УДК 343.3/.7
DOI https://doi.org/10.32782/2524-0374/2021-9/49

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: ВИКЛИКИ СУЧАСНОСТІ

CYBERCRIMES IN UKRAINE: THE CHALLENGES OF THE PRESENT

Никончук Н.С., студентка IV курсу
Інститут прокуратури та кримінальної юстиції
Національного юридичного університету імені Ярослава Мудрого

Маслова О.О., к.ю.н.,
асистент кафедри кримінального права № 1
Національний юридичний університет імені Ярослава Мудрого

Надзвичайно швидкий розвиток технологій створює нові можливості у використанні інформаційного простору, які тягнуть за собою і нові загрози в цій сфері. Такий стрімкий розвиток, своєю чергою, вимагає ефективного державного регулювання у сфері запобігання та протидії кіберзлочинності.

Стаття присвячена дослідженню сучасного стану кіберзлочинності в Україні шляхом визначення викликів та загроз у сфері кібербезпеки України.

Також у статті автор визначає поняття «кіберзлочинність», «кіберпростір», «кібербезпека», виокремлює основні критерії класифікації кіберзлочинів через призму наукової доктрини та міжнародно-правових актів, досліджує державно-правовий механізм протидії кіберзлочинності в Україні.

Проаналізовано міжнародно-правові акти та законодавство України у сфері боротьби з кіберзлочинністю. Конвенція про кіберзлочинність від 23 листопада 2001 року, яку Україна ратифікувала у 2005 році, зіграла значну роль у розвитку нормативно-правового регулювання кіберзлочинності в Україні. Серед нормативно-правових актів України, що регулюють питання боротьби з кіберзлочинністю, відзначені Стратегія кібербезпеки України від 27 січня 2016 року та від 14 травня 2021 року, а також Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року, який став основою розвитку державної системи захисту в зазначеній сфері.

Основна увага зосереджена на дослідженні проявів кіберзлочинності та кібератак на світовому рівні, зокрема тих, які торкнулися українського інформаційного простору.

Саме тому, враховуючи зростання кількості кібератак, необхідним є не лише дослідження світових тенденцій розвитку кіберзлочинності, ефективне нормативно-правове забезпечення, а й створення системи заходів для захисту та попередження кіберзлочинності шляхом визначення викликів та загроз у сфері кібербезпеки України.

Ключові слова: кіберзлочин, кіберзлочинність, цифровий простір, кібератака, CIA-злочини, загрози, виклики.

The extremely rapid development of an information-aware society requires the effective regulation of the state policy in the field of combating cybercrime. The rapid development of technology creates new opportunities in the use of information space, but new opportunities entail new threats in this area.

The article is devoted to the study of the current state of cybercrime in Ukraine by identifying challenges and threats in the field of cybersecurity in Ukraine.

The author of the article studies the concept and essence of cybercrime. The main criteria for classifying cybercrime are determined through the prism of scientific doctrine and international legal acts. Cybercrime is divided into types depending on the basis of the classification and its purpose and can have both forensic, and criminological or criminal law significance. The article examines the state-legal mechanism of counteraction to cybercrime in Ukraine. The analysis of international legal acts and legislation of Ukraine in the field of combating cybercrime is made, the conclusion is drawn on the need to improve national legislation and establish international cooperation in the development of mechanisms to counter cybercrime and minimize its negative consequences. Crimes provided for in the Convention are enshrined in different chapters of the Criminal Code of Ukraine.

The cybercrime place and role in national cyber security are determined. The main focus is concentrated on the study of cybercrime manifestations and cyberattacks activity on a global level, as well as those which have occurred in Ukrainian information space.

According to the growing number of cyberattacks in the world, it is necessary not only research of global cybercrime trends, creation of the effective legal support, but also measures to prevent and protect against cybercrime.

Key words: cybercrimes, cybercrime, cyberterrorism, cyberattacks, threats, challenges.

