УДК 343.9:004.056
DOI https://doi.org/10.32782/apdp.v106.2025.21

І. І. Татарин, М. М. Яремчук, Ю. О. Літвінова

МЕТОДИ ПОПЕРЕДЖЕННЯ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УМОВАХ СУЧАСНОСТІ

Постановка проблеми. У сучасному світі, що характеризується стрімким розвитком інформаційних технологій, кіберзлочинність стала однією з найбільших загроз для безпеки держав, підприємств та окремих осіб. Зростання кількості кіберінцидентів, таких як крадіжка особистих даних, фінансові шахрайства, атаки на інфраструктуру та розповсюдження шкідливого програмного забезпечення, вимагає термінового реагування з боку правоохоронних органів та суспільства в цілому. Для ефективного розслідування потрібно аналізувати сучасні методи попередження та протидії кіберзлочинності, виявляти їхні недоліки і переваги, а також розробляти рекомендації щодо вдосконалення цих методів з урахуванням нових викликів у сфері кібербезпеки.

Аналіз останніх досліджень і публікацій. Питання пов`язані з попередженням та протидією кіберзлочинністю у своїх статтях досліджували В. Батигареєва, В. Болгов, Н. Гадіон, О. Гладун, С. Демедюк, Т. Демедюк, А. Лавник, М. Сащенко та інші. На дисертаційному рівні взаємодію правоохоронних органів, зокрема проблеми міжнародного співробітництва, що виникають під час розслідування кіберзлочинів, досліджував І. І. Васильковський. Проте, недостатньо уваги приділяється особливостям взаємодії правоохоронних органів різних країн під час збору електронних доказів у справах про злочини, що стосується теми методів попередження та протидії кіберзлочинності в сучасних умовах.

Метою статті є огляд і аналіз методів, які використовуються для запобігання кіберзлочинності, а також для боротьби з нею в сучасному цифровому світі.

Виклад основного матеріалу. В умовах інформаційної війни під час діючої військової агресії з боку росії, найбільш вразливі до кібератак є державні установи, великі корпорації, оборонні підприємства та підприємства критичної інфраструктури, а також компанії, які забезпечують все необхідне для населення та оборони у воєнний час [9, с. 17].

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [1].

Нормативно-правове підґрунтя для боротьби з кіберзлочинністю в Україні становлять: Конституція України, Кримінальний кодекс України, Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», Конвенція Ради Європи про кіберзлочинність [11, с. 203].

Після повномасштабного вторгнення росії на територію України кількість кримінальних правопорушень у сфері інформаційних технологій різко збільшилась, а відповідно виникла необхідність удосконалення досудового розслідування по таких кримінальних провадженнях. Країна-агресор використовує інтернет-технології задля дезінформації щодо вторгнення в Україну, пропаганди ворожих ідей тощо. У зв'язку з цим, Верховна Рада України здійснила оптимізацію кримінального та кримінального процесуального законодавства, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності злочинців. Так, було внесено зміни до відповідних законів: «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» з питання підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15 березня 2022 року та «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24 березня 2022 року [2; 3].

Кіберзлочинність є транснаціональною за своєю природою, а тому, факторами, що сприяють затримці кіберзлочинності, є:

1) складність і масштабність механізмів кіберзлочинності та широкий спектр наслідків, а також «комп'ютерна неграмотність» багатьох потенційних жертв кіберзлочинності та нехтування питаннями безпеки;

2) негативна поведінка жертв (свідків) злочинів – потерпілі або особи, які володіють інформацією про злочин, не повідомляють про правопорушення або про вчинення кіберзлочину правоохоронним органам;

3) існують недоліки в роботі правоохоронних органів щодо реагування на заяви або повідомлення про кіберзлочини [9, с. 16].

