перед слідчим на такому етапі є збір і фіксація, як матеріальних так і ідеальних слідів вчинення кримінального правопорушення.

Список використаних джерел

1. Щербаковський М.Г. Використання доказів як етап доказування у кримінальному провадженні. *Вісник Харківського національного університету внутрішніх справ*. 2017. Вип. 2. С. 88–95.

2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

3. Балонь А.Б. Обставини, що підлягають встановленню за злочинами у сфері службової діяльності, пов'язаної з наданням публічних послуг. *Митна справа*. 2013. № 3. Ч. 2. Кн. 2. С. 55–60.

Сенюк Ольга Петрівна,
слухач навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ
Лапка Оксана Ярославівна,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, кандидат юридичних наук, доцент

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

У сучасному світі цифрові технології стали фундаментом функціонування не лише економіки та державного управління, а й усіх сфер суспільного життя. Вони забезпечують швидкий обмін інформацією, зручну комунікацію, дистанційне управління системами та сервісами. Проте у період воєнного стану роль цифрових технологій набуває подвійного значення: з одного боку, вони сприяють оперативному управлінню та координації, а з іншого — стають потенційною ціллю для кібератак, інформаційного впливу та деструктивного втручання.

Сучасні війни дедалі більше набувають гібридного характеру, і кібервиміри конфліктів стають одними з ключових інструментів тиску. Кіберзагрози здатні спричинити колапс критичної інфраструктури, завдати шкоди економіці, паралізувати державне управління та підірвати довіру населення до органів влади. У цьому контексті інформаційна безпека стає визначальним чинником національної стійкості, а цифрові технології — головним засобом її забезпечення [4].

Кіберзагрози під час воєнного стану мають системний характер. Злочинці і ворожі структури здійснюють атаки на державні інформаційні системи з метою

знищення або викривлення важливої інформації, доступу до стратегічних баз даних або поширення деструктивного контенту. Ці атаки спрямовані не лише на технічне порушення роботи об'єктів, а й на створення «інформаційного шуму», що ускладнює громадянам відокремлення правди від маніпуляцій [2, с. 42–49]. Це підриває довіру до державних інституцій, дестабілізує моральний стан громадян і послаблює суспільну єдність.

Найбільш вразливими до таких загроз є об'єкти критичної інфраструктури: енергетичні мережі, банківська система, транспорт, зв'язок, а також системи охорони здоров'я. Саме тому кіберзахист цих елементів має стати пріоритетом державної політики у сфері національної безпеки. До ключових заходів, що забезпечують ефективну протидію кіберзагрозам, належать: впровадження багаторівневої автентифікації, шифрування даних, автоматизовані системи виявлення атак (IDS/IPS), постійний аудит інформаційної безпеки, а також моніторинг інцидентів у режимі реального часу [1].

Агресивні кібердії противника становлять складну комбінацію інформаційного впливу та техногенного втручання. Їх метою є порушення комунікаційної цілісності суспільства, послаблення психологічної стійкості населення та посів недовіри до органів влади. Через цілеспрямоване поширення деструктивного контенту та фальсифікованих повідомлень, противник намагається розмити межу між правдою і вигадкою, що створює ефект «інформаційного шуму». Одночасно здійснюються втручання в роботу військових систем, урядових порталів, логістичних і банківських мереж з метою їхньої тимчасової нейтралізації або виведення з ладу. Ці дії не лише створюють технологічні ризики, а й провокують ланцюгову реакцію суспільної напруги, що в умовах воєнного стану набуває особливої ваги [4, с. 24].

Незважаючи на важливість цифрової безпеки, чинна правова база України у сфері кібербезпеки поки що залишається недостатньо адаптованою до швидко змінюваної природи кіберзагроз. Указ Президента України №447/2021 «Про Стратегію кібербезпеки України» визначає загальні напрями політики, однак у практичному вимірі органи влади часто діють в умовах нормативної невизначеності, що ускладнює своєчасне реагування на складні кіберінциденти [3].

На наш погляд, в умовах збройного конфлікту та після його завершення надзвичайно актуальним є питання відновлення цифрової інфраструктури. Доцільно виділити три ключові етапи цього процесу::

- 1-*й етап* – детальний аудит зруйнованих об'єктів, оцінка рівня пошкоджень та формування черговості відновлення, зокрема, у сферах енергетики, зв'язку та банківської інфраструктури;
- *2-й етап* – впровадження передових технологій захисту, включаючи штучний інтелект для автоматичного виявлення загроз, розширене шифрування, системи резервного збереження;
- *3-й етап* – підготовка кадрів і міжнародне співробітництво — створення кіберрезерву, залучення експертів, інтеграція досвіду партнерів і навчання фахівців для протидії майбутнім загрозам..

Важливим елементом інформаційної безпеки є також формування цифрової грамотності серед населення. Кожен користувач має розуміти базові принципи захисту персональних даних, способи розпізнавання фейкової інформації та шкідливих посилань. Без належної цифрової обізнаності навіть найсучасніші технічні системи можуть виявитися вразливими.

В умовах воєнного стану, коли боротьба відбувається не лише за території, а й за свідомість, саме цифрові технології визначають ефективність державного управління, сталість соціальної системи й перемогу в інформаційному просторі. Цифрова безпека – це не лише технічне завдання, а й стратегічна складова виживання держави у XXI столітті.

Список використаних джерел

1. Ковалів М.В., Єсімов С.С., Ярема О.Г. Інформаційне право України : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2022. 416 с.

2. Кудінов В.А., Яровий К.В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). *Сучасна спеціальна техніка.* 2023. № 3 (74). С. 42-49.

3. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

4. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. К.: Вид. НАВС, 2012. 104 с.

Уколов Олексій Леонідович,
аспірант Інститут держави і права імені В.М. Корецького НАН України

ЮРИДИЧНІ ФІКЦІЇ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ: МІЖ НЕОБХІДНІСТЮ ТА МАНІПУЛЯЦІЄЮ

Актуалізація проблематики інформаційної безпеки в умовах воєнного стану зумовила необхідність перегляду низки правових підходів до регулювання інформаційних відносин. Одним із таких підходів є використання юридичних фікцій – особливих правових конструкцій, що дозволяють створювати правову реальність, необхідну для захисту державних інтересів, незалежно від фактичного стану справ.

У загальній теорії права поняття юридичної фікції досліджували такі науковці, як А. Росс, Г. Радбрух, С. Алексі. Зокрема, А. Росс визначав юридичну фікцію як усвідомлену невідповідність між юридичними положеннями та реальними фактами, що, однак, визнається необхідною для ефективного