Постановка проблеми. На сучасному етапі свого розвитку ми перебуваємо в стані трансформаційних перетворень. Інтернет, комп'ютери, мобільні телефони та інші цифрові технології здійснили революцію у всіх сферах людського життя за останні декілька десятиліть, тобто повністю змінили наше життя, включаючи те, як ми спілкуємося, здійснюємо банківські операції, робимо покупки, дізнаємося новини, розважаємося тощо. Наприклад, Україна стала першою у світі державою, де цифрові паспорти прирівняні до паперових і пластикових. Проте всі ці технічні досягнення відкрили і нові можливості для вчинення різних правопорушень у цифровому просторі, які часто називають кіберзлочинністю, адже правопорушник використовує спеціальні знання про кіберпростір.

Кожного року вчиняються десятки тисяч злочинів з використанням інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання, кожного дня у людей та компаній крадуть персональні дані, кошти з рахунків, збирають безліч конфіденційної та комерційної інформації, блокують діяльність тощо.

Україна, як і всі країни світу, щодня зіштовхується з такими викликами, адже тільки за останні декілька років державні установи неодноразово були піддані кібератакам. Наприклад, однією з таких атак був запуск у 2017 році різновиду вірусу «Petya», який спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Внаслідок атаки була заблокована діяльність таких підприємств, як: аеропорт «Бориспіль», ЧАЕС, «Укртелеком», «Укрпошта», «Ощадбанк», «Укрзалізниця» і так далі. Також були заражені інформаційні системи Міністерства інфраструктури, Кабінету міністрів, сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та служби спецзв'язку України [1].

Або ж, відповідно до повідомлення прес-центру Служби безпеки України від 19 жовтня 2020 року: «Служба безпеки України з початку року нейтралізувала 460 кіберінцидентів і кібератак на органи державної влади

та критично важливі об'єкти інфраструктури. Також за цей період заблоковано 2,5 тисячі вебресурсів, які використовувалися зі злочинною метою, та діяльність 20 хакерських угруповань» [2].

Саме тому поняття «кіберзлочинності» дедалі більше турбує фахівців з інформаційної безпеки, адже наразі запобігання таких правопорушень, їх викриття та притягнення винних осіб до відповідальності є доволі складним процесом.

Аналіз останніх досліджень і публікацій. Поняття «кіберзлочинності» стало об'єктом дослідження у працях багатьох українських та зарубіжних науковців, зокрема, таких як Д.С. Азаров, П.Д. Біленчук, В.А. Глушков, Н.А. Гуторова, Н.В. Карчевський, Н.І. Хавронюк, В.І. Алескеров, В.Б. Вехов, М.А. Єфремова, В.А. Кемпф тощо, і нині дедалі більше турбує вчених та фахівців у сфері інформаційної безпеки.

Метою статті є дослідження поняття кіберзлочинності, а також аналіз сучасного стану кіберзлочинності в Україні шляхом визначення викликів та загроз у сфері кібербезпеки України.

Виклад основного матеріалу. Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі – відповідно до п. 5 ч.1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», прийнятого 5 жовтня 2017 року (набув чинності 9 травня 2018 року). Цей закон визначає основні напрями та цілі державної політики у сфері кібербезпеки, закріплює повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері та основні засади координації їхньої діяльності із забезпечення кібербезпеки. Проте слід зазначити, що в Законі відсутні правові інструменти для його практичного застосування під час здійснення кібератак [3].

Термін «кіберзлочин» є відносно молодим для науки кримінального права, який утворений сполученням двох слів: **«кібер»** (розуміється як «кіберпростір», «віртуальний світ», «інформаційний простір») і **«злочин»**.

Під поняттям **«кіберзлочину»** слід розуміти соціальне явище, що являє собою навмисну мотивовану атаку з використанням мережі Інтернет на інформацію в комп'ютерній системі, програми або дані, що чиниться окремою особою або угрупуваннями, яке має суспільну небезпеку для суспільного ладу України, його політичної й економічної системи, власності, особі, політичним, трудовим, майновим та іншім правам і свободам громадян [4, с. 166].

