DOI https://doi.org/10.51647/kelm.2020.3.4.33

WYKORZYSTANIE DOŚWIADCZEŃ ZAGRANICZNYCH W ZAKRESIE TECHNICZNO-KRYMINALISTYCZNEGO ZABEZPIECZENIA DOCHODZENIA W SPRAWIE PRZESTĘPSTW ZWIĄZANYCH Z UŻYTKOWANIEM KOMPUTERÓW, SYSTEMÓW I SIECI KOMPUTEROWYCH ORAZ SIECI TELEKOMUNIKACYJNYCH

Bronislav Teplytskyi
pierwszy zastępca dyrektora Państwowego Naukowo-Badawczego Centrum Ekspercko-Kryminalistycznego Ministerstwa Spraw Wewnętrznych Ukrainy (Kijów, Ukraina)
ORCID ID: 0000-0002-0126-6782
e-mail: Bronislav_Teplytskyi@gmail.com

Adnotacja. W artykule omówiono międzynarodowe doświadczenia głównych krajów świata w dziedzinie działalności publicznej dotyczące prawnych mechanizmów regulujących ochronę informacji w nowoczesnych warunkach, przeciwdziałania cyberprzestępczości, zapewniania dochodzeń w sprawie przestępstw w zakresie korzystania z komputerów, systemów i sieci komputerowych oraz sieci telekomunikacyjnych. W szczególności podano i przeanalizowano organizację takich działań w Stanach Zjednoczonych Ameryki, Kanadzie, Francji i Niemczech. Skupiono się na jednostkach głównych, których działalność związana jest z przeciwdziałaniem cyberprzestępczości, wskazano ich zadania. Koncentruje się na głównych dokumentach normatywnych i prawnych, które mają na celu zapewnienie walki z tego rodzaju przestępstwami.

Słowa kluczowe: informacje, bezpieczeństwo informacji, dochodzenie, cyberprzestępczość, Federalne Biuro Śledcze, bezpieczeństwo narodowe, Interpol, cyberobrona.

USE OF FOREIGN EXPERIENCE TECHNICAL AND CRIMINAL PROVISION OF CRIME INVESTIGATION IN THE FIELD OF USE OF COMPUTERS, SYSTEMS AND COMPUTER NETWORKS AND TELECOMMUNICATIONS

Bronislav Teplytsky
First Deputy Director of the State Research
forensic center of the Ministry of Internal Affairs of Ukraine (Kyiv, Ukraine)
ORCID ID: 0000-0002-0126-6782
e-mail: Bronislav_Teplytskyi@gmail.com

Abstract. The article examines the international experience of the world's leading countries in the field of state activity on legal mechanisms for regulating the protection of information in modern conditions, combating cybercrime, ensuring the investigation of crimes in the use of computers, systems and computer networks and telecommunications networks. In particular, the organization of such activities in the United States of America, Canada, in such countries of the European Union as France and Germany is presented and analyzed. Emphasis is placed on the main units involved in cybercrime and their tasks are outlined. The focus is on the main legal documents that are designed to combat these types of crimes.

Key words: information, information security, investigation, cybercrime, Federal Bureau of Investigation, national security, Interpol, cyber defense.

ВИКОРИСТАННЯ ЗАРУБІЖНОГО ДОСВІДУ ТЕХНІКО-КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ КОМП'ЮТЕРІВ, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Броніслав Теплицький
перший заступник директора Державного науково-дослідного експертно-криміналістичного центру МВС України (Київ, Україна)
ORCID ID: 0000-0002-0126-6782
e-mail: Bronislav_Teplytskyi@gmail.com

Анотація. У статті розглянуто міжнародний досвід провідних країн світу у сфері державної діяльності щодо правових механізмів регулювання захисту інформації в сучасних умовах, протидії кіберзлочинності, забезпечення розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. Зокрема, наведено та проаналізовано організацію такої діяльності у Сполучених Штатах Америки, Канаді, Франції та Німеччині. Акцентовано увагу на головних підрозділах, діяльність яких пов'язана з протидією

кіберзлочинності, окреслено їх завдання. Зосереджено увагу на головних нормативно-правових документах, які покликані забезпечувати боротьбу з такими видами злочинів.

