DOI: https://doi.org/10.32844/ibpala-2025-2.02
УДК 343.9:004.738.5(73)

ЗАРУБІЖНИЙ ДОСВІД ДІЯЛЬНОСТІ ОРГАНІВ ПОЛІЦІЇ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ (НА ПРИКЛАДІ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ)

Білобров Тетяна Віталіївна,
кандидат юридичних наук,
старший науковий співробітник
Науково-дослідного інституту публічного права
tvtkach@outlook.com
ORCID ID: https://orcid.org/0009-0009-4439-4404

В умовах удосконалення діяльності органів державної влади, особливого значення набуває дослідження позитивного зарубіжного досвіду діяльності органів державної влади, діяльність яких спрямована на забезпечення кібербезпеки держави та протидії кіберзлочинності. Одним із таких суб'єктів є органи та підрозділи поліції, що виступають суб'єктом забезпечення як внутрішньої складової безпеки держави так й зовнішнього блоку національної безпеки держави. У цій праці ми розглянемо досвід США у досліджуваній сфері, оскільки саме ця країна стала однією з перших, яка на національному рівні визначила та прийняла низку законів та нормативно-правових актів у сфері протидії кіберзлочинності та забезпечення кібербезпеки держави. Причинами такого оперативного затвердження концепцій та стратегій протидії інформаційним злочинам та кібератакам стали події 11 вересня 2001 року, коли було скоєно серію терактів, членами терористичної організації «Аль-Каїда». Встановлено, що ФБР є провідним федеральним агентством США з розслідування кібератак, що вчиняються злочинцями, зарубіжними противниками і терористами. Оскільки кібервторгнення стають все більш поширеним явищем, сьогодні діяльність ФБР постійно удосконалюється, щоб краще протистояти терористичній загрозі після терактів 11 вересня 2001 року. Поряд із цим, одним із пріоритетних напрямків протидії кіберзлочинності в США є протидія торгівлі людьми, що здійснюється із застосуванням інформаційних технологій у віртуальному просторі та завдає шкоди охоронюваним законом правам та основоположним свободам людини й громадянина. Визначено, що в США з метою ефективної боротьби з кіберзлочинністю та забезпечення кібербезпеки держави, створено належне правове поле діяльності спеціалізованих суб'єктів боротьби з кіберзлочинністю та створено дієву систему органів, основними функціями визначено забезпечення кіберзахисту та протидії всім проявам кіберзлочинності, що беззаперечно суттєво впливає на стан правопорядку в державі.

Ключові слова: *зарубіжний досвід, кіберзлочинність, кібербезпека, кіберполіція, ФБР, Сполучені Штати Америки.*

Рекомендоване посилання:
Білобров Т. В. Зарубіжний досвід діяльності органів поліції у сфері протидії кіберзлочинам (на прикладі Сполучених Штатів Америки). *International Bulletin on Public Administration and Legal Affairs*. 2025. № 2. С. 13–20. DOI:

FOREIGN EXPERIENCE OF POLICE ACTIVITIES IN COMBATING CYBERCRIME (ON THE EXAMPLE OF THE UNITED STATES OF AMERICA)

Bilobrov Tetiana Vitaliivna,
PhD in Law,
Senior Researcher
Research Institute of Public Law
tvtkach@outlook.com
ORCID ID: https://orcid.org/0009-0009-4439-4404

In the context of improving the activities of public authorities, it is of particular importance to study the positive foreign experience of public authorities whose activities are aimed at ensuring the cybersecurity of the State and countering cybercrime. One of these entities is the police, which are responsible for ensuring both the internal component of the state's security and the external component of the state's national security. In this paper, we will consider the experience of the United States in this area, since this country was one of the first to define and adopt a number of laws and regulations at the national level in the field of combating cybercrime and ensuring the cybersecurity of the state. The reasons for such prompt approval of concepts and strategies for countering information crimes and cyberattacks were the events of September 11, 2001, when a series of terrorist attacks were committed by members of the al-Qaeda terrorist organization. The FBI is the leading U. S. federal agency for investigating cyberattacks committed by criminals, foreign adversaries and terrorists. As cyber intrusions are becoming more and more common, the FBI's activities are constantly being improved to better counter the terrorist threat after the September 11, 2001 terrorist attacks. At the same time, one of the priority areas of combating cybercrime in the United States is combating human trafficking, which is carried out with the use of information technology in the virtual space and harms the rights and fundamental freedoms of man and citizen protected by law. It is determined that in order to effectively combat cybercrime and ensure the cybersecurity of the State, the United States has created an appropriate legal framework for the activities of specialized entities fighting cybercrime and established an effective system of bodies, the main functions of which are to ensure cyber defense and counteract all manifestations of cybercrime, which undoubtedly significantly affects the state of law and order in the State.