Важливим аспектом правопорушень у кіберпросторі є їхній нелокальний характер, що створює серйозні проблеми для правоохоронних органів, адже національні злочини, які раніше мали місцеве значення, зараз потребують міжнародної співпраці. Тому більшість держав зацікавлені в зупиненні дій, пов'язаних з витоком персональних даних своїх громадян в мережу Інтернет, та зменшенні кібератак, які перешкоджають роботі органів державної влади, підприємств, установ, організацій, банків тощо.

Нормативно-правове підґрунтя для боротьби з кіберзлочинністю в Україні становлять: Конституція України, Кримінальний кодекс України, Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та ін., Доктрина інформаційної безпеки України від 2017 р., Конвенція Ради Європи про кіберзлочинність, Додатковий протокол до неї та ін. міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

7 вересня 2005 року Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність, яка була прийнята з метою співробітництва й координації діяльності правоохоронних органів різних держав у сфері протидії комп'ютерним злочинам. Конвенція виокремлює чотири групи злочинів, які пов'язані з використанням комп'ютерних технологій. До **першої** групи належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (так звані «CIA-злочини»), зокрема, це:

– незаконний доступ – навмисний доступ до цілої комп'ютерної системи або її частини без права на це з метою отримання комп'ютерних даних або з іншою недобросовісною метою (ст. 2 Конвенції);

– нелегальне перехоплення – протиправне перехоплення технічними засобами комп'ютерних даних (ст. 3 Конвенції);

– втручання в дані – навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації без права на це (ст. 4 Конвенції);

– втручання в систему – навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це (ст. 5 Конвенції);

– зловживання пристроями, а саме: їх виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином (ст. 6 Конвенції) [5].

До **другої** групи унаслідено правопорушення, пов'язані з використанням комп'ютерів, включаючи підробку й шахрайство:

– підробка, пов'язана з комп'ютерами – введення, зміна, знищення або приховування комп'ютерних даних, що призводить до створення недійсних даних з метою, щоб вони розглядались наче справжні, незалежно від того, можна чи ні їх прочитати чи зрозуміти (ст. 7 Конвенції);

– шахрайство з використанням комп'ютерів – позбавлення іншої особи її власності шляхом введення, зміни, знищення чи приховування комп'ютерних даних або втручання у функціонування комп'ютерної системи (ст. 8 Конвенції).

До **третьої** групи – правопорушення, пов'язані зі змістом (інформацією), зокрема, дитяча порнографія (ст. 9 Конвенції), акти расизму та ксенофобії (ст. 3 Додаткового протоколу до Конвенції) [6].

До **четвертої** групи, своєю чергою, належать правопорушення, пов'язані з порушенням авторських і суміжних прав відповідно до чинних міжнародних угод (наприклад, Бернської Конвенції про захист літературних та художніх творів та ін.) (ст. 10 Конвенції) [5].

У багатьох інших регіональних міжнародно-правових актах передбачено криміналізацію й інших злочинних діянь, які не отримали такого загального визнання, але закріплені в окремих угодах, зокрема, це: правопорушення, пов'язані з расизмом та ксенофобією; правопорушення, пов'язані з геноцидом та злочинів проти людства; злочини, пов'язані з тероризмом; злочини проти приватності; незаконне використання електронних платіжних засобів і т.д.

Рівень кіберзлочинності в Україні останнім часом також швидко зростає. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Росією, Бразилією, Китаєм та меншою мірою – Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування [7, с. 16–25].

Зростання кіберзлочинності в національному сегменті кіберпростору є масштабною загрозою, яка завдає шкоди державним інформаційним ресурсам, суспільним процесам, особисто громадянам, що знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення інших злочинів (проти основ національної безпеки, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми, незаконного обігу

зброї, наркотичних засобів та інших предметів і речовин, які загрожують життю та здоров'ю людей). Ситуація ускладнюється через низький рівень кіберграмотності населення, зокрема пересічних користувачів електронних послуг [8, с. 9].

Передумовами та чинниками, які формують **загрози** у сфері кібербезпеки України, є:

– недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

– відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;

– відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;

– відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

– незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

– відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [8, с. 11].