Ключові слова: інформація, інформаційна безпека, розслідування, кіберзлочинність, Федеральне бюро розслідувань, національна безпека, Інтерпол, кіберзахист.

Вступ. Серед сучасних тенденцій розвитку суспільства варто зазначити глобальну інформатизацію практично всіх сфер життєдіяльності людини. Крім прямої шкоди від можливих випадків несанкціонованого доступу до інформації, її модифікації або знищення, інформатизація може перетворитися на джерело серйозної загрози державній безпеці і правам людини. Для підвищення ефективності боротьби з кіберзлочинністю Україна досить давно почала здійснювати, необхідні заходи для створення власної стратегії кібербезпеки. Верховною Радою України зроблено спробу врегулювати відносини, що виникають у кіберпросторі, а саме ухвалено Закон України «Про основні засади забезпечення кібербезпеки в Україні». Незважаючи на ці кроки, Україна постійно стає жертвою кібератак, у зв'язку з чим питання протидії кіберзлочинності набуває особливої актуальності.

Питання забезпечення кібербезпеки та протидії кіберзлочинності неодноразово ставали предметом наукових дискусій і досліджень. Так, зазначену проблематику відображено у працях таких вітчизняних учених та науковців, як В.Б. Авер'янов, О.Ф. Андрійко, О.М. Бандурка, В.Ю. Баскаков, В.В. Береза, К.І. Бєляков, О.В. Бойченко, В.М. Бутузов, В.В. Василевич, В.П. Горбулін, С.М. Гусаров, І.В. Діордіца, Є.В. Додін, О.Ю. Дрозд, М.Г. Каращук, Н.В. Коваленко, Т.О. Коломоєць, В.К. Колпаков, А.Т. Комзюк, О.Є. Користін, В.І. Куріло, А.М. Лобода, В.А. Ліпкан, Ю.Є. Максименко, В.В. Марков, Л.В. Могілевський, О.М. Музичук, А.М. Новицький, О.П. Орлюк, О.Ю. Салманова, Р.Ю. Сень, О.Ю. Синявська, Т.Л. Сироїд, В.С. Сідак, В.В. Сокуренко, В.О. Тімашов, В.В. Чернєй, В.В. Чумак, Д.В. Швець, О.В. Шепета та ін.

Наразі недостатньо уваги приділено діяльності спеціалізованих державних, зокрема міжнародних, органів та організацій у сфері протидії кіберзлочинності як сучасного виду злочинності в Україні та за кордоном. Саме тому питання вивчення і запозичення міжнародного досвіду провідних країн світу у сфері державної діяльності щодо правових механізмів регулювання захисту інформації в сучасних умовах, протидії кіберзлочинності, забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку є недостатньо дослідженим та потребує наукового вивчення.

Метою статті є вивчення та аналіз закордонного досвіду техніко-криміналістичного забезпечення розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку для подальшого удосконалення боротьби з кіберзлочинністю в Україні.

Результати дослідження. Першою країною, що прийняла відповідний закон та створила Національну стратегію безпеки в кіберпросторі, є Сполучені Штати Америки. Причиною написання цього документа стала терористична атака 11 вересня 2001 р. Стратегія була частиною більш загальної Стратегії забезпечення національної безпеки (National Strategy for Homeland Security). Крім того, за оцінками фахівців, саме в США щорічно втрати корпорацій від злочинності перевищують 200 млрд, а від комп'ютерних злочинів – 6 млрд дол., тому питання боротьби з кіберзлочинністю для цієї країни є надзвичайно актуальним (Youtsen, 1987: 57).

