УДК 343.9
DOI 10.33244/2617-4154.1(10).2023.151-160

О. О. Колосов,
аспірант,
Державний податковий університет
e-mail: kolosov2424@gmail.com
ORCID ID 0000-0003-0128-5565

ОСОБЛИВОСТІ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ У СПОЛУЧЕНИХ ШТАТАХ АМЕРИКИ

У цій статті визначено особливості протидії кіберзлочинам у Сполучених Штатах Америки. Визначено відповідні органи США, які займаються боротьбою із кіберзлочинністю, до яких належать: Федеральне бюро розслідувань США (провідний орган), Міністерство національної безпеки США, до складу якого входять Секретна служба США та Міграційна та митна правоохоронна служба США. Важливу роль у протидії та боротьбі з кіберзлочинністю в США відіграє центр скарг на інтернет-злочини (IC3) – центральний пункт, через який жертви інтернет-злочинів можуть повідомляти та сповіщати відповідні органи про підозру в злочинній діяльності в інтернеті.

У Секретній службі США є цільові групи з електронних злочинів, які зосереджені на виявленні та знаходженні міжнародних кіберзлочинців, пов'язаних з кібер-вторгненнями, банківськими шахрайствами, витоком даних та іншими комп'ютерними злочинами. Центр кіберзлочинів підрозділу розслідувань з питань внутрішньої безпеки Міграційної та митної правоохоронної служби США надає комп'ютерні технічні послуги для підтримки внутрішніх та міжнародних розслідувань транскордонних злочинів.

Національний центр захисту інфраструктури отримав національну місію із захисту критичної інфраструктури, яка включає: виявлення, оцінку, попередження та розслідування значних загроз та інцидентів щодо критичної інфраструктури США. Це міжвідомчий центр, який фізично розташований у відділі боротьби з тероризмом у штаб-квартирі ФБР.

ФБР спільно з центром створило Національну програму захисту інфраструктури та комп'ютерних вторгнень як слідчу програму в рамках відділу боротьби з тероризмом. Також у статті зосереджено увагу на «гібридних» загонах, сформованих рядом відділень на місцях ФБР, які об'єднують ресурси та слідчих Національної програми захисту інфраструктури та комп'ютерних вторгнень, групи комп'ютерного аналізу та реагування, а також слідчих, які займаються розслідуванням злочинів білих комірців, насильницьких злочинів та боротьбою з організованою злочинністю/ торгівлею наркотиками в одній команді для вирішення питань кіберзлочинності.

Також наголошено на важливості співпраці ФБР у питанні боротьби з кіберзлочинністю з приватним сектором. Цільові групи створюються з приватним сектором для розвитку довгострокових робочих відносин, які допомагають у визначенні проблем кіберзлочинності та впливу, який вони мають на їхній бізнес, а також у формуванні проактивних стратегій для подолання загроз.

Наголошено на співпраці між Україною та США у контексті протидії кіберзлочинності. Федеральне бюро розслідувань США надало пряму підтримку своїм українським партнерам з національної безпеки та правоохоронних органів, включаючи інформування українських партнерів про кібероперації російських спецслужб.

Наголошено на співпраці Адміністрації Державної служби спеціального зв'язку та захисту інформації України і Агентства з кібербезпеки та безпеки інфраструктури Державного департаменту США. Також приділено увагу підписаній міністрами оборони України та США Рамковій угоді про стратегічні основи оборонного партнерства, яка дає змогу розвивати співпрацю в галузях кіберзахисту й розвитку кібервійськ, захисту критичної інформаційної інфраструктури. Це співробітництво у сфері кіберзахисту має на меті стримування шкідливої кібердіяльності проти систем національної безпеки, розвиток медичних спроможностей, співпрацю у сфері протидії дезінформації.

Надано відповідні пропозиції покращення протидії кіберзлочинності в Україні. Зокрема, щодо створення в Україні спеціального вебсайту для повідомлень про кіберзлочини – Центру скарг на інтернет-злочини за прикладом американського центру – Internet Crime Complaint Center (IC3); використання досвіду США у частині створення «гібридних» відділів протидії та боротьбі з кіберзлочинами; створення цільових груп національних правоохоронних органів з приватним сектором задля вирішення проблем кіберзлочинності в Україні.