Keywords: *foreign experience, cybercrime, cybersecurity, cyberpolice, FBI, UnitedStates of America.*

Вступ

Сьогодні, в умовах удосконалення діяльності органів державної влади, особливого значення набуває дослідження позитивного зарубіжного досвіду діяльності органів державної влади, діяльність яких спрямована на забезпечення кібербезпеки держави та протидії кіберзлочинності. Одним із таких суб'єктів є органи та підрозділи поліції, що виступають суб'єктом забезпечення як внутрішньої складової безпеки держави так й зовнішнього блоку національної безпеки держави. При цьому, окрему увагу слід приділити тим державам, які першими стали на шлях побудови національного законодавства у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності. Такими державами є країни Європейського Союзу та Сполучених Штатів Америки, а також країни пост-радянського простору (Латвія, Литва. Естонія та деякі інші).

Мета статті

Таким чином, аналіз діяльності органів поліції зазначених держав та їх національного законодавства є на сьогодні вельми актуальним та своєчасним в умовах удосконалення адміністративно-правового статусу Департаменту кіберполіції Національної поліції України, що й обумовлює мету нашого дослідження. З огляду на обмеження щодо розміру статті, у цій праці ми розглянемо досвід США у досліджуваній сфері, оскільки саме ця країна стала однією з перших, яка на національному рівні визначила та прийняла низку законів та нормативно-правових актів у сфері протидії кіберзлочинності та забезпечення кібербезпеки держави.

Аналіз останніх досліджень та публікацій

Питання забезпечення кібербезпеки та протидії кіберзлочинності неодноразово ставали предметом наукових дискусій та досліджень. Так, зазначена проблематика знайшла своє відображення у працях таких вітчизняних вчених та науковців як: О. М. Бандурка, В. В. Василевич, І. В. Діордіца, О. Ю. Дрозд, Т. О. Коломоєць, В. А. Ліпкан, О. П. Орлюк, В. В. Сокуренко, В. В. Чернєй та інші. У той же час, наразі недостатньо уваги приділено діяльності спеціалізованих державних в тому числі міжнародних органів та організацій у сфері протидії кіберзлочинності як сучасного виду злочинності в Україні та за кордоном. У зв'язку з чим наразі активізуються питання щодо дослідження зарубіжного

та міжнародного досвіду діяльності органів, уповноважених на вжиття заходів з протидії кіберзлочинності та забезпечення кібербезпеки держави.

Виклад основного матеріалу

Сьогодні у багатьох зарубіжних країнах налагоджена система співробітництва, що обумовлюється необхідністю обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: Сполучені Штати Америки та більшість країн-учасниць Європейського Союзу у своїх стратегіях виносять питання боротьби з кіберзлочинністю на передові позиції (Петровський & Лівчук, 2019). Відповідно наразі слушним є дослідження досвіду тих держав, котрі першими запровадили політику забезпечення кібербезпеки держави та протидії злочинності.

Насамперед, вбачаємо цілком слушним розпочати дослідження успішного (позитивного) зарубіжного досвіду діяльності органів поліції у сфері протидії кіберзлочинності такої потужної держави як Сполучені Штати Америки (далі – США). Оскільки саме вказана держава стала однією з перших, хто визначив на національному рівні визначила та прийняла низку законів та нормативно-правових актів у сфері протидії кіберзлочинності та забезпечення кібербезпеки держави. Причинами такого оперативного затвердження концепцій та стратегій протидії інформаційним злочинам та кібератакам стали події 11 вересня 2001 року, коли було скоєно серію терактів, членами терористичної організації «Аль-Каїда».

Першочергово зазначимо, що в США відсутнє єдине поліцейське управління, оскільки у кожному штаті діють свої закони та функціонують органи, діяльність яких може відрізнятися від функціонування аналогічних органів інших штатів. Так, Департамент кіберполіції Нью-Йорку, що створений у 1845 році, є одним із найбільших підрозділів муніципальної поліції США.

Структурно Департамент поліції штату Нью-Йорк складається із бюро та офісів, серед яких: Бюро патрульної служби, Бюро спеціальних операцій, Транзитне бюро, Бюро по боротьбі з тероризмом, Бюро по боротьбі зі злочинністю, Бюро детективів та інші.