Водночас особлива увага приділяється функціонуванню такого органу в США, як Федеральне бюро розслідувань, що є головним суб'єктом забезпечення кібербезпеки держави та протидії кіберзлочинності на всій території США. ФБР є провідним федеральним агентством США з розслідування кібератак, що вчиняють злочинці, зарубіжні противники і терористи. При ФБР створено інтернет-центр скарг на кіберзлочини, місією якого є розгляд скарг на злочин в Інтернеті, надання громадськості надійного і зручного механізму звітності про підозрюваних, схеми шахрайства з використанням Інтернету і створення ефективних альянсів з правоохоронними органами та галузевими партнерами. Інформація аналізується і поширюється зі слідчою і розвідувальною метою серед співробітників правоохоронних органів і для інформування громадськості (The Cyber Threat, 2019).

У Бюро по боротьбі з тероризмом функціонують і такі групи: 1) Об'єднана оперативна група з питань тероризму та кіберзлочинності (розслідує факти кіберзлочинності та тероризму, що вчиненні на території штату Нью-Йорк, здійснюють систематизацію вчинених злочинів та їх аналіз); 2) група забезпечення кібербезпеки Нижнього Манхеттена (призначена виявляти та попереджувати загрози кібератак і тероризму на території Нижнього Манхеттена); 3) група з аналізу ризиків та загроз тероризму і кіберзлочинності (здійснює заходи стратегічної розвідки щодо виявлення кібератак і загроз тероризму та здійснює їх аналіз) (Білобров, 2020: 97).

Новелою в 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, що існують в Інтернеті, і сприяти запобіганню злочинам стосовно дітей). Він просуває кібергроматні ідеї та положення серед студентів, залучаючи їх до веселої, відповідної віку, конкурентоспроможної онлайн-програми, де вони вчаться безпечному і відповідальному використанню Інтернету. Аналогічні програми існують у Латвії (Чумак, 2015: 146).

З метою обміну інформацією, ФБР спростило свою систему відстеження та управління погрозами Guardian для захищеного інформаційного порталу, що дозволяє окремим партнерам у галузі повідомляти про інциденти, пов'язані з кіберзлочинністю, у режимі реального часу (Борьба с преступностью в Интернете (онлайновая преступность, 2006: 136).

Отже, у США для ефективної боротьби з кіберзлочинністю та забезпечення кібербезпеки держави створено належне правове поле діяльності спеціалізованих суб'єктів боротьби з кіберзлочинністю та дієву систему органів, головними функціями визначено забезпечення кіберзахисту та протидії всім проявам кіберзлочинності, що суттєво впливає на стан правопорядку в державі (Чумак, 2015: 114).

Одним із важливих напрямів діяльності поліції Канади є боротьба з комп'ютерними і телекомунікаційними злочинами, розслідування яких здійснює підрозділ Королівської канадської кінної поліції (федеральної поліції, КККП) з боротьби з комп'ютерною злочинністю. Секція захисту інформаційних технологій забезпечує захист федеральних державних комп'ютерних центрів, приватного сектора, надає консультації, готує персонал для роботи зі здійснення комп'ютерного захисту. Співробітники підрозділу допомагають поліцейським у проведенні розслідувань злочинів, пов'язаних з комп'ютерними системами (Варунц, 2012: 74). Зважаючи на те, що завдання, які стоять перед підрозділами поліції з боротьби з комп'ютерною злочинністю, мають міжнародний характер і не є специфічними для Канади, вони активно співпрацюють з іншими країнами та Інтерполом з метою вдосконалення законодавства у цьому напрямі (Маланчук, 2020: 103).

Поряд із США та Канадою активно протидіють кіберзлочинності в країнах Європейського Союзу, де створено необхідний нормативно-правовий фундамент з питань захисту кіберпростору (Петровський, Лівчук, 2019: 56). Стратегію кібербезпеки ЄС прийнято в 2013 р. Її особливістю є те, що стратегією охоплено різні аспекти кіберпростору, зокрема, внутрішній ринок, правосуддя, внутрішня та зовнішня політика. Разом із Стратегією розроблено та прийнято законодавчу пропозицію щодо посилення безпеки інформаційних систем ЄС (Чумак, 2018: 152).

Міністр внутрішніх справ Франції Мішель Алліот-Марі 14 лютого 2008 р. оприлюднив французьку Стратегію з питань боротьби з кіберзлочинністю. Мета Стратегії – співпраця між приватним бізнесом та правоохоронними органами з обміну інформацією та вирішення питань щодо об'єднання зусиль у боротьбі з кіберзлочинністю.