Основними заходами щодо запобігання кіберзлочинності, які здійснюються Національною поліцією (в особі Департаменту кіберполіції), є розробка та затвердження Міністерством внутрішніх справ стратегії боротьби з кіберзлочинністю. Ця стратегія має включати концепцію діяльності із запобігання злочинам, стратегічні з точки зору науки та тактичні заходи запобігання злочинам, а також механізм моніторингу їхньої якості. Збільшити кількість регулярних та нерегулярних перевірок відповідними органами поліції компаній, діяльність яких безпосередньо пов'язана з кіберзлочинністю [9, с. 17].

Методів попередження кіберзлочинності є безліч та всі вони як схожі за своєю природою, так і різняться в залежності від ситуації та обставин. За допомогою накопичення та використання набутих знань у взаємодії з міжнародними партнерами, України йде у вірному напрямку щодо зменшення рівня небезпеки, спричиненої кіберзлочинністю.

Необхідно зазначити, що активно розвивається і співпраця з іноземними партнерами, поглиблюється співробітництво України з ЄС та НАТО, проводяться кібернавчання за участю інших держав та міжнародних організацій. Так, наприклад, протягом останніх років правоохоронними органами України, США, Великої Британії, Японії, Філіппін, Індонезії, Малайзії було проведено такі операції:

– «секс Торшн», внаслідок якої затримано 56 осіб, ліквідовано 4 транснаціональні кримінальні угрупування;

– «Зевс», завданням якої було знешкодження міжнародної організованої злочинної групи, котра з метою викрадення фінансових реквізитів і доступу до банківських рахунків розповсюджувала шкідливе програмне забезпечення «Зевс».

Під час операції знешкоджено інфраструктуру в мережі, що включала понад 40 тис. інфікованих комп'ютерів і серверів, левова частка яких знаходилась на території України. Спричинені збитки понад 300 млн доларів. Члени організованого злочинного угруповання – хакери з Одеси та Харкова на чолі з громадянином російської федерації [5, с. 68].

Боротьба з кібершахрайством в Україні реалізується в трьох основних напрямках діяльності:

1) попередження кіберзлочинів;

2) загальна організація боротьби з кіберзлочинністю та правоохоронна діяльність, спрямована саме на виявлення, запобігання та розкриття кіберзлочинів;

3) застосування заходів кримінальної відповідальності і покарання осіб, які вчинили кіберзлочини [7, с. 549].

Попередження як одна з форм боротьби зі злочинністю передбачає як загальнодержавні заходи економічного, ідеологічного, правового та виховного характеру, так і спеціальні організаційні, технічні, програмні та криптографічні. В Україні діє багато платформ для інформування громадян щодо шахрайських схем та засобів, як не стати жертвою кібершахрайства. На спеціальному ресурсі пояснюють правила кібербезпеки й надають поради українцям, як надійніше захистити свої гроші. У межах кампанії Національний банк разом із партнерами інформуватимуть громадян про те, як вберегтися від платіжного шахрайства, зокрема через оновлену тематичну вебсторінку (лендинг) #ШахрайГудбай із детальною інформацією про кампанію та правила поведінки у віртуальному просторі [7, с. 549].

Необхідність у посиленні кримінальної відповідальності за кримінальні правопорушення у сфері інформаційних технологій назріла давно. Зміни до законодавства стосуються збільшення повноважень правоохоронних органів щодо розслідування кіберзлочинів, передбачених статями 361, 361-1 КК України. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових кримінальних правопорушень. Важливим є запровадження відповідальності за вищевказані кримінальні правопорушення, вчинені під час воєнного стану.

Суворі санкції за такі протиправні діяння зумовлена ситуацією в країні, адже особа, яка завдає шкоди національним інтересам України у кіберпросторі, тим самим допомагаючи агресору у цій війні, не може нести відповідальності меншої, ніж військові злочинці.

О. М. Бодунова наголошує, що задля побудови ефективної системи запобігання злочинності у сфері інформаційних технологій доцільно не лише посилювати відповідальність за вчинені кримінальні правопорушення, а й розробити соціально-економічні, організаційно-управлінські та морально-психологічні напрями,

спрямовані на нейтралізацію чинників, що зумовлюють вчинення кримінальних правопорушень [4, с. 86].

