

**Денис СУКОНЧЕНКО**

курсант 2 курсу факультету № 1  
Криворізького навчально-наукового  
інституту Донецького державного  
університету внутрішніх справ

**Науковий керівник:**

**Тетяна ПАВЛИШ**

доцент кафедри спеціальних дисциплін та  
професійної підготовки факультету № 1  
Криворізького навчально-наукового  
інституту Донецького державного  
університету внутрішніх справ, кандидат  
педагогічних наук

## **РОЛЬ КІБЕРПОЛІЦІ У СУЧАСНІЙ БОРОТБІ ЗІ ЗЛОЧИННІСТЮ**

Цифрові технології стали необхідною складовою сучасного суспільства, формуючи нові можливості та виклики в усіх аспектах нашого життя. Сьогодні уявити життя без комп'ютера та різних гаджетів дуже складно. Вони дозволяють нам зберігати зв'язок з друзями та родиною, навіть на великій відстані; завдяки їм, ми можемо розважатися, дивлячись фільми, слухаючи музику або граючи в ігри, в будь-який час та в будь-якому місці; завдяки їм маємо відкритий доступ до навчання; вони роблять можливим працювати з будь-якої точки світу та сприяють розвитку глобальної економіки; вони перетворюють спосіб функціонування багатьох галузей та визначають нові професійні напрямки, а відтак впливають на соціальні норми та взаємодії.

Хоча Інтернет відкриває безліч можливостей для спілкування, але є і певні проблеми. Багато людей в Інтернеті використовують анонімність для створення віртуального образу, який може відрізнитися від їхньої реальної особистості, що призводить до великої кількості шахрайства. Зростання спілкування в Інтернеті також призводить до збільшення загроз кібербезпеці. Атаки на особисті дані, шахрайства та інші кіберзлочини можуть погіршити якість віртуального спілкування.

За таких умов, «кіберпростір широко використовується злочинцями як місце вчинення протиправних діянь і містить сліди їхньої злочинної діяльності. Необхідність посилення боротьби зі злочинністю у кіберпросторі вимагає від правоохоронних органів розробки та впровадження в практичну діяльність нових оперативно-розшукових заходів і методів, які б урахували специфіку функціонування кіберпростору» [1].

Кіберзлочинність в Україні сьогодні є однією з найбільших загроз національній безпеці в інформаційній сфері. Кіберпростір використовується для незаконної торгівлі людьми, наркотичними засобами, зброєю, розповсюдження дитячої порнографії, проведення різної екстремістської діяльності (зокрема

пропаганди насильства, жорстокості, расової, національної, релігійної нетерпимості), порушення авторських прав тощо.

Кількість злочинів, що вчиняється у кіберпросторі, зростає пропорційно кількості користувачів комп'ютерних мереж.

За оцінками Інтерполу, швидкість зростання злочинності в глобальній мережі Інтернет є найбільшою порівняно з іншими видами злочинів, зокрема торгівлею наркотиками та зброєю.

Постановою Кабінету Міністрів України у жовтні 2015 року був утворений Департамент кіберполіції, що набув статусу міжрегіонального територіального органу Національної поліції України [2]. Проте, необхідно звернути увагу, що такі терміни, як «кіберзлочинність», «кіберзагроза», «кібербезпека», отримали визначення на рівні законодавства лише у 2017 році [3], тобто через 2 роки потому. А ще через рік Департамент звітував, що його працівники протягом 2018 року взяли участь у розслідуванні понад 11 000 кримінальних проваджень [4]. Водночас, як переконує статистика, кіберзлочинність має тенденцію до зростання. Така ситуація спостерігається не лише в нашій країні але й у всьому світі.

Відповідно до законодавства України Департамент кіберполіції забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. До основних завдань департаменту належать: 1) участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; 2) сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень [9].

Кіберзлочини є різноманітними та поширеними в інтернет-середовищі. Деякі з найпоширеніших кіберзлочинів включають:

– **Фішинг:** злочинець використовує хитрі та маніпулятивні методи для отримання конфіденційної інформації, такої як паролі та номери кредитних карт.

– **Вірусні програми:** шкідливий програмний код, який може впливати на пристрої та системи, завдяки розповсюдженню через заражені файли, електронні листи або вразливості програмного забезпечення; блокування доступу до файлів чи системи, а зловмисник вимагає викуп для їхнього відновлення.

– **Кібершпигунство:** електронне шпигунство, де зловмисники або кібершпигуни використовують технології для незаконного збору конфіденційної інформації.