Викликами для України у сфері кібербезпеки є:

– активне використання кіберзасобів у міжнародній конкуренції за світове лідерство, змагальний характер розвитку засобів кібербезпеки та реалізації кіберзагроз у процесі швидких прогресуючих змін інформаційно-комунікаційних технологій, хмарних обчислень, 5G-мереж, великих даних, Інтернету речей, машинного навчання/штучного інтелекту (AI) тощо;

– мілітаризація кіберпростору та зростаючі технологічні можливості кіберзброї, які дають можливість здійснювати приховане проведення противником кібератак та кібероперацій, віддаленого взяття під контроль систем управління, завдання шкоди та руйнування критичної інформаційної інфраструктури;

– зростання технологічного рівня протиправних посягань на інтереси держави, суспільства та окремих громадян із застосуванням методів соціальної інженерії, використання технологій штучного інтелекту та криптотехнологій;

– вплив на економічну діяльність та соціальну поведінку поширення пандемії COVID-19, що спричинило швидку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем. Це посилило загрозу порушення прав громадян під час використання кіберпростору [8, с. 7].

Відповідно до Стратегії розвитку кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року [9], головним органом, що відповідає за інформаційну безпеку, є підрозділ Національної поліції – кіберполіція. Крім того, обов'язки щодо протидії кіберзлочинності покладаються на Міністерство оборони України, Державну службу спеціального зв'язку та захисту інформації України, Службу безпеки України, Національний банк України, розвідувальні органи.

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [9].

Стратегія розвитку кібербезпеки України передбачає, що основними напрямами забезпечення безпеки у кіберпросторі України є:

– розвиток безпечного, стабільного і надійного кіберпростору, тобто створення єдиної нормативно-правової бази і доведення її до широких мас із метою підвищення рівня обізнаності населення;

– кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, тобто вироблення ефективної методики протидії на рівні державних і місцевих органів;

– кіберзахист критичної інфраструктури - передбачає розроблення єдиного механізму державно-приватного партнерства у запобіганні кіберзагрозам;

– розвиток потенціалу сектору безпеки й оборони у всі попередні категорії і зв'язування їх у єдиний комплекс, тобто створення умов для впровадження в Україні сучасних технологій кіберзахисту [10, с. 184];

Тобто, враховуючи всі позитивні та негативні аспекти, за умовами Стратегії Україна повинна утворити велику високотехнічну систему для забезпечення надійності і безпеки зв'язку в інформаційній сфері.

Реалізовуючи Стратегію кібербезпеки України на 2016–2020 роки, наша держава змогла сформувати ядро національної системи кібербезпеки, наростила потенціал, який дає можливість здійснювати подальшу розбудову національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії.

Крім того, з 2018 року в Україні запрацювала Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка функціонує в рамках Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України, та до досягнень якої можна віднести їх спільно зі Службою зовнішньої розвідки України виявлення нової модифікації шкідливого програмного забезпечення типу Pterodo на комп'ютерах державних органів України яка, ймовірно, є підготовчим етапом для проведення кібератаки. Такий вірус збирає дані про системи, регулярно відправляє їх на командно-контрольні сервери й очікує подальших команд. Зокрема, CERT-UA під час дослідження інформації про кіберінциденти (за останніми даними від 03.03.2021) спостерігає збільшення кількості кібератак з використанням шкідливого програмного забезпечення Pterodo хакерського угрупування Armageddon/Gamaredon, яке пов'язують з урядом РФ [11].

Крім того, активно розвивається і співпраця з іноземними партнерами, поглиблюється співробітництво України з ЄС та НАТО, проводяться кібернавчання за участю інших держав та міжнародних організацій.

Так, наприклад, правоохоронними органами України, США, Великої Британії, Японії, Філіппін, Індонезії, Малайзії було проведено такі операції:

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

– «Зевс», завданням якої було знешкодження міжнародної організованої злочинної групи, котра з метою викрадення фінансових реквізитів і доступу до банківських рахунків розповсюджувала шкідливе програмне забезпечення «Зевс». Під час операції знешкоджено інфраструктуру в мережі, що включала понад 40 тис. інфікованих комп'ютерів і серверів, левова частка яких знаходилась на території України. Спричинені збитки понад 300 млн доларів. Члени організованого злочинного

угруповання – хакери з Одеси та Харкова на чолі з громадянином Російської Федерації [12, с. 68].