Авторка зазначає про доцільність розробки заходів запобігання кібершахрайству, які може реалізувати кожен орган державної влади, місцевого самоврядування, приватні підприємства або ж окремі особи. До таких віднесено:

1) до діяльності органів державної влади, приватних підприємств обов'язково залучати технічного спеціаліста або спеціалізованої компанії, що суттєво підвищить рівень кібербезпеки;

2) особам, які перебувають в зоні кіберризику, варто слідкувати за відповідними повідомленнями на офіційних ресурсах Держспецзв'язку та CERT-UA, адже органи публікують офіційні попередження не лише про можливі кіберзагрози, а й про те, як мінімізувати ризики;

3) якщо особа стала жертвою кібератаки, потрібно повідомити про це тих, на кого така атака може поширитися – інші співробітники, клієнти та контрагенти або ж родичі чи друзі;

4) у разі кібератаки потрібно обов'язково інформувати офіційні суб'єкти забезпечення кібербезпеки України, CERT-UA та кіберполіцію [4, с. 86].

Автор Д. Є. Денищук пропонує наступні введення у освіту кадрів МВС для забезпечення якісного розслідування кіберзлочинів:

– для тенденції розвитку юридичної освіти є необхідність спрямування до європейських стандартів, та потреба розумно використовувати напрацювання моделі відомчої освіти МВС;

– з необхідністю підвищення якості освіти майбутніх кіберполіцейських, необхідно збільшити роль практичної складової підготовки у навчальному процесі;

– для забезпечення якісної освіти кіберполіцейських треба сформувати ґрунтовну наукову базу у вигляді відповідних структурних підрозділів, колективу науково-педагогічних працівників та матеріально-технічної бази;

– для підвищення якості навчальної підготовки треба розбудовувати систему зв'язків із органами, організаціями, установами та об'єднаннями різних форм власності, вітчизняними, іноземними і міжнародними [6, с. 233].

В час війни виникли нові, безпосередньо зумовлені війною, корисливі кіберзлочини, що виявлено Кіберполіцією України останнім часом: псевдо благодійність, пропозиції з оренди неіснуючого житла, фейкові пасажирські перевезення, продаж неіснуючих товарів, зокрема й військової амуніції, шахрайства під виглядом організації переправлення через державний кордон чоловіків призовного віку, шахрайства під приводом надання інформації щодо безвісно зниклих громадян. Стрімке зростання кількості корисливих кіберзлочинів обумовило додаткове навантаження на кіберполіцію України, саме у той час, коли Україні потребується підсилити боротьбу з кіберзлочинами, що є продовженням гібридної війни рф проти України, у той час, коли все більше офіцерів потрібно для безпосередньої участі у бойових діях. Через це проводити реструктуризацію кіберполіції та збільшувати могутність підрозділів, що відповідають за боротьбу з корисливою кіберзлочинністю навряд чи можливо і тому недоцільно [12, с. 213].

Прикладом застережень кіберполіції щодо убезпечення від можливості стати жертвою кіберзлочинності є наступні:

– застереження від замовлення документів, що нібито дозволять перетнути кордон чоловікам у віці 18–60 років. Окрім ризику потрапити на гачок шахраїв, замовникам фейкових документів загрожує кримінальна відповідальність.

– злочинці поширюють серед громадян України повідомлення зі шкідливим посиланням на нібито вебсайт Telegram, щоб отримати несанкціонований доступ до облікових записів, у тому числі і з можливістю перехоплення одноразового коду з SMS. В результаті подібних атак зловмисники викрадають дані сесії, список контактів та історії листування в Telegram [8].

Задля вирішення глобальних викликів з боку рф, найбільш пріоритетний партнер – США, за результатами кібердіалогів надає Україні фінансування на розвиток проектів з посилення кібербезпек, а також для підготовки кіберфахівців [9, с. 42].