– **Кібератаки на корпоративні мережі:** захоплення чи порушення безпеки корпоративних мереж для отримання конфіденційної інформації, викрадання даних або завдання іншої шкоди.

– **Соціальна інженерія:** використання маніпуляцій та обману людей для отримання конфіденційної інформації чи незаконного доступу до систем.

– **Недозволенний доступ та витік даних:** отримання несанкціонованого доступу до систем чи даних, а також неправомірне використання чи розголошення цих даних.

Кіберполіція відіграє ключову роль у боротьбі з кіберзлочинністю. Її завдання включають виявлення, розслідування та запобігання кібератак, в тому числі крадіжки особистих даних, шахрайство, атаки на інфраструктуру та інші інтернет-злочини. Кіберполіція співпрацює з іншими правоохоронними органами та міжнародними агенціями, щоб ефективно боротися з транскордонною кіберзлочинністю. Застосування сучасних технологій та аналіз великих обсягів даних є важливою частиною їхньої діяльності для виявлення та припинення кіберзлочинів.

С.В. Демедюка і В.В. Маркова, зазначають, що до функцій кіберполіції відносять такі: визначає, розробляє та забезпечує реалізацію комплексу заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності; у межах своїх повноважень уживає необхідних оперативних-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності; уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень; організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності; проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті; забезпечує формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності; організовує виконання у межах компетенції доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях [7].

Проаналізувавши наукову літературу, ми дійшли висновку, що кіберполіція відіграє важливу роль у боротьбі зі злочинністю, пов'язаною з використанням технологій. Основні аспекти цієї ролі включають:

– **Превентивні заходи:** розробка та впровадження заходів з попередження кіберзлочинності; забезпечення освіти та навчання громадян, компаній і державних установ щодо кібербезпеки.

– **Виявлення та розслідування кіберзлочинів:** моніторинг інтернет-простору для виявлення потенційно небезпечних дій; проведення розслідувань у випадках кібератак, кібершахрайств і інших електронних злочинів.

- **Співпраця з іншими органами:** взаємодія з національними та міжнародними правоохоронними органами для обміну інформацією та спільного реагування на кіберзагрози.
- **Захист критичної інфраструктури:** забезпечення безпеки критичних інфраструктур, таких як енергетика, транспорт і медична сфера, від кібератак.
- **Законотворча:** активна участь у формуванні та вдосконаленні законодавства, спрямованого на протидію кіберзлочинності.
- **Технічна експертиза:** використання високотехнологічних методів для аналізу кіберзлочинів та забезпечення ефективності розслідувань.

Загалом, кіберполіція відіграє важливу роль у забезпеченні безпеки в електронному середовищі та захисті суспільства від сучасних кіберзагроз.

Все перераховане вказує, що: по-перше, держава має потребу у підготовці відповідних висококваліфікованих фахівців в сфері кібербезпеки; а по-друге, для того щоб випереджати трансформування кіберзлочинності, освітня робота з підготовки кіберполіцейських повинна віднайти та втілити найпрогресивніші засоби навчання.

Таким чином, сучасний стан суспільних відносин, що складаються в мережі «Інтернет», характеризується інтенсивним розвитком з дещо негативними наслідками та появою нових видів злочинів. У вказаних процесах особливе місце повинні зайняти заходи із протидії кіберзлочинності як новому віртуальному явищу, що завдає шкоди правам, свободам та інтересам громадян. Заходи боротьби з кіберзлочинністю повинні мати сьогодні комплексний характер та бути спрямованими на мінімізацію ризиків віртуальних загроз та на підвищення засобів і способів захисту у віртуальному просторі. У вказаних процесах кіберполіція стає центральним суб'єктом боротьби з кіберзлочинністю.

#### **Список використаних джерел**

1. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13.10.2015 № 831 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: <https://zakon.rada.gov.ua/laws/show/831-2015-п> (дата звернення: 20.11.2023).
2. Харківський національний університет внутрішніх справ, Новини від 16.10.2015 р. : «До кіберполіції наберуть 400 співробітників – Арсен Аваков (відео, інфографіка)». URL: <http://univd.edu.ua/uk/news/771> (дата звернення: 20.11.2023).
3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 20.11.2023).
4. Підсумки 2018 року в цифрах // Кіберполіція України : офіц. сайт. URL: <https://cyberpolice.gov.ua/results/2018> (дата звернення: 20.11.2023).
5. Всесвітнє дослідження економічних злочинів та шахрайства 2018 року: результати опитування українських організацій // PWS: сайт. URL: <https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf> (дата звернення: 20.11.2023).