УДК 343.9
Федоров М. П., *к. ю. н., професор,*
професор кафедри кримінального права
та процесу, Львівський торговельно-економічний
університет, м. Львів.

ПРОБЛЕМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Анотація. *У статті досліджується державно-правовий механізм протидії кіберзлочинності в Україні. Аналізуються основні положення чинних законодавчих та інших підзаконних актів. Що регулюють відносини у сфері захисту прав та законних інтересів держави, юридичних та фізичних осіб від злочинних посягань у інформаційно-цифровій сфері. Розглядається діяльність державних органів та їх структур, що спеціалізуються на питаннях забезпечення інформаційної та кібербезпеки держави та її суб'єктів.*

Результатом проведеного дослідження є сформульовані обґрунтовані пропозиції щодо вдосконалення чинного законодавства України у сфері кіберзахисту, покращення діяльності спеціалізованих державних органів, що протидіють кіберзагрозам.

Ключові слова: кіберзлочинність, кіберзлочин, кібербезпека, кібератака, кіберзахист, критична інфраструктура.

M. P. Fedorov,
Ph.D., professor, professor of the department of criminal law and process, Lviv University of Trade and Economics, Lviv.

PROBLEMS OF CIBERCULARITY IN UKRAINE

Abstract. *The article examines the state-legal mechanism of counteraction to cybercrime in Ukraine. The main provisions of the current legislative and other subordinate acts are analyzed. Regulating relations in the sphere of protection of rights and legitimate interests of the state, legal entities and individuals from criminal encroachments in the information and digital sphere. The activity of state bodies and their structures specializing in issues of information and cyber security of the state and its subjects is considered.*

The result of the research is the formulation of substantiated proposals to improve the current legislation of Ukraine in the field of cyber defense, and improve the activities of specialized state agencies that counteract cyber threats.

Keywords: cybercrime, cybercrime, cyber security, cyberattack, cyber defense, critical infrastructure.

DOI: https://doi.org/10.36477/2616-7611-2018-07-24

Постановка проблеми. Проблема забезпечення інформаційної безпеки є актуальною з часу, коли люди розпочали обмінюватися інформацією, накопичувати її, зберігати, аналізувати та використовувати. У сучасному суспільстві проблема інформаційної безпеки особливо актуальна. Оскільки інформація стала невід'ємною важливою частиною його життя. Розвиток сучасного суспільства визначається глобальними інформаційними процесами. Сучасні цифрові інформаційні технології застосовуються в усіх без винятку сферах суспільного життя. Суспільний прогрес завдячує цифровим технологіям, конвергенції та глобалізації комп'ютерних мереж. Інформація стала вартісним товаром, який можна продати, придбати, обміняти, а то й викрасти чи незаконно використати.

Комп'ютерні мережі та електронна інформація використовуються також і для здійснення кримінальних правопорушень. Розвиток інформаційно-комунікаційних технологій супроводжується винайденням нових способів кібератак та шахрайства в мережі Інтернет. Безпека кіберпростору стала пріоритетною складовою міжнародної політики.

За оцінками експертів у сфері кібербезпеки провідних країн світу відзначається стійка тенденція до значного зростання кількості та збільшення різновидів кібератак на державні інформаційні ресурси, зокрема на такі, що забезпечують діяльність об'єктів критичної інформаційної інфраструктури, з метою порушення їх конфіденційності, цілісності і доступності.

Експерти впевнені, що саме кіберзлочинність в недалекому майбутньому стане світовою загрозою номер один, переважить тероризм, наркоторгівлю та інші найбільш поширені сьогодні злочини. Сьогодні немає розроблених ефективних методик прогнозування можливого стану кіберзлочинності, її рівня й структури навіть на кілька років наперед. Не можна передбачити які й проти чого будуть спрямовані руйнівні кібератаки, а відповідно й запобігти їм. Значні фінансово-економічні збитки або інші непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем безпосередньо впливають на стан національної безпеки і оборони держави.

Злочини у кіберпросторі виявилися серйозною проблемою для розвинених країн. За даними Комісії з внутрішніх справ Палати громад парламенту Великобританії, глобальна економіка щороку втрачає $388 млрд. Це значно більше, ніж збитки від обігу наркотиків [1].

Захищеність та надійність інформаційних систем та комп'ютерних мереж є необхідною умовою ефективного функціонування державного апарату та його складових, діяльності господарюючих суб'єктів, безпечного життя окремих людей.

Питання забезпечення кібербезпеки є надзвичайно актуальними і для України. У 2017 році, за статистичними даними Генеральної прокуратури України, було зареєстровано 2573 злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (статті 361–363-1 КК), із них 1272 злочини, у яких

винним особам було вручено повідомлення про підозру. За 9 місяців 2018 року ці цифри склали 2017 і 1414 відповідно [2].

Доводиться констатувати, що, у нашій державі заходи протидії кіберзлочинності, передбачені законодавчими та іншими нормативно-правовими актами Уряду є недостатньо ефективними. У зв'язку з цим, існуючі кіберзагрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки, удосконалення нормативно-правового забезпечення, структури та методів діяльності всього державно-правового механізму України щодо протидії кіберзагрозам.

Аналіз останніх досліджень і публікацій. Дослідженням окремих проблем безпеки держави, її об'єктів критичної інфраструктури в кіберпросторі присвячені праці П. П. Андрушка, А. Андрощук, І. В. Арістової П. С. Берзіна, Ю. Р Гарасима, В. Д. Гулкевича, Б. А. Кормича С. Я. Лихової, О. Е. Радутного, Д. В. Супацького, С. О. Харламової та інших науковців. У своїх працях автори формулюють авторське бачення сучасного стану і шляхів удосконалення забезпечення, переважно, інформаційної безпеки держави та інших суб'єктів, охорони інтелектуальної власності в Україні. Пропонують заходи щодо використання кращого досвіду діяльності правоохоронних органів зарубіжних країн у цьому напрямі в Україні. Разом з тим, недостатньо уваги приділяється питанням удосконалення державно-правового механізму щодо протидії саме кіберзлочинності в Україні.

Постановка завдання. Метою даної статті є розмежування понять "інформаційний злочин", "комп'ютерний злочин" та "кіберзлочин", "інформаційна безпека" та "кібербезпека", виявлення проблем забезпечення кібербезпеки держави від злочинних посягань та формулювання обґрунтованих пропозицій щодо вдосконалення державно-правового механізму протидії кіберзлочинності.

Виклад основного матеріалу дослідження.

З початком