Глобальна кібербезпека мусить спрямовувати зусилля на захист та безпеку мережі з використанням наступних рівнів захисту інформації:

1) попередження – вхід в базу даних та технологій надається лише уповноваженому персоналу з відповідними спеціальними навичками;

2) ииявлення – забезпечити раннє виявлення злочинів та зловживань, навіть якщо існують механізми захисту;

3) стримування – зменшує розмір збитків, якщо правопорушення вчиняються, не дивлячись на запобігання та виявлення;

4) відновлення – забезпечує суттєво нові дані за наявності задокументованого та протестованого плану відновлення [10].

Висновки. Отже, ефективність протидії явищу кіберзлочинності вбачається у спільних діях державного і приватного секторів, вдосконаленні міжнародно-правових інструментів та національного законодавства (удосконалення процесу збору, аналізу та використання цифрових доказів; розробка чіткого механізму для легалізації процедури вилучення цифрових доказів, зокрема з міжнародних серверів), організації інституційного механізму боротьби з кіберзлочинами.

Задля побудови ефективної системи запобігання злочинності у сфері інформаційних технологій доцільно не лише посилювати відповідальність за вчинені кримінальні правопорушення, а й розробити соціально-економічні, організаційно-управлінські та морально-психологічні напрями, спрямовані на нейтралізацію чинників, що зумовлюють вчинення кримінальних правопорушень.

Література

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

3. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 берез. 2022 року № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

4. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського університету: серія: Право* / голов. ред. Ю. М. Бисага. Ужгород: Видавничий дім «Гельветика», 2023. Т. 2. Вип. 75. С. 83–87. Бібліогр.: с. 86–87.

5. Демедюк С. В., Демедюк Т.С. Міжнародний досвід протидії кіберзлочинності. *Вісник ХНУВС*. 2014. № 4 (67). С. 65–75.

6. Денищук Д. Є. Особливості підготовки поліцейських кіберполіції в умовах сьогодення на прикладі Харківського національного університету внутрішніх справ. Підготовка поліцейських в умовах реформування системи МВС України. Харків, 2020. С. 233–237.

7. Діброва Т. А. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 11. С. 546–549.

8. Кіберполіція попереджає про атаки, спрямовані на отримання доступу до облікових записів українців у Телеграмі. *Interfax-Україна*. URL: https://interfax.com.ua/news/telecom/821387.HTML

9. Лавник А. М. Державна політика протидії кіберзлочинності в умовах інформаційної війни рф проти України. Національний авіаційний університет. 2023. 55 с.

10. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. Київ : КНТ, 2020. 280 с.

11. Никончук Н. С. Кіберзлочинність в Україні: виклики сучасності. *Юридичний науковий електронний журнал*. 2021. № 9. С. 202–205.

12. Пядишев В. Г. Національна поліція України у боротьбі з корисливими кіберзлочинами, що поширилися або виникли під час аргесії рф. *Наукові проблеми запровадження правового режиму воєнного стану в Україні: сучасний вимір* : матеріали науково-практичного онлайн-заходу. 29 квітня 2022 р. Одеса: ОДУВС, 2022. С. 212–213.

Анотація

Татарин І. І., Яремчук М. М., Літвінова Ю. О. **Методи попередження та протидії кіберзлочинності в умовах сучасності.** – Стаття.

У статті розглядається актуальна проблема кіберзлочинності, яка стала однією з найзначніших загроз для безпеки держав, приватного бізнесу та громадян у сучасному світі, де інформаційні технології розвиваються стрімкими темпами. Звернуто увагу на стрімкому зростанні кількості каберзлочинів, таких як крадіжка особистих даних, фінансові шахрайства, атаки на критичну інфраструктуру та поширення шкідливого програмного забезпечення. У зв'язку з цим виникає необхідність у постійному вдосконаленні методів боротьби з кіберзлочинністю. Для досягнення цієї мети необхідно аналізувати сучасні методи протидії кіберзлочинності, виявляти їхні недоліки та переваги, а також розробляти рекомендації щодо їхнього покращення, враховуючи нові виклики у сфері кібербезпеки.