Окрему увагу слід приділити функціонуванню Бюро по боротьбі з тероризмом (NYPD, 2025), оскільки його діяльність спрямована на захист штату від внутрішніх та міжнародних (зовнішніх) загроз терористичного характеру, а тому числі кіберзагроз. На території штату діє так звана «Команда критичного реагування», що здійснює: прогноз можливих кіберзагроз та загроз тероризму; здійснює розробку новаторською та довгострокової політики та механізмів захисту від кібератака, інформаційних та комп'ютерних злочинів; готує до оперативного втручання служби первинного реагування та спеціальні підрозділи; а також, нарощує потенціал розвідувальних спроможностей для виявлення та протидії кібератакам та терористичним загрозам. При цьому, слід вказати, що діяльність Команди критичного реагування здійснюється у відповідності з національним та федеральним законодавством, а її функціонування координується федеральними, штатними та іншими правоохоронними органами з метою збору оперативної інформації щодо кібератак та загроз тероризму.

Команда критичного реагування Бюро по боротьбі з тероризмом є однією з перших груп оперативного реагування та захисту Департаменту поліції Нью-Йорка та штату від терористичних атак та кіберзагроз. Співробітники Команди критичного реагування, пройшовши відповідну спеціальну підготовку, мають навички володіння спеціальними видами зброї, в тому числі, великої дальності, виявлення слідів вибухових речовин, радіологічного та ядерного опромінення, обізнані про біологічну та хімічну зброю та оснащені технікою для виявлення кібератак. Команда критичного реагування Бюро по боротьбі з тероризмом з метою постійної готовності до нових кіберзагроз та загроз тероризму, проводить щоденні контр терористичні розгортання на критично важливих об'єктах інфраструктури по всьому штату Нью-Йорк.

Загалом, Бюро по боротьбі з тероризмом (NYPD, 2025), має наступні повноваження:

1) розробка та реалізація великомасштабних контр терористичних проектів, та проектів протидії кіберзлочинності як: «Ініціатива з безпеки Нижнього Манхеттена», "Операція Sentinel";

2) розробка і впровадження навчальних курсів по боротьбі з тероризмом, кібератаками включаючи курси для інших правоохоронних органів і організацій;

3) моніторинг сучасного стану кіберзагроз, визначення критично важливих об'єктів інфраструктури;

4) розробка стратегій захисту для приватного сектору;

5) дослідження та випробування нових інформаційних та комп'ютерних технологій, що використовуються для виявлення і боротьби з хімічною, біологічною, радіологічною, ядерною і вибуховою зброєю, а також для виявлення та боротьби із різними видами кіберзлочинності;

6) розробка планів і політики використання інформаційних та комп'ютерних технологій;

7) розробка систем і програм для підвищення безпеки на території порту; використання системи визначення характеристик тактичного радіологічного збору даних (TRACS) для про активного розгортання і картування фонового випромінювання в порту Нью-Йорк / Нью-Джерсі;

8) здійснення заходів управлінського державно-приватного партнерства в області безпеки штату, навчання та інформування для приватного сектора і вирішення проблем, пов'язаних з приватним сектором у сфері кіберзлочинності та протидії тероризму та деякі інші.

Також, слід зазначити, що окрім Команди критичного реагування Бюро по боротьбі з тероризмом, з метою протидії кіберзлочинності та тероризму в Бюро по боротьбі з тероризмом функціонують також такі групи: Об'єднана оперативна група з питань тероризму та кіберзлочинності; група забезпечення кібербезпеки Нижнього Манхеттена; та група з аналізу ризиків та загроз тероризму та кіберзлочинності. Кожна із зазначених груп виконує ряд своїх завдань та функцій, що в кінцевому підсумку спрямовані на вжиття заходів з протидії кіберзлочинності та тероризму.

Зокрема, Об'єднана оперативна група з питань тероризму та кіберзлочинності розслідує факти кіберзлочинності та тероризму, що вчиненні на території штату Нью-Йорк, а також здійснюють систематизацію вчинених злочинів та їх аналіз.

Група забезпечення кібербезпеки Нижнього Манхеттена призначена виявляти та попереджувати загрози кібератак та тероризму на території Нижнього Манхеттена.

Група з аналізу ризиків та загроз тероризму та кіберзлочинності здійснює заходи стратегічної розвідки щодо виявлення кібератак та загроз тероризму та веде їх аналіз.

Таким чином, при Департаменті поліції Нью-Йорка функціонує ряд поліцейських підрозділів, що здійснюють завдання протидії кіберзлочинності та тероризму.

В той же час, належний рівень функціонування поліцейських органів, що здійснюють заходи боротьби з кіберзлочинністю залежить від належного рівня їх нормативно-правового регулювання, що в США складає досить потужну базу для ефективної реалізації національної політики забезпечення кібебезпеки держави.