Ключові слова: *Федеральне бюро розслідувань США, Секретна служба США, кіберзлочин, безпека, протидія.*

Мета статті полягає у дослідженні досвіду Сполучених Штатів Америки у питаннях протидії кіберзлочинам та формування відповідних пропозицій щодо покращення комплексу заходів протидії кіберзлочинності в Україні.

Постановка проблеми. Станом на сьогодні проблематика кіберзлочинності є, як ніколи, актуальною, враховуючи розвиток комп'ютеризації у світі та збільшення у зв'язку з цим можливостей для викрадення, спотворення та знищення даних. Сполучені Штати Америки є однією з найбільш комп'ютеризованих країн світу [1]. Також варто зауважити щодо значної підтримки України Сполученими Штатами у питанні забезпечення кібербезпеки нашої держави. Так, Федеральне бюро розслідувань США надало пряму підтримку своїм українським партнерам з національної безпеки та правоохоронних органів, включаючи інформування українських партнерів про кібероперації російських спецслужб. Також ФБР забезпечує обмін інформацією, що стосується кіберзагроз, щодо потенційної або поточної шкідливої кіберактивності; сприяє зриву зусиль національних держав з поширення дезінформації та націлювання

на український уряд та військових; здійснює обмін методами розслідування та найкращими методами реагування на кіберінциденти [2]. Саме тому доцільно звернутися до американського досвіду щодо протидії кіберзлочинам.

Аналіз останніх публікацій. Проблематиці протидії кіберзлочинності присвячено роботи таких вітчизнаних учених: Д. С. Азарова, П. Д. Біленчука, В. М. Бутузова, В. Б. Вєхова, В. Д. Гавловського, В. О. Голубєва, О. Ю. Іванченко, М. В. Карчевського, А. А. Музики, Д. В. Пашнєва, В. С. Цимбалюка, В. П. Шеломенцева та ін.

Виклад основного матеріалу. Уряд Сполучених Штатів заявив, що одна з найсерйозніших проблем економічної та національної безпеки, з якими США зіштовхується як нація, стосується кібербезпеки [3]. 60 мільйонів американців зіштовхувались із шахрайським використанням особистих даних, як показує статистика крадіжки особистих даних. Згідно зі статистикою кіберзлочинності за 2017 рік особисті облікові дані 16,7 млн споживачів були вкрадені та використані без їх відома. Це призвело до розкрадання 16,8 млрд доларів у споживачів за один рік. 59 % американців повідомляють, що стикалися з кіберзлочинами або якимось чином потрапили до рук комп'ютерного хакера. Це становить 152 млн американських споживачів, чия безпека в Інтернеті так чи інакше була порушена. У 2018 році 105 млн американців заявили, що стикалися з кіберзлочинами. Кіберзлочинність вплинула на 41 % американського населення станом на 2018 рік [4].

Міністерство юстиції США визначає комп'ютерну злочинність як будь-які порушення кримінального законодавства, що передбачають знання комп'ютерних технологій для їх вчинення, розслідування або судового переслідування [5]. У США провідним органом, який займається боротьбою із кіберзлочинністю, є Федеральне Бюро Розслідувань (англ. Federal Bureau of Investigation) (надалі – ФБР), зокрема, у цьому напрямі ФБР працює так:

— у ФБР є спеціально навчені кіберзагони в кожному з 56 відділень на місцях ФБР, які працюють пліч-о-пліч з партнерами міжвідомчих оперативних груп;

— група швидкого реагування Cyber Action Team може бути розгорнута по всій країні впродовж кількох годин для реагування на великі інциденти;

— маючи помічників з юридичних питань (англ. cyber assistant legal attachés) у посольствах у всьому світі, ФБР тісно співпрацює з міжнародними партнерами, домагаючись справедливості для жертв зловмисної кіберактивності;

— центр скарг на інтернет-злочини (IC3) (англ. Internet Crime Complaint Center) (надалі – IC3) збирає повідомлення про інтернет-злочини від громадськості. Використовуючи такі скарги, команда IC3 із відновлення активів (англ. IC3's Recovery Asset Team) допомогла заморозити сотні тисяч доларів для жертв кіберзлочинів;

— CyWatch – це оперативний центр ФБР 24/7, що працює цілодобово і без вихідних, забезпечує цілодобову підтримку для відстеження інцидентів та зв'язку з відділеннями на місцях по всій країні [6].

