Київ, Україна

ЦИФРОВА КРИМІНАЛІСТИКА: ФОРМУВАННЯ ТА РОЛЬ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКОВОГО СЕРЕДОВИЩА УКРАЇНИ

У сьогоднішніх реаліях цифровізація стає не лише сучасним трендом у суспільстві, а й вирішальним фактором економічного, соціального, політичного та міжнародного зростання будь-якої країни. Надання Україні статусу кандидата на членство в ЄС створило додатковий імпульс для

гармонізації підходу до цифрової трансформації. У цьому контексті участь України у програмі «Цифрова Європа» до 2027 року є важливою подією, спрямованою на прискорення економічного відновлення та цифрової трансформації України, створення єдиного цифрового ринку з ЄС та наближення цифрового сектору України до європейського, що зробило її пріоритетом національної політики цифрової трансформації в умовах війни [1, с. 325-327].

З 24 лютого 2022 року на розвиток та функціонування України, суспільства та світу в цілому суттєво вплинула повномасштабна збройна агресія російської федерації та запровадження воєнного стану в нашій країні, що змінило завдання та пріоритети нашої держави. Згідно з офіційною статистикою Генеральної прокуратури, найпоширенішими злочинами є: а) агресія та воєнні злочини – 37037 зареєстрованих злочинів (станом на 1 грудня 2022 року); б) злочини проти основ національної безпеки – 16542 злочини; в) злочини проти дітей – 396 дітей загинули та 779 дітей отримали поранення [2].

Очевидно, що така кримінальна динаміка та тенденції в Україні у воєнний час суттєво вплинули на визначення пріоритетних завдань судової влади та зміну діяльності системи кримінальної юстиції. У цьому контексті існує нагальна потреба у виробленні нових підходів до протидії сучасним військовим викликам, модернізації та оновленні правоохоронних і судових інституцій відповідно до умов воєнного стану, а також у створенні та впровадженні ефективної системи протидії сучасним загрозам, у тому числі й судовими засобами [3, с. 92-102].

Зокрема, збільшення ролі криміналістичних знань в удосконаленні та забезпеченні безпечного середовища в нашій країні стає дедалі актуальнішим, а оптимізація та підвищення ефективності протидії сучасним злочинам, (в тому числі воєнним та кіберзлочинам) вирішується, шляхом активного використання цифрових технологій. Найбільш відомими напрями цього процесу є цифрове обсягове моделювання (Digital Forensic Imaging), яке полягає у створенні точної копії цифрового пристрою для подальшого аналізу, не змінюючи вихідних даних; відновлення видалених даних (Deleted Data Recovery), що використовується для відновлення втраченої інформації з цифрових пристроїв; можливости комп’ютерної, в тому числі мобільної криміналістики, що включають збір, аналіз та інтерпретацію даних з комп’ютерів, з мобільних пристроїв, таких як смартфони та планшети для використання у кримінальних справах; дослідження діяльності у мережі для виявлення та відслідковування кіберзлочинців, розслідування витоків даних та аналізу потоків даних тощо. Крім того, все більш обертів набирають цифровий аналіз медіа (Digital Media Analysis) - включає аналіз зображень, відео та аудіофайлів для виявлення підробок, маніпуляцій або інших доказів; цифрова стеганографія (Digital Steganography) -

дослідження та розкриття прихованої інформації в цифрових зображеннях, відео або аудіофайлах.

У цьому контексті можна говорити про посилення тенденцій формування та впровадження нових наукових дисциплін - цифрової криміналістики, цифрової судової експертизи та цифрової кримінології [4].

У воєнних реаліях технології штучного інтелекту стали центральними для забезпечення безпекового середовища України та збору доказів воєнних злочинів у сфері цифрової криміналістики. У сучасних умовах війни особливого значення набувають такі напрямки цифрової криміналістики: отримання інформації з мобільних пристроїв мобільних телефонів, вилучених у фігурантів кримінальних справ; отримання інформації з персональних комп'ютерів фізичних та юридичних осіб; отримання інформації з серверів та інших носіїв інформації установ та організацій; отримання інформації з радіочастотних ідентифікаторів, GPS-трекерів, датчиків, інформації відеоспостереження та позиціонування, а також з наступних мережевих сервісів [5].