Так, на державному рівні в США прийняті такі важливі програмні документи, що створюють фундамент для боротьби з кіберзлочинністю, як: Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі» (2011); Кіберстратегія Міністерства оборони від квітня 2015 року; Міжвідомчий план дій з кібербезпеки систем управління (Cross-Sector Roadmap for Cybersecurity of Control Systems); План дій з посилення кібербезпеки найважливіших об'єктів інфраструктури (Roadmap for Improving Critical Infrastructure Cybersecurity, 2014); План дій з забезпечення кібербезпеки систем енергопостачання (Roadmap to Achieve Energy Delivery Systems Cybersecurity) (Петровський & Лівчук, 2019). У 2016 році були прийняті Національний план з протидії кіберзлочинності та Директива-41 Президентської політики (PPD-41) (Лапта, 2017).

Зазначена нормативно-правова база заклала потужний фундамент для успішного виконання спеціалізованими суб'єктами своїх повноважень у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності.

Взявши до уваги позитивний досвід США, слід наголосити, що Україною, зокрема, Міністерством внутрішніх справ України та США, у напрямку протидії кіберзлочинності сьогодні здійснено ряд заходів. Зокрема, у січні 2020 року Міністр внутрішніх справ України та заступник держсекретаря США ДжорганЕндрюс обговорили спільні напрями взаємодії щодо протидії наркозлочинності та кіберзлочинам (УНН, 2020). При цьому, особлива увага приділяється функціонуванню такого органу в США є Федеральне бюро розслідувань (далі – ФБР), що головним суб'єктом забезпечення кібербезпеки держави та протидії кіберзлочинності на всій території США.

ФБР є провідним федеральним агентством США з розслідування кібератак, що вчиняються злочинцями, зарубіжними противниками і терористами. Оскільки кібервторгнення стають все більш поширеним явищем, сьогодні діяльність ФБР постійно удосконалюється, щоб краще протистояти терористичній загрозі після терактів 11 вересня 2001 року. Поряд із цим, одним із пріоритетних напрямків протидії кіберзлочинності є протидія торгівлі людьми, що здійснюється із застосуванням інформаційних технологій у віртуальному просторі та завдає шкоди охоронюваним законом правам та основоположним свободам людини й громадянина (Чумак, 2017).

З метою забезпечення кібербезпеки держави т протидії всім формам кіберзлочинності, в ФБР створені:

− кібервідділ в штаб-квартирі ФБР для скоординованої і узгодженої боротьби з кіберзлочинністю;

− спеціально навчені кібердружини в штаб-квартирі ФБР і в кожному з офісів на місцях, де працюють з агентами і аналітиками, які захищають від і розслідування комп'ютерних вторгнень, крадіжки інтелектуальної власності та особистої інформації, дитячої порнографії та експлуатації, а також онлайн -шахрайства;

− нові групи по кібердіям, які в будь-який момент подорожують по всьому світу, щоб допомогти у випадках комп'ютерного вторгнення з метою збору життєво важливих відомостей, що допомагають виявляти кіберзлочини, що є найбільш небезпечними для національної безпеки і для економіки;

− цільові групи з комп'ютерних злочинів, які поєднують в собі найсучасніші технології і ресурси федеральних, штатних і місцевих колег.

Реалізуючи програму по боротьбі з кіберзлочинністю, ФБР тісно співпрацює з Міністерством оборони та Міністерством національної безпеки, що часто вирішують схожі задачі. Для найбільш оперативного отримання інформації щодо вчинених комп'ютерних злочинів, у рамках ФБР створено Центр з прийому заяв стосовно вчинених інтернет-злочинів (Inernet Crime Complaint Center), де як потерпілі, так і треті особи, заповнивши спеціальну форму онлайн або просто зателефонувавши, можуть надати інформацію стосовно вчинених злочинів у мережі Інтернет (2025).

Також, при ФБР створено інтернет-центр скарг на кіберзлочини, місією якого є розгляд скарг на злочин в Інтернеті, надання громадськості надійний і зручний механізм звітності про підозрюваних, схеми шахрайства з використанням Інтернету і створення ефективних альянсів з правоохоронними органами та галузевими партнерами. Інформація аналізується і поширюється в слідчих і розвідувальних цілях серед співробітників правоохоронних органів і для інформування громадськості (2025).