У 2015 р. Франція прийняла Національну стратегію інформаційної безпеки, що спрямована на супровід переходу французького суспільства до цифрових технологій і на вирішення нових завдань, пов'язаних зі зміною використання цифрових технологій і викликаними цим погрозами. Стратегію доповнили: 1) Міжнародна стратегія Франції в галузі інформаційних технологій (2017 р.), у якій узагальнено стратегічні цілі в галузі інформаційних технологій у трьох основних сферах: управлінні, економіці і безпеці; 2) Стратегічний огляд з питань кіберзахисту (2018 р.), у якому визначено доктрину управління кіберкрізісами, роз'яснено цілі національної стратегії в галузі кіберзахисту (Бутузов, 2007: 316).

На технічному й оперативному рівні ефективності французької системи сприяє низка учасників, зокрема: Французьке агентство безпеки інформаційних систем (ANSSI), створене в 2009 р., є національним органом, що відповідає за кібербезпеку; Міністерство збройних сил, що виконує подвійну місію із захисту мереж, які забезпечують його діяльність, і з інтеграції цифрової протидії у військових операціях; Міністерство внутрішніх справ, що протидіє усім формам кіберзлочинності, спрямованої як проти національних установ й інтересів, господарюючих суб'єктів і державних органів, так і проти фізичних осіб.

Крім того, протягом останніх декількох років Франція повністю переформатувала свої пріоритети у галузі оборони й національної безпеки. Так, «Біла книга з питань національної оборони і безпеки» 2008 р. була першим основоположним документом, адресованим виключно проблематиці національних кіберзагроз як основного ризику для національної безпеки і суверенітету. У ній визначалися нові пріоритети, такі як запобігання і реагування на кібератаки, а також передбачалися інституційні зміни, необхідні для забезпечення національної безпеки (Гавловський, Тітуніна, 2009: 40).

Штаб з кіберзахисту Франції (COMCYBER) є оперативним підрозділом, створеним у 2017 р., що здійснює оперативний нагляд за майже 3400 кіберкомбатантами в міністерстві. Для виконання своїх місій Штаб має штат і повноваження над трьома спільними організаціями: CALID, CASSI і CPROC (Жевелєва, 2014: 143).

Відтак з метою забезпечення кібербезпеки держави у Франції створено належну нормативно-правову базу функціонування уповноважених на забезпечення кібербезпеки держави органів. При цьому захист кібернетичного простору та протидія кіберзлочинності вважаються пріоритетом для забезпечення національної безпеки Франції та здійснюються не лише органами поліції (жандармерії), а й Міністерством оборони та спеціально створеними органами (Чумак, 2015: 118).

На наше переконання, особливу увагу доцільно приділити дослідженню позитивного досвіду протидії кіберзлочинності, як у Німеччині, що є однією з провідних держав-членів ЄС. Саме Німеччина продемонструвала прихильність пріоритету забезпечення безпеки і боротьби щодо протидії кіберзлочинності, підписавши (у 2001 р.) і ратифікувавши (у 2009 р.) Міжнародну конвенцію Ради Європи про кіберзлочини, також відому як Будапештська конвенція, здійснивши низку заходів для її реалізації в країні. Німеччина підписала і ратифікувала Додаткові протоколи до Конвенції про кіберзлочини, які криміналізують расистську і ксенофобську діяльність, здійснювану за допомогою комп'ютерних систем (Киберготовность Германии 2.0: киберпреступность и охрана правопорядка, 2017).

Так, у липні 2015 р. в Німеччині прийнято Акт про інформаційну безпеку (IT Security Act), метою якого є запобігання шкоди найважливішим IT-системам, таким, наприклад, як системи Міністерства внутрішніх справ (BSI), провайдерів телекомунікаційних послуг, операторів критично важливих елементів інфраструктури та ін. Нині BSI здійснює реалізацію положень цього Акта, що включає в себе мінімальні стандарти кібербезпеки для понад 2000 критично важливих інфраструктурних компаній.