Таким чином, завдяки науково-технічному прогресу процес досудового розслідування дозволяє більш повно формувати доказову базу у кримінальних розслідуваннях, гарантуючи таким чином якість судового розгляду у кримінальних провадженнях, а застосування цифрової криміналістики значно покращує можливості збору, дослідження та використання цифрової інформації як доказів у сучасній війні, в тому числі у забезпеченні безпекового середовища України. У цьому контексті посилення досліджень ролі цифрової криміналістики у документуванні воєнних злочинів, скоєних російською федерацією на території України, є перспективним та стратегічним напрямом розвитку криміналістики як європейської науки.

Література

1. Шевчук В.М. Європейський вектор розвитку сучасної криміналістики. Адаптація правової системи України до права Європейського союзу: теоретичні та практичні аспекти: *матеріали VI Всеукр. наук.-практ. конф*. (м. Полтава, 29.09.2022). Полтава: Полт. юрид. ін-т, 2022. С. 325-327.

2. Сайт Офіса Генерального прокурора. URL: https://www.gp.gov.ua/.

3. Шепітько В.Ю., Коновалова В.О., Шевчук В.М. та ін. Науково-технічне забезпечення слідчої діяльності в умовах змагального кримінального процесу. Питання боротьби зі злочинністю. 2021. Вип. 42. С. 92-102.

4. Борисова К.Є., Світличний В.А. Застосування цифрової криміна-лістики. Сучасні тенденції розвитку криміналістики та кримінального процесу в умовах воєнного стану: тези доп. Міжнар. наук.-практ. конф.(м. Харків, 25 лист. 2022 р.). Харків: ХНУВС, 2022. С. 83-84.

5. Степанюк Р.Л., Перлін С.І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник*

Луганського держ. ун-ту внутр. справ ім. Е.О. Дідоренка. 2022. № 3 (99). С. 283-294. С. 288

УДК 343.9(043.2)

Дрижакова Д.Ю., здобувач вищої освіти
третього (освітньо-наукового) рівня,
Київський національний університет імені Тараса Шевченка,
м. Київ, Україна

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЯК СПОСІБ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНИХ СИСТЕМ

За останні декілька десятиліть життя більшості людей та суспільства, в цілому, було настільки автоматизовано, що будь-яка звичайна діяльність людини не уявляється без персональних комп'ютерів, комп'ютерних мереж, мереж електрозв'язку.

Ефективна протидія кіберзлочинності потребує чіткого визначення шкідливого програмного забезпечення (ШПЗ).

Законодавством не встановлено чіткого визначення ШПЗ, однак шкідливі програмні засоби визначають як створення або пристосування комп'ютерної програми, що призначена для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. На їхнє переконання, це, здебільшого, різноманітні види комп'ютерних вірусів [1].

Відсутність чіткої дефініції ШПЗ у законодавстві України створює ряд проблем:

– Ускладнює кваліфікацію протиправних діянь, пов'язаних з використанням ШПЗ.

– Заважає формуванню єдиного підходу до пошуку, фіксації та експертизи ШПЗ.

– Унеможливлює чітке розмежування шкідливих та легальних програм.

Для вирішення цих проблем:

– Необхідно розробити та прийняти чітке визначення ШПЗ у законодавстві.

– Це визначення має включати криміналістичні ознаки та критерії віднесення програм до категорії шкідливих.

– Важливо також розробити методики та стандарти для пошуку, фіксації та експертизи ШПЗ.

Тільки за умови чіткого визначення ШПЗ та наявності відповідних методик правоохоронні органи зможуть ефективно протидіяти