Кожен громадянина США має право подати скаргу до інтернет-центру скаргу на кіберзлочини, при цьому він має вказати наступні інформацію:

- ім'я жертви, адресу, телефон і адресу електронної пошти;
- інформацію про фінансові транзакції (наприклад, інформація про рахунок, дата і сума транзакції, хто отримав грошові кошти);
- ім'ясуб'єкта, адреса, телефон, адреса електронної пошти, вебсайт і IP-адреса;
- конкретні деталі того, як ви стали жертвою;
- обов'язково вказується тема електронної пошти
- будь-яка інша важлива інформація, яку ви вважаєте необхідною для підтримки вашої скарги.

Також на офіційному сайті інтернет-центру скарг на кіберзлочини, міститься розділ, що визначає поради по попередженню злочинності в мережі Інтернет. Так, розділ містить наступні теми:

- «Шахрайство на аукціоні»;
- «Фальшивий касовий чек»;
- «Шахрайство з кредитними картами»;
- «Ліквідація заборгованості»;
- «UPS DHL»;
- «Можливості працевлаштування / бізнесу»;
- Ескроу-Сервіс Шахрайство»;
- «Крадіжка особистих даних»;
- «Інтернет-вимагання»;
- «Інвестиційне шахрайство»;
- «Кібербулінг»;
- «Фішинг»;
- «Спам»;
- «Сторонній одержувач коштів» та деякі інші (Internet Crime Complaint Center, 2025).

Також, з метою попередження вчинення кіберзлочинності, на офіційному сайті ФБР розміщені матеріали щодо захисту своїх персональних даних у віртуальному просторі. Зокрема, також є наявна інструкція захисту свого персонального комп'ютера від різних програм та шпигунського програмного забезпечення. Така інструкція передбачає наступні кроки для користувача:

1) тримайте брандмауер включеним: брандмауер захистить ваш комп'ютер від хакерів, які можуть спробувати отримати доступ, або зламати його, видалити інформацію або навіть вкрасти паролі або іншу конфіденційну інформацію. Програмні брандмауери широко рекомендуються для окремих комп'ютерів. Програмне забезпечення попередньо упаковано в деяких операційних системах або може бути придбано для окремих комп'ютерів. Для кількох мережевих комп'ютерів апаратні маршрутизатори зазвичай забезпечують захист брандмауера;

2) встановіть або оновіть антивірусне програмне забезпечення. Антивірусне програмне забезпечення призначене для запобігання вбудовування шкідливих програм в ваш комп'ютер. Якщо він виявляє шкідливий код, такий як вірус або черв як, він знімає або видаляє його. Віруси можуть заразити комп'ютери без відома користувача. Більшість типів антивірусного програмного забезпечення можна налаштувати для автоматичного оновлення;

3) встановіть або оновіть свою технологію захисту від шпигунських програм: шпигунські програми – це те програмне забезпечення, що таємно встановлюється на ваш комп'ютер, щоб дозволити іншим вдивлятися в ваші дії на комп'ютері. Деякі шпигунські програми збирають інформацію про вас без вашої згоди або створюють небажані спливаючі вікна у вашому веб-браузері. Деякі операційні системи пропонують безкоштовний захист від програм-шпигунів, а недороге програмне забезпечення легко доступно для завантаження через Інтернет або в вашому місцевому комп'ютерному магазині. Остерігайтеся реклами в Інтернеті, що пропонує завантажуваніантишпигунські програми – в деяких випадках ці продукти можуть бути підробленими і можуть фактично містити шпигунське ПЗ або інший шкідливий код. Це схоже на покупку продуктів – магазин, де ви довіряєте;

4) підтримуйте свою операційну систему в актуальному стані: комп'ютерні операційні системи періодично оновлюються, щоб відповідати технологічним вимогам і усувати діри в безпеці. Обов'язково встановіть оновлення, щоб забезпечити новий захист вашого комп'ютера;

5) будьте уважні з тим, що ви завантажуєте: необережне завантаження вкладень електронної пошти може обійти навіть саме пильне антивірусне програмне забезпечення. Ніколи не відкривайте вкладення електронної пошти від кого-то, кого ви не знаєте, і будьте обережні з переадресацією вкладень від людей, яких ви знаєте. Вони можуть мати мимоволі просунутий шкідливий код;

6) вимкніть комп'ютер. З ростом швидкості високошвидкісного підключення до Інтернету багато хто воліє залишати свої комп'ютери ввімкненими і готовими до дії. Недоліком є те, що «завжди включений» робить комп'ютери більш сприйнятливими. Крім того, відключення комп'ютера ефективно розриває з'єднання зловмисника – будь то шпигунське ПЗ або ботнет, який використовує ресурси вашого комп'ютера для зв'язку з іншими мимовільними користувачами.