Водночас у Німеччині діють й інші закони, що забороняють такі злочинні дії, як комп'ютерне шахрайство, фальсифікація даних, комп'ютерний саботаж, кібершпигунство, фішинг, а також інші подібні кіберзлочину, за які, відповідно до національного законодавства, передбачено покарання, як і за звичайні злочини (Киберготовность Германии 2.0: киберпреступность и охрана правопорядка, 2017). Щодо правоохоронної діяльності в Німеччині створені достатні умови для протидії різним видам кіберзлочинності. NCAZ, BSI і BKA спільно працюють щодо протидії кіберзлочинності в національному масштабі. Зокрема, NCAZ об'єднує ресурси різних урядових агентств, зокрема Федеральної поліції і Федеральної розвідувальної служби, а також приватного сектору.

У лютому 2019 р. інформаційне агентство Agence France-Presse повідомило, що Німеччина вступила до лав країн НАТО та надала Альянсу власні кіберможливості в боротьбі з кіберзламами та електронною війною (Германия поделится с НАТО своими кибервозможностями, 2019).

Отже, у Німеччині для забезпечення кібербезпеки держави створено низку спеціальних органів, зокрема кібернетичну авіацію, що є важливою складовою протидії кіберзлочинності.

З метою посилення кібербезпеки країн Європейського Союзу Єврокомісія запропонувала у вересні 2017 р. пакет заходів, що включає створення Агентства з кібербезпеки ЄС і введення сертифікатів для продукції, що випускається в ЄС, цифрової продукції і послуг.

На сьогодні зазначене Агентство успішно функціонує на території країн-членів ЄС та, відповідно до Стратегії ЄС, у своїй діяльності керується також прийнятою Директивою ЄС з інформаційної безпеки (Директива (ЕС) 2016/1148 Европейского парламента и Совета, 2016).

Крім того, на початку березня 2020 р. шість європейських країн підписали угоду для створення загальних кібернетичних військ, очолюваних Литвою. Так, Естонія, Литва, Хорватія, Польща, Нідерланди та Румунія в Загребі підписали меморандум про взаєморозуміння. Відповідно до угоди, у всіх цих країнах буде створено міжнародні команди, готові відповісти на кібератаку в будь-який час. Меморандум на законних підставах дозволяє використовувати ці сили в юрисдикціях різних країн, визначає механізм роботи команд, їх правовий статус, роль і процедури (Эстония, Польша, Хорватия, Нидерланды, Румыния и Литва создали общие кибернетические войска, 2020.).

Висновки. Сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу до глобального інформаційного простору. Саме тому необхідно використовувати досвід країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки, оскільки вона є невід'ємним напрямом побудови інформаційного суспільства, розвиток якого повинен відбуватися не лише через нарощування технологічних можливостей здійснення інформаційного обміну, а й через глибоке усвідомлення всіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо захисту інформаційних ресурсів та забезпечення безпеки держави, беручи до уваги зарубіжний досвід протидії кіберзлочинності у сфері забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку. Переконані, що удосконалення техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку має відбуватися з урахуванням національних культурно-історичних, соціально-економічних особливостей країни на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн у сфері боротьби з кіберзлочинністю з метою оптимального входження у європейське та світове правове поле.

Список використаних джерел:

1. Білобров Т.В. Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України: дис. … канд. юрид. наук: 12.00.07. Київ, 2020. 209 с.
2. Борьба с преступностью в Интернете (онлайновая преступность). Інформаційний бюлетень Міжвід. наук.-дослід. центру з проблем боротьби з орг. злочинністю. 2006. № 7. С. 133–141.
3. Бутузов В.М. Сучасні загрози: комп'ютерний тероризм. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2007. № 17. С. 316–325.
4. Варунц Л.Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні: дис. канд. юрид. наук: 12.00.07. Дніпропетровськ, 2012. 203 с.
5. Гавловський В.Д., Тітуніна К.В. Актуальні питання міжнародного співробітництва у боротьбі з комп'ютерною злочинністю. Організація протидії у сфері інтелектуальної власності та комп'ютерних технологій: доповіді провідних вчених, представників громадськості, державних службовців та працівників підрозділів ДСБЕЗ на міжвід. семінарі. Київ, 2009. С. 36–42.
6. Германия поделится с НАТО своими кибервозможностями. SecurityLab.ru. 2019. Новости. URL: https://www.securitylab.ru/news/497967.php.
7. Директива (ЕС) 2016/1148 Европейского парламента и Совета от 6 июля 2016 г. о мерах по обеспечению высокого общего уровня безопасности сетевых и информационных систем в рамках Союза. Доступ к законодательству Европейского Союза. URL: https://eurlex.europa.eu/eli/dir/2016/1148/oj.
8. Жевелєва І.С. Зарубіжний досвід взаємодії правоохоронних органів із суб'єктами господарювання у процесі захисту інформації з обмеженим доступом. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2014. № 1. С. 140–145.

9. Кіберготовность Германии 2.0: киберпреступность и охрана правопорядка. Digital. 2017. URL: https://digital.report/kibergotovnostgermanii-2-0-kiber-prestupnost-i-ohrana-pravoporyadka/
10. Маланчук П.М. Порівняння боротьби з кіберзлочинністю в Україні та зарубіжних країнах. Актуальні проблеми вітчизняної юриспруденції. 2020. № 1. С. 101–104.
11. Петровський О.М., Лівчук С.Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. Молодий вчений. 2019. № 12.1 (76.1). С. 55–59.
12. Чумак В.В. Організаційно-правові засади діяльності KNAB Латвії та ДБР України: порівняльний аналіз. Роль та місце правоохоронних органів у розбудові демократичної правової держави: матеріали XI міжнар. наук.-практ. інтернет-конф, (Одеса, 25 берез. 2019 р.). Одеса, 2018. С. 60–61.
13. Чумак В.В. 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. (Львів, 17 груд. 2015 р.) / МВС України; Львів. держ. ун-т внутр. справ. Львів, 2015. С. 146–149.
14. Эстония, Польша, Хорватия, Нидерланды, Румыния и Литва создали общие кибернетические войска. Tadviser. 2020. URL: https://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Европа
15. The Cyber Threat. FBI. 2019. URL: https://www.fbi.gov/investigate/cyber
16. Youtsen M. Research on European Juvenile Delinquency. HEUNI Publication Series. 1987. № 7. С. 57−62.

References:

1. Bilobrov, T.V. (2020). Administratyvno-pravovyi status Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy [Administrative and legal status of the Cyber Police Department of the National Police of Ukraine]: dys. … kand. yuryd. nauk: 12.00.07. Kyiv, 209 p. [in Ukrainian].
2. Borba s prestupnostiu v Internete (onlainovaia prestupnost) [Fighting crime on the Internet (online crime)]. Informatciinii biuleten Mizhvid. nauk.-doslid. tcentru z problem borotbi z org. zlochinnistiu. 2006. № 7. pp. 133–141. [in Russian].
3. Butuzov, V.M. (2007). Suchasni zahrozy: kompiuternyi teroryzm [Current threats: computer terrorism]. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka). № 17. pp. 316–325. [in Ukrainian].
4. Varunts, L.D. (2012). Dosvid orhanizatsii diialnosti Korolivskoi kanadskoi kinnoi politsii ta shliakhy yoho vykorystannia v Ukraini [Experience in organizing the activities of the Royal Canadian Mounted Police and ways to use it in Ukraine]: dys. kand. yuryd. nauk: 12.00.07. Dnipropetrovsk. 203 p. [in Ukrainian].
5. Havlovskyi, V.D., Titunina, K.V. (2009). Aktualni pytannia mizhnarodnoho spivrobitnytstva u borotbi z kompiuternoiu zlochynnistiu. [Current issues of international cooperation in the fight against cybercrime]. Orhanizatsiia protydii u sferi intelektualnoi vlasnosti ta kompiuternykh tekhnolohii: dopovidi providnykh vchenykh, predstavnykiv hromadskosti, derzhavnykh sluzhbovtsiv ta pratsivnykiv pidrozdiliv DSBEZ na mizhvid. seminari. Kyiv. pp. 36–42. [in Ukrainian].
6. Germaniia podelitsia s NATO svoimi kibervozmozhnostiami [Germany will share its cyber capabilities with NATO]. SecurityLab.ru. 2019. Novosti. URL: https://www.securitylab.ru/news/497967.php. [in Russian].
7. Direktiva (ES) 2016/1148 Evropeiskogo parlamenta i Soveta ot 6 iiulia 2016 g. o merakh po obespecheniiu vysokogo obshchego urovnia bezopasnosti setevykh i informatcionnykh sistem v ramkakh Soiuza [Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high overall level of security for network and information systems within the Union]. Dostup k zakonodatelstvu Evropeiskogo Soiuza. URL: https://eurlex.europa.eu/eli/dir/2016/1148/oj. [in Russian].
8. Zhevelieva, I.S. (2014). Zarubizhnyi dosvid vzaiemodii pravookhoronnykh orhaniv iz subiektamy hospodariuvannia u protsesi zakhystu informatsii z obmezhenym dostupom. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka). № 1. pp. 140–145. [in Ukrainian].
9. Kibergotovnost Germanii 2.0: kiberprestupnost i okhrana pravoporiadka [Germany Cyber Readiness 2.0: Cybercrime and Law Enforcement]. Digital. 2017. URL: https://digital.report/kibergotovnostgermanii-2-0-kiber-prestupnost-i-ohrana-pravoporyadka/ [in Russian].
10. Malanchuk, P.M. (2020). Porivniannia borotby z kiberzlochynnistiu v Ukraini ta zarubizhnykh krainakh [Comparison of the fight against cybercrime in Ukraine and foreign countries]. Aktualni problemy vitchyznianoi yurysprudentsii. № 1. pp. 101–104. [in Ukrainian].
11. Petrovskyi, O.M., Livchuk, S.Iu. (2019). Problemy borotby z kiberzlochynnistiu: mizhnarodnyi dosvid ta ukrainski realii [Problems of combating cybercrime: international experience and Ukrainian realities]. Molodyi vchenyi. № 12.1 (76.1). pp. 55–59. [in Ukrainian].
12. Chumak, V.V. (2018). Orhanizatsiino-pravovi zasady diialnosti KNAB Latvii ta DBR Ukrainy: porivnialnyi analiz [Organizational and legal bases of activity of KNAB of Latvia and DBR of Ukraine: the comparative analysis]. Rol ta mistse pravookhoronnykh orhaniv u rozbudovi demokratychnoi pravovoi derzhavy: materialy KhI mizhnar. nauk.-prakt. internet-konf, (Odesa, 25 berez. 2019 r.). Odesa. pp. 60– 61. [in Ukrainian].
13. Chumak, V.V. (2015). Osnovni napriamy ta osoblyvosti orhanizatsii diialnosti politsii Latvii [The main directions and features of the organization of activity of police of Latvia]. Problemy zastosuvannia informatsiinykh tekhnolohii, spetsialnykh tekhnichnykh zasobiv u diialnosti OVS ta navchalnomu protsesi: materialy nauk.-prakt. konf. (Lviv, 17 hrud. 2015 r.) / MVS Ukrainy; Lviv. derzh. un-t vnutr. sprav. Lviv, 2015. S. 146–149. [in Ukrainian].
14. Estoniia, Polsha, Khorvatiia, Niderlandy, Rumyniia i Litva sozdali obshchie kiberneticheskie voiska [Estonia, Poland, Croatia, Netherlands, Romania and Lithuania have created common cybernetic troops]. Tadviser. 2020. URL: https://www.tadviser.ru/index.php/Statia:Kiberprestupnost_i_kiberkonflikty_:_Evropa [in Russian].
15. The Cyber Threat. FBI. 2019. URL: https://www.fbi.gov/investigate/cyber [in English].
16. Youtsen, M. (1987). Research on European Juvenile Delinquency. HEUNI Publication Series № 7. pp. 57−62. [in English].