У своїй діяльності у боротьбі з кіберзлочинністю IC3:

— здійснює партнерство з приватним сектором, а також з місцевими, державними, федеральними та міжнародними агенствами;

— розміщує портал, на якому жертви повідомляють про інтернет-злочини на www.ic3.gov;

— забезпечує центральний хаб для оповіщення громадськості;

— здійснює проведення аналізу, передачу скарг, і допомогу у заморожуванні активів;

— розміщує бази даних віддаленого доступу для всіх правоохоронних органів через вебсайт LEEP ФБР [7].

До основних функцій IC3 належать:

1. Збирання (англ. Collection) (IC3 є центральним пунктом, через який жертви інтернет-злочинів можуть повідомляти та сповіщати відповідні органи про підозру в злочинній діяльності в інтернеті. Правоохоронні органи заохочують та часто спрямовують жертв подавати скаргу онлайн на сайті www.ic3.gov. Скаржників просять надати точну та повну інформацію щодо інтернет-злочинів, а також будь-яку іншу відповідну інформацію, необхідну для підтримки скарги.

2. Аналіз (англ. Analysis) (IC3 переглядає та аналізує дані, подані через свій вебсайт з метою виявлення виникаючих загроз та нових тенденцій. Крім того, IC3 швидко повідомляє фінансові установи про шахрайські транзакції, що дозволяє заморожувати кошти жертви).

3. Інформування населення (англ. Public awareness) (службові оголошення, галузеві сповіщення та інші публікації, що описують конкретні шахрайства, розміщені на веб-сайті www.ic3.gov. Оскільки все більше людей дізнається про злочини в інтернеті та методи, які використовуються для їх здійснення, потенційні жертви мають більш широке розуміння небезпек, пов’язаних з інтернет-діяльністю, і мають кращу позицію, щоб не стати жертвою онлайнових схем).

4. Звернення (англ. Referrals) (IC3 об’єднує пов’язані скарги для створення звернень, які пересилаються до місцевих, державних, федеральних та міжнародних правоохоронних органів для потенційного розслідування. Якщо правоохоронні органи проводять розслідування та встановлюють факт вчинення злочину, проти винного може бути порушена кримінальна справа) [5].

Відповідно до щорічного звіту ФБР щодо злочинів в інтернеті (англ. FBI's annual Internet Crime Report), опублікованого 22 березня 2022 року, в 2021 році люди втратили більше ніж 6,9 млрд доларів у результаті інтернет-злочинів, що на 2 млрд більше, ніж у 2020 році [8]. У 2021 році IC3 отримав 19 954 скарги щодо компроментації ділової електронної пошти (англ. Business Email Compromise) (надалі – BEC) / компроментації облікового запису електронної пошти (англ. Email Account Compromise) (надалі – EAC) зі скоригованими збитками на суму майже 2,4 млрд доларів. BEC/EAC – це складне шахрайство, спрямоване як на підприємства, так і на фізичних осіб, які здійснюють переказ коштів. Шахрайство часто здійснюється, коли суб’єкт компроментує законні ділові облікові записи електронної пошти за допомогою соціальної інженерії або методів комп’ютерного вторгнення задля здійснення несанкціонованого переказу коштів [7].

Також боротьбою з кіберзлочинністю займається Міністерство національної безпеки США (англ. Department of Household Security). Міністерство національної безпеки США (далі – DHS) співпрацює з іншими федеральними агенціями для проведення високоефективних кримінальних розслідувань, спрямованих на припинення злочинної діяльності та боротьбу проти кіберзлочинців, визначення пріоритетів набору та навчання технічних експертів, розробки стандартизованих методів і широкого обміну передовим досвідом та інструментами реагування на кіберзлочини. Слідчі кримінальних справ та експерти з мережевої безпеки, які глибоко розуміють технології, які використовують зловмисники, і конкретні вразливості, на які вони націлені, працюють з метою ефективного реагування на кіберінциденти та їх розслідування [9].