Окремо розглянуто нормативно-правову базу України для боротьби з кіберзлочинністю, яка включає Конституцію України, Кримінальний кодекс, Закони «Про основні засади забезпечення кібербезпеки України», «Про інформацію» та інші важливі акти, а також міжнародні документи, такі як Конвенція Ради Європи про кіберзлочинність. Після початку повномасштабної військової агресії росії кількість кіберзлочинів значно зросла, що призвело до оновлення та вдосконалення кримінального законодавства України.

У статті також досліджено роль державних органів, зокрема Національної поліції та Департаменту кіберполіції, у розробці та впровадженні стратегії боротьби з кіберзлочинністю. Описано сучасні методи запобігання кіберзлочинності, які включають організаційні, технічні, правові та криптографічні заходи. Наголошується на важливості взаємодії правоохоронних органів різних країн під час збору електронних доказів, а також необхідності регулярних перевірок компаній, що працюють у кіберпросторі.

Особливу увагу приділено міжнародній співпраці України з іншими державами та організаціями, у сфері кібербезпеки. Описані конкретні операції, проведені спільно з правоохоронними органами інших країн для нейтралізації транснаціональних злочинних угруповань. У статті робиться висновок про необхідність продовження активної міжнародної співпраці, вдосконалення національного законодавства та підвищення рівня освіти фахівців у сфері кіберзахисту для забезпечення ефективної боротьби з кіберзлочинністю в умовах сучасних викликів.

Ключові слова: злочинні угрупування, кібербезпека, взаємодія, розслідування, кримінальне правопорушення, електронні докази, доказування, правоохоронні органи, попередження кримінальних правопорушень, протидія.

Summary

Tataryn I. I., Yaremchuk M. M., Litvinova Yu. O. **Methods of preventing and countering cybercrime in modern conditions.** – Article.

The article examines the current problem of cybercrime, which has become one of the most significant threats to the security of states, private businesses and citizens in the modern world, where information technologies are developing at a rapid pace. Attention has been drawn to the rapid growth of cybercrimes such as identity theft, financial fraud, attacks on critical infrastructure and the spread of malware. In this connection, there is a need for constant improvement of methods of combating cybercrime. To achieve this goal, it is necessary to analyze modern methods of combating cybercrime, identify their shortcomings and advantages, as well as develop recommendations for their improvement, taking into account new challenges in the field of cyber security.

The regulatory and legal framework of Ukraine for combating cybercrime, which includes the Constitution of Ukraine, the Criminal Code, the Laws "On the Basic Principles of Ensuring Cybersecurity of Ukraine", "On Information" and other important acts, as well as international documents such as the Council of Europe Convention on cybercrime. After the beginning of the full-scale military aggression of Russia, the number of cybercrimes increased significantly, which led to the renewal and improvement of the criminal legislation of Ukraine.

The article also explores the role of government agencies, including the National Police and the Cyber Police Department, in the development and implementation of cybercrime strategies. Modern methods of cybercrime prevention are described, which include organizational, technical, legal and cryptographic measures. It emphasizes the importance of cooperation between law enforcement agencies of different countries during the collection of electronic evidence, as well as the need for regular inspections of companies operating in cyberspace.

Special attention is paid to the international cooperation of Ukraine with other states and organizations in the field of cyber security. Specific operations conducted jointly with law enforcement agencies of other countries to neutralize transnational criminal groups are described. The article concludes on the need to continue active international cooperation, improve national legislation and raise the level of education of specialists in the field of cyber protection in order to ensure the effective fight against cybercrime in the conditions of modern challenges.

Key words: criminal groups, cybersecurity, interaction, investigation, criminal offense, electronic evidence, proving, law enforcement agencies, prevention of criminal offenses, counteraction.