Також, новелою у американському законодавстві у сфері кібербезпеки є затвердження

програми ФБР щодо безпечного онлайн-серфінгу (FBI-SOS) – це загальнонаціональна ініціатива, покликана інформувати дітей 3–8 класів про кібернебезпеки, з якими вони стикаються в Інтернеті, і сприяти запобіганню злочинів проти дітей. Він просуває кібергроматні ідей та положення серед студентів, залучаючи їх у веселу, відповідну віку, конкурентоспроможну онлайн-програму, де вони вчаться безпечного і відповідального використання Інтернету. Програма підкреслює важливість питань кібербезпеки, таких як захист паролем, розумні звички серфінгу та захист особистої інформації. Аналогічні програми існують у Латвії (Чумак, 2015).

Зазначена програма має вигляд яскравих картинок для конкретного віку дітей з інтерактивними іграми. Кожна гра передбачає проходження по черзі рівнів гри, що мають відповідну назву.

Окрім зазначених дитячих програм та інструкцій, в США при ФБР функціонує проект «Безпечне дитинство», що реалізується спільно з Міністерством юстиції США.

Зазначений проект – це загальнонаціональна ініціатива з боротьби зі зростаючою епідемією сексуальної експлуатації та наруги над дітьми в мережі Інтернет, запущена міністерством юстиції в травні 2006 року. На чолі з офісами адвокатів США і Секцією по експлуатації і непристойності дітей (CEOS), Кримінального відділу проекту «Безпечне дитинство» збираються федеральні, штатні і місцеві ресурси для кращого пошуку, затримання і переслідування осіб, які експлуатують дітей через Інтернет, а також для виявлення і рятувати жертв (U. S. Department of Justice, 2025).

У рамках зазначеного проекту створена робоча група з питань протидії кібербулінгу, що має назву stopbullying. gov, та активно веде інтернет-блог з актуальних питань протидії кібербулінгу. Працівниками групи stopbullying. gov здійснюються систематичні заходи в школах та інших освітніх закладах, щоб допомогти учням дізнатися про профілактику кібербулінгу. Приклади занять з кібербулінгу включають в себе:

- інтернет або бібліотечні дослідження, такі як пошук типів знущань, як їм запобігти і як діти повинні реагувати;
- презентації, такі як мова або рольова гра про припинення кібербулінгу;
- обговорення таких тем, як повідомлення про кібербулінг;
- письменницька творчість, таке як вірш, що виступає проти кібербулінгу, або розповідь або пародія, навчальні свідків того, як допомогти;
- художні твори, такі як колаж про повагу або наслідки від дії кібербулерів;
- зустрічі в класі, щоб поговорити про відносини з однолітками (Stopbullying. gov., 2017). Також, в межах діяльності робочої групи постійно дії практичний дитячий психолог, який завжди готовий допомогти у скрутній для дитини ситуації.

Таким чином, в США при ФБР спільно з іншими державними органами створено ряд бюро та робочих груп з питань протидії кіберзлочинності з різними категоріями громадян та у відповідності до їх соціального статусу. Особливу цінність на наш погляд складає досвід щодо врегулювання питання забезпечення кібербезпеки дітей у Інтернет-просторі та протидії кібербулінгу.

Задовго до того, як кіберзлочинність була визнана серйозною загрозою злочинності для національної безпеки, ФБР підтримало ініціативу щодо створення перспективної організації для активного вирішення проблеми кіберзлочинності. Названа Національним альянсом по кіберкриміналістиці і навчання (NCFTA) організація, створена в 1997 році, що базується в Піттсбурзі, стала міжнародною моделлю для об'єднання зусиль правоохоронних органів, приватного сектора і наукових кіл для створення та обміну ресурсами, стратегічною інформацією і аналіз загроз для виявлення і припинення виникають кіберзагроз та вжиття заходів щодо їх протидії.

З моменту свого створення NCFTA розвивалася, щоб йти в ногу з мінливим ландшафтом кіберзлочинності. Сьогодні організація займається обробкою та протидією погроз з боку транснаціональних злочинних груп, включаючи спам, ботнети, схеми маніпулювання запасами, крадіжки інтелектуальної власності, фармацевтичне шахрайство, шахрайство в сфері телекомунікацій і інші схеми фінансового шахрайства, які призводять до збитків для компаній і споживачів в мільярди доларів.

Підрозділ CyberInitiativeandResource (CIRFU) кібервідділу ФБР співпрацює з NCFTA, що спирається на інформацію сотень членів NCFTA з приватного сектора, аналітиків NCFTA, групи реагування на комп' ютерні інциденти (CERT) при Університеті Карнегі-Меллона та інтернету ФБР. Ця велика база знань допомогла CIRFU зіграти ключову стратегічну роль в деяких з найбільш значних кіберсправ ФБР за останні кілька років.