Відповідно, пріоритетами забезпечення кібербезпеки України є: *убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки* [8, с. 11].

Висновки. Сучасний рівень інформатизації суспільства вимагає від України забезпечити належний та ефективний механізм боротьби із кіберзлочинами як однієї з серйозних загроз національній безпеці держави. Така потреба стає ще більш очевидною, враховуючи транснаціональний характер цих злочинів, що вимагає від правоохоронних органів України ще більш якісних технічного забезпечення та компетентності для здійснення належної співпраці як у рамках, зокрема, міжнародного співробітництва під час кримінальних проваджень цієї категорії справ, так і загалом у питаннях протидії кіберзлочинності.

Україна має необхідний потенціал для нарощування спроможностей у сфері кібербезпеки для адекватної протидії сучасним викликам і загрозам.

ЛІТЕРАТУРА

1. Нікулеско Д. Ера нових видів злочинів. *Юридична газета online : Всеукраїнське юридичне професійне видання.* 2019. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (дата звернення: 24 квітня 2021 р.)

2. 460 кібератак і 20 хакерських угруповань нейтралізувала СБУ з початку року. *Служба безпеки України* : веб-сайт. URL: https://ssu.gov.ua/novyny/460-kiberatak-i-20-khakerskykh-uhrupovan-neitralizuvala-sbu-z-pochatku-roku (дата звернення: 24 квітня 2021 р.)

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. *Законотворчість : база даних / Верховна Рада України*. URL: https://zakon.rada.gov.ua/ laws/show/2163-19 (дата звернення: 24 квітня 2021 р.)

4. Кирбят'єв О.О. Комп'ютерні злочини: реалії сучасності, проблеми боротьби з ними та ймовірні шляхи їх вирішення. *Вісник Запорізького національного університету*. 2010. № 1. С. 165–170. URL: http://web.znu.edu.ua/herald/issues/2010/Ur-1-2010/165-170.pdf (дата звернення: 24 квітня 2021 р.)

5. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001. *Законотворчість : база даних / Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/994_575/ (дата звернення: 22 квітня 2021 р.)

6. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Протокол Ради Європи від 28.01.2003. *Законотворчість : база даних / Верхов. Рада України*. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення: 25 квітня 2021 р.)

7. 29. Довбиш М.О. Кіберзлочинність в Україні. *«Наука – от теории к практике»* : матеріали Міжнар. наук. конф. (Сопот, Польща, 29.03.13 р.). Сопот : ТОВ «БТТ». 2013. С. 16–25.

8. Проєкт «Стратегія кібербезпеки України на 2021–2025 роки». *Рада національної безпеки і оборони України* : веб-сайт. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 25 квітня 2021 р.)

9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. *Законотворчість : база даних / Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/92/2016#Text (дата звернення: 24 квітня 2021 р.)

10. Яцик Т. П., Кисла К. О., Пушкарьова Т. М. Кіберзлочинність в Україні: аналіз дієвості способів розлідування кіберзлочинів і напрями їх вдосконалення. *Юридичний науковий електронний журнал.* № 1. 2019. С. 184-186. URL: http://www.lsej.org.ua/1_2019/51.pdf (дата звернення: 24 квітня 2021 р.)

11. Поновлення кібератак з використанням ШПЗ Pterodo хакерського угрупування Armageddon/Gamaredon 2021. *Computer Emergency Response Team of Ukraine.* URL: https://cert.gov.ua/article/10702 (дата звернення: 26 квітня 2021 р.)

12. Демедюк С.В., Демедюк Т.С. Міжнародний досвід протидії кіберзлочинності. *Вісник ХНУВС*. 2014. № 4 (67). С. 65–75. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/6023/Mizhnarodnyi%20dosvid%20protydii%20kiberzlochynnosti_%20Demediuk%20SV_Demediuk_2014.pdf?sequence=1&isAllowed=y (дата звернення: 24 квітня 2021 р.)