Складові DHS – Секретна служба США (англ. U.S. Secret Service) та Міграційна та митна правоохоронна служба США (англ. Immigration and Customs Enforcement) мають спеціальні підрозділи, які займаються боротьбою з кіберзлочинністю. Так, у Секретній службі США є цільові групи з електронних злочинів, які зосереджені на виявленні та знаходженні міжнародних кіберзлочинців, пов'язаних з кібервторгненнями, банківськими шахрайствами, витоком даних та іншими комп'ютерними злочинами [9].

Відповідно до щорічного звіту DHS за 2020 рік у 2020 фінансовому році розслідування Секретної служби США притягли до відповідальності багаточисленних кіберзлочинців високого рівня. Завдяки постійному розслідуванню зі сторони спеціальних агентів та аналітиків слідчі Секретної служби США закрили справи на суму 1,0 млрд доларів збитків жертв. Заарештовуючи осіб до того, як вони змогли повністю усвідомити вигоди від своїх злочинів, розслідування Секретної служби США також запобігли потенційним збиткам від шахрайства ще на 2,6 млрд доларів [10].

Центр кіберзлочинів (англ. Cyber Crimes Center) підрозділу розслідувань з питань внутрішньої безпеки (англ. Homeland Security Investigations) Міграційної та митної правоохоронної служби США надає комп'ютерні технічні послуги для підтримки внутрішніх та міжнародних розслідувань транскордонних злочинів. Центр кіберзлочинів пропонує підтримку та навчання у сфері кіберзлочинності для федеральних, державних, місцевих та міжнародних правоохоронних органів. Центр кіберзлочинів також керує повністю обладнаною лабораторією комп'ютерної криміналістики, яка спеціалізується на вилученні цифрових доказів, а також пропонує навчання навичкам комп'ютерного розслідування та судово-медичної експертизи [9].

Створений у лютому 1998 року Національний центр захисту інфраструктури (англ. National Infrastructure Protection Center) (далі – NIPC, а також «центр») отримав національну місію із захисту критичної інфраструктури відповідно до Президентської директиви 63. Місія NIPC включає: виявлення, оцінку, попередження та розслідування значних загроз та інцидентів щодо критичної інфраструктури США. Це міжвідомчий центр, який фізично розташований у відділі боротьби з тероризмом у штаб-квартирі ФБР. ФБР спільно з центром створило Національну програму захисту інфраструктури та комп'ютерних вторгнень (англ. National Infrastructure Protection and Computer Intrusion Program) (далі – NIPCIP, а також «програма») як слідчу програму в рамках

відділу боротьби з тероризмом. Початкові розслідування випадків комп'ютерного вторгнення в основному проводилися загонами NIPCIP. У ході таких розслідувань усе частіше з'ясовується, що вторгнення було лише першим кроком у більш традиційній злочинній схемі, пов'язаній з шахрайством чи іншою фінансовою вигодою. На цьому етапі розслідування справа зазвичай передається до основного відділу, який займається такими видами злочинних схем. Через природу кіберзлочинності та спосіб, у який вона перетинає традиційні межі програми, ряд відділень на місцях ФБР сформували «гібридні» загони, які об'єднують ресурси та слідчих NIPCIP, групи комп'ютерного аналізу та реагування, а також слідчих, які займаються розслідуванням злочинів білих комірців, насильницьких злочинів та боротьбою з організованою злочинністю/ торгівлею наркотиками в одній команді для вирішення питань кіберзлочинності [11].

Не менш важливою є співпраця ФБР у питанні боротьби з кіберзлочинністю з приватним сектором. Цільові групи були і будуть створюватися з приватним сектором для розвитку довгострокових робочих відносин, які допоможуть у визначенні проблем кіберзлочинності та впливу, який вони мають на їхній бізнес, а також у формуванні проактивних стратегій для подолання загроз. Ці відносини сприяють інформуванню приватним сектором про злочинну діяльність, оцінці / попередження загроз приватному сектору та наданню допомоги приватним сектором правоохоронним органам (експертиза предметної області, технічна експертиза тощо) [11].

Для України важливою є співпраця з США у контексті протидії кіберзлочинності. Так, у 2021 році делегація Адміністрації Державної служби спеціального зв'язку та захисту інформації України і представники Агентства з кібербезпеки та безпеки інфраструктури Державного департаменту США домовилися про співпрацю [12].