Навіть після виконання своїх обов'язків щодо забезпечення національної безпеки після 11 вересня ФБР продовжує грати ключову роль в боротьбі з насильницькими злочинами в великих містах і місцевих громадах по всій території Сполучених Штатів.

Через глобальне охоплення кіберзлочинності жодна організація, агентство або країна не можуть захиститися від нього. Життєво важливі партнерства, такі як NCFTA, є ключем до захисту кіберпростору і забезпечення більш безпечного кібермайбутнього для наших громадян і країн по всьому світу (ФБР, 2025).

Оскільки кіберзагрози продовжують з'являтися майже кожного дня, для ФБР в області кримінальної та національної безпеки, вкрай важливо залучення державних і приватних партнерів щодо обміну інформацією поряд з правоохоронними

та розвідувальними колами. Щоб залучити надійних галузевих партнерів в розвідувальну групу, ФБР спростило свою систему відстеження та управління погрозами Guardian з метою захищеного інформаційного порталу, що дозволяє окремим партнерам в галузі повідомляти про інциденти, пов'язані з кіберзлочинністю, в режимі реального часу.

iGuardian надає приватним компаніям стандартизований спосіб повідомляти інформацію в ФБР, якщо вони стають жертвами комп'ютерних вторгнень. Портал iGuardian – це еволюція платформи, через яку правоохоронні партнери ФБР надають потенційні загрози тероризму і повідомлення про підозрілі дії. У той час як eGuardian залучає співробітників правоохоронних органів, iGuardian був розроблений спеціально для партнерів в критичних секторах телекомунікацій, оборони, банківської справи та фінансів, а також в області енергетичної інфраструктури і доступний через чутливу, але несекретну мережу InfraGard.

InfraGard – це коаліція ФБР щодо захисту державної і приватної інфраструктури, в яку входять тисячі перевірених і націлених на галузь членів. Організація підтримує свою власну захищену мережу для поширення попереджень та бюлетенів ФБР і дозволяє обмінюватися інформацією про ключові загрози серед своїх членів. Використовуючи систему iGuardian, учасникам пропонується направляти інформацію про вторгнення безпосередньо в ФБР, в тому числі детальну інформацію про зараження шкідливим ПЗ, псування вебсайтів і атаках типу «відмова в обслуговуванні». Програма iGuardian також надає партнерів InfraGard доступ до інформації та відомостями, отриманими в результаті пов'язаних інцидентів (Боротьба зі злочинністю в Інтернеті (онлайн злочинність), 2006).

Кожен звіт про інцидент в iGuardian направляється через Guardian в CyWatch, цілодобовий центр кібероперацій ФБР, де агенти і аналітики сортують і знімають конфлікт з вхідних даних, повідомляють раніше невідомих жертв вторгнення і призначають висновки до відповідних польові офіси для подальшого розслідування. Таке централізоване управління кіберзлочинами в області кримінальної безпеки і національної безпеки дозволяє ФБР більш ефективно працювати з нашими партнерами, щоб використовувати відомі розвіддані і проводити розслідування і операції в очікуванні. Оскільки iGuardian надає важливий, додаткове джерело відповідної інформації про кібервторгнення, він також дозволяє сфокусуватися на загальному уявленні про загрозу, яку представляють терористи, національні держави і злочинні групи, які проводять мережеві операції проти США. Створення цієї широкої бази загроз обізнаність і партнерство дуже важливі для кібер місії ФБР (Боротьба зі злочинністю в Інтернеті (онлайн злочинність), 2006).

Окрім, зазначеної платформи iGuardian, в США на постійній основі діє Національна об'єднана оперативна група з кіберрозслідувань (NCIJTF), що була офіційно створена в 2008 році. Національна об'єднана оперативна група по кіберрозслідувань складається з більш ніж 20 партнерських агентств з правоохоронних органів, розвідувального співтовариства та Міністерства оборони, представники яких знаходяться в одному місці і працюють спільно, щоб виконати місію організації з точки зору всього уряду. Будучи унікальним кіберцентром Національна об'єднана оперативна група з кіберрозслідувань несе головну відповідальність за координацію, інтеграцію та обмін інформацією для підтримки розслідувань кіберзагроз, надання та підтримки аналітичного аналізу для осіб, які приймають рішення в співтоваристві, і для забезпечення цінності інших поточних зусиль в боротьбі. проти кіберзагрози нації (2008).

Національна об'єднана оперативна група з кіберрозслідувань також синхронізує спільні зусилля, спрямовані на виявлення, переслідування і знищення реальних терористів, шпигунів і злочинців, які прагнуть експлуатувати системи нашої країни. Для досягнення цієї мети цільова група використовує колективні повноваження і можливості своїх членів і співпрацює з міжнародними партнерами і партнерами з приватного сектора, щоб задіяти всі наявні ресурси для боротьби з внутрішніми кіберзагрозами і їх виконавцями.

За допомогою координації, співпраці і обміну інформацією, яка відбувається в NCIJTF, члени уряду США працюють над тим, щоб посадити кіберзлочинців за ґрати і видалити їх з національних мереж. NCIJTF слід букві і духу закону, щоб забезпечити захист прав на недоторканність приватного життя всіх американців в ході розслідувань і зусиль, які він координує і підтримує (2008).

Підсумовуючи викладене, зазначимо, в США з метою ефективної боротьби з кіберзлочинністю та забезпечення кібербезпеки держави, створено належне правове поле діяльності спеціалізованих суб'єктів боротьби з кіберзлочинністю та створено дієву систему органів, основними функціями визначено забезпечення кіберзахисту та протидії всім проявам кіберзлочинності, що беззаперечно суттєво впливає на стан правопорядку в державі.

Висновки

Аналіз функціонування органів та підрозділів, що здійснюють протидію кіберзлочинності у США підтверджується прагненням України налагодити міжнародну співпрацю у зазначеній сфері. Встановлено, що ФБР є провідним федеральним агентством США з розслідування кібератак, що вчиняються злочинцями, зарубіжними противниками і терористами. Оскільки кібервторгнення стають все більш поширеним явищем, сьогодні діяльність ФБР постійно удосконалюється, щоб краще протистояти терористичній загрозі після терактів 11 вересня 2001 року.

Поряд із цим, одним із пріоритетних напрямків протидії кіберзлочинності в США є протидія торгівлі людьми, що здійснюється із застосуванням інформаційних технологій у віртуальному просторі та завдає шкоди охоронюваним законом правам та основоположним свободам людини й громадянина.

Визначено, що в США з метою ефективної боротьби з кіберзлочинністю та забезпечення кібербезпеки держави, створено належне правове поле діяльності спеціалізованих суб'єктів боротьби з кіберзлочинністю та створено дієву систему органів, основними функціями визначено забезпечення кіберзахисту та протидії всім проявам кіберзлочинності, що беззаперечно суттєво впливає на стан правопорядку в державі.

Список використаних джерел

Петровський О. М., Лівчук С. Ю. (2019). Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Молодий вчений.* № 12.1 (76.1). С. 55–59.

NYPD. (2025). Бюро по боротьбі з тероризмом. URL: https://www1.nyc.gov/site/nypd/bureaus/investigative/counterterrorism.page

Лапта С. П. (2017). ФБР у боротьбі з кіберзлочинністю. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : матеріали Всеукр. наук.-практ. конф., м. Харків, МВС України. Харків. Нац. ун-т внутр. справ. Харків. С. 197–199.

УНН. (2020). Україна та США обговорили спільну протидію кіберзлочинності. URL: https://www.unn.com.ua/uk/news/1849243-ukrayina-ta-ssha-obgovorili-spilnu-protidiyu-kiberzlochinnosti

Чумак В. В. (2017). Європейський досвід реформування правоохоронних органів (на прикладі Естонії). URL: http://univd.edu.ua/general/publishing/konf/25_11_2017/pdf/171.pdf

ФБР. (2025). Кіберзлочинність. URL: https://www.fbi.gov/investigate/cyber

Internet Crime Complaint Center (2025). Інтернет-центр скарг на кіберзлочини. URL: https://www.ic3.gov/preventiontips.aspx

Чумак В. В. (2015). Основні напрями та особливості організації діяльності поліції Латвії. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі : матеріали наук.-практ. конф., м. Львів, 17 груд. 2015 р., МВС України. Львів. Держ. ун-т внутр. справ. Львів, С. 146–149.

U. S. Department of Justice (2025). Проєкт безпечне дитинство. Міністерство юстиції США. URL: https://www.justice. gov/psc

Stopbullying.gov. (2017). Профілактика у школі. URL: https://www.stopbullying.gov/prevention/at-school

Боротьба зі злочинністю в Інтернеті (онлайн злочинність). (2006). *Інформаційний бюлетень Міжвід. наук.-дослід. центру з проблем боротьби з організованою злочинністю.* № 7. С. 133–141.

Національна об'єднана оперативна група з кіберрозслідувань. *ФБР.* (2008). URL: https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force