Також 2021 року міністрами оборони України та США було підписано Рамкову угоду про стратегічні основи оборонного партнерства. Угода дає змогу розвивати співпрацю в галузях кіберзахисту й розвитку кібервійськ, захисту критичної інформаційної інфраструктури [13]. Зокрема, це співробітництво у сфері кіберзахисту з метою стримування шкідливої кібердіяльності проти систем національної безпеки, розвитку медичних спроможностей, співпраця у сфері протидії дезінформації [14].

Висновки і пропозиції. Отже, на сьогодні питання протидії кіберзлочинності є нагальним та потребує уваги. Вважаємо позитивною співпрацю між Україною та США у питаннях протидії кіберзлочинності. На основі досвіду Сполучених Штатів Америки пропонуємо таке:

— створити в Україні спеціальний вебсайт для повідомлень про кіберзлочини – Центр скарг на інтернет-злочини за прикладом американського центру – Internet Crime Complaint Center (IC3). Важливість створення такого Центру (вебсайту) полягає в тому, що повідомлення про кіберзлочини здійснюється в спеціально створеній інтернет-платформі, що забезпечує єдиний підхід щодо аналізу та оцінки отриманої інформації, а також інформування держаних органів влади, органів місцевого самоврядування, бізнесу та громадськості щодо актуального стану справ, потенційних і можливих кіберзагроз, кібератак та кіберзлочинів і порад щодо того, як уберегтися від таких загроз, атак та злочинів;

— перейняти досвід США у частині створення «гібридних» відділів протидії та боротьби з кіберзлочинами, у які повинні входити спеціалісти, які володіють традиційними навичками і знаннями розслідування злочинів, а також спеціалісти зі спеціальними високотехнологічними навичками та знаннями;

— створити цільові групи національних правоохоронних органів з приватним сектором задля вирішення проблем кіберзлочинності в Україні. Зокрема, завдяки такій співпраці можливим є покращення збирання та аналізу інформації щодо кіберзагроз; розробка інструментів (наприклад, спеціальних комп'ютерних програм тощо) щодо боротьби з кібератаками; поглиблення знань бізнесу щодо кіберзагроз та боротьби з ними, що є вкрай важливим для належного функціонування економіки в державі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber Terrorism Now at the Top of the List of Security Concerns / Military.com: вебсайт. URL: https://www.military.com/defensetech/2011/09/12/cyber-terrorism-now-at-the-top-of-the-list-of-security-concerns (дата звернення: 10.05.2022).

2. U.S. Support for Connectivity and Cybersecurity in Ukraine / Федеральне Бюро Розслідувань США. URL: https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/#:~:text=Prior%20to%20February%202022%2C%20the,capacity%20development%20assistance%20since%202017 (дата звернення: 12.05.2022).

3. Brian J Greer. The Growth of Cybercrime in the United States. URL: https://www.researchgate.net/profile/Brian-Greer (дата звернення: 12.05.2022).

4. More Than 70 Cybercrime Statistics – A $6 Trillion Problem / DataProt: вебсайт. URL: https://dataprot.net/statistics/cybercrime-statistics/#:~:text=60%20million%20Americans%20have%20experienced%20identity%20fraud%2C%20identity%20theft%20statistics%20show.&text=According%20to%20cyber%20crime%20statistics%20from%202017%2C%2016.7%20million%20consumers,consumers%20in%20a%20single%20year (дата звернення: 12.05.2022).

5. Cyber Crime Legislation / International Telecommunication Union (ITU): вебсайт. URL: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf (дата звернення: 15.05.2022).

6. The Cyber Threat / Федеральне Бюро Розслідувань США. URL: https://www.fbi.gov/investigate/cyber (дата звернення: 15.05.2022).

7. Internet Crime Report 2021 / Federal Bureau of Investigation Internet Crime Complaint Center IC3: вебсайт. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (дата звернення: 15.05.2022).

8. Internet Crime Cost People More Than $6.9B in 2021, FBI Says / CNET: вебсайт. URL: https://www.cnet.com/tech/computing/internet-crime-cost-people-more-than-6-9b-in-2021-fbi-says/ (дата звернення: 15.05.2022).

9. Combating Cyber Crime / Агентство з кібербезпеки та безпеки інфраструктури США. URL: https://www.cisa.gov/combating-cyber-crime (дата звернення: 15.05.2022).

10. Annual Report FY 2020 / Секретна служба США. URL: https://www.secretservice.gov/sites/default/files/reports/2021-03/2020-Annual-Report.pdf (дата звернення: 16.05.2022).

11. Archived material from the Federal Bureau of Investigation (FBI) website / Федеральне Бюро Розслідувань США. URL: https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem (дата звернення: 17.05.2022).

12. Держспецзв'язку співпрацюватиме зі службою кібербезпеки Держдепу США – готують угоду. *Мультимедійна платформа іномовлення України «Укрінформ».* URL: https://www.ukrinform.ua/rubric-technology/3309439-derzspeczvazku-spivpracuvatime-zi-sluzbou-kiberbezpeki-derzdepu-ssa-gotuut-ugodu.html (дата звернення: 17.05.2022).

13. Америка не полишає нас у боротьбі з агресором. *Урядовий кур'єр* / Кабінет Міністрів України. URL: https://ukurier.gov.ua/uk/articles/amerika-ne-polishaye-nas-u-borotbi-z-agresorom/ (дата звернення: 18.05.2022).

14. Мінветеранів вітає підписання у США рамкової угоди щодо стратегічних основ оборонного партнерства / Міністерство у справах ветеранів України. URL: https://mva.gov.ua/ua/news/minveteraniv-vitaye-pidpisannya-u-ssha-ramkovoyi-ugodi-shchodo-strategichnih-osnov-oboronnogo-partnerstva (дата звернення: 18.05.2022).

REFERENCES

1. Cyber Terrorism Now at the Top of the List of Security Concerns / Military.com: vebsayt. URL: https://www.military.com/defensetech/2011/09/12/cyber-terrorism-now-at-the-top-of-the-list-of-security-concerns [in English].

2. U.S. Support for Connectivity and Cybersecurity in Ukraine / US Federal Bureau of Investigation. URL: https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/#:~:text=Prior%20to%20February%202022%2C%20the,capacity%20development%20assistance%20since%202017 [in English].

3. Brian J Greer. The Growth of Cybercrime in the United States. URL: https://www.researchgate.net/profile/Brian-Greer [in English].

4. More Than 70 Cybercrime Statistics – A $6 Trillion Problem / DataProt: vebsayt. URL: https://dataprot.net/statistics/cybercrime-statistics/#:~:text=60%20million%20Americans%20have%20experienced%20identity%20fraud%2C%20identity%20theft%20statistics%20show.&text=According%20to%20cyber%20crime%20statistics%20from%202017%2C%2016.7%20million%20consumers,consumers%20in%20a%20single%20year [in English].

5. Cyber Crime Legislation / International Telecommunication Union (ITU): vebsayt. URL: https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/Tafazzoli-cybercrime%20legislations.pdf [in English].

6. The Cyber Threat / US Federal Bureau of Investigation. URL: https://www.fbi.gov/investigate/cyber [in English].

7. Internet Crime Report 2021 / Federal Bureau of Investigation Internet Crime Complaint Center IC3: vebsayt. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf [in English].

8. Internet Crime Cost People More Than $6.9B in 2021, FBI Says / CNET: vebsayt. URL: https://www.cnet.com/tech/computing/internet-crime-cost-people-more-than-6-9b-in-2021-fbi-says/ [in English].

9. Combating Cyber Crime / Cybersecurity Infrastructure Security Agency. URL: https://www.cisa.gov/combating-cyber-crime [in English].

10. Annual Report FY 2020 / United States Secret Service. URL: https://www.secretservice.gov/sites/default/files/reports/2021-03/2020-Annual-Report.pdf [in English].

11. Archived material from the Federal Bureau of Investigation (FBI) website / US Federal Bureau of Investigation. URL: https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem [in English].

12. Derzhspetszv″yazku spivpratsyuvatyme zi sluzhboyu kiberbezpeky Derzhdepu SSHA – hotuyut′ uhodu. *Mul'tymediyna platforma inomovlennya Ukrayiny «Ukrinform»*. URL: https://www.ukrinform.ua/rubric-technology/3309439-derzspeczvazku-spivpracuvatime-zi-sluzbou-kiberbezpeki-derzdepu-ssa-gotuut-ugodu.html [in Ukrainian].

13. Ameryka ne polyshaye nas u borot′bi z ahresorom. *Uryadovyy kur'yer* / Kabinet Ministriv Ukrayiny. URL: https://ukurier.gov.ua/uk/articles/amerika-ne-polishaye-nas-u-borotbi-z-agresorom/ [in Ukrainian].

14. Minveteraniv vitaye pidpysannya u SSHA ramkovoyi uhody shchodo stratehichnykh osnov oboronnoho partnerstva / Ministerstvo u spravakh veteraniv Ukrayiny. URL: https://mva.gov.ua/ua/news/minveteraniv-vitaye-pidpisannya-u-ssha-ramkovoyi-ugodi-shchodo-strategichnih-osnov-oboronnogo-partnerstva [in Ukrainian].

O. Kolosov. Features of Combating Cybercrimes in the United States of America

This article defines the features of combating cybercrime in the United States of America. The relevant US agencies involved in the fight against cybercrime have been identified, which include: the US Federal Bureau of Investigation (the lead agency), the US Department of Household Security, which includes the US Secret Service and the US Immigration and Customs Enforcement. An important role in countering and combating cybercrime in the United States is played by the Internet Crime Complaint Center (IC3) - a central point through which victims of Internet crime can report and notify the appropriate authorities of suspicion of criminal activity on the Internet.

The US Secret Service has e-crime task forces that focus on identifying and finding international cybercriminals associated with cyber intrusions, bank fraud, data breaches, and other computer crimes. The U.S. Immigration and Customs Enforcement Homeland Security Investigations Cyber Crimes Center provides computer technical services to support domestic and international cross-border crime investigations.

The National Infrastructure Protection Center was given a national critical infrastructure protection mission that includes: detecting, assessing, warning of and investigating

significant threats and incidents concerning US critical infrastructures. It is an interagency center physically located within the Counterterrorism Division at FBI headquarters.

The FBI in conjunction with the center created the National Infrastructure Protection and Computer Intrusion Program as an investigative program within the Counterterrorism Division. Also, the article focuses on the "hybrid" squads formed by a number of FBI field offices which combine National Infrastructure Protection and Computer Intrusion Program, cart, white collar crime, violent crime, and organized crime/drug trafficking resources and investigators on one squad to address cyber crime matters.

Also, the importance of the cooperation of the FBI in the fight against cybercrime with the private sector was noted. Focus groups are being formed with the private sector to develop long term working relationships which aid in identifying cyber crime problems and the impact they have on their businesses as well as the formation of proactive strategies to address the threats.

The cooperation between Ukraine and the United States in the context of combating cybercrime was noted. The U.S. Federal Bureau of Investigation has provided direct support to its Ukrainian national security and law enforcement partners, including briefing Ukrainian partners on Russian intelligence services' cyber operations.

The cooperation between the State Service of Special Communications and Information Protection of Ukraine and the Cybersecurity and Infrastructure Security Agency of US Department of Homeland Security was noted. Attention was also paid to the Framework Agreement on the Strategic Foundations of Defense Partnership signed by the Ministers of Defense of Ukraine and the United States which allows developing cooperation in the areas of cyber defense and development of cyber troops, protection of critical information infrastructure. This cooperation in the field of cyber defense pursues the goal of deterring harmful cyber activities against national security systems, the development of medical capabilities, and cooperation in the field of countering disinformation.

Relevant proposals for improving the fight against cybercrime in Ukraine are presented. In particular, on the creation in Ukraine of a special website for reporting cybercrime - Internet Crime Complaint Center following the example of the American center - Internet Crime Complaint Center (IC3); using the experience of the United States in terms of creating «hybrid» squads for countering and combating cybercrime; creation of focus groups of national law enforcement agencies with the private sector to address the problems of cybercrime in Ukraine.

Key words: *US Federal Bureau of Investigation, US Secret Service, cybercrime, security, countermeasures.*

Стаття надійшла до редколегії 9 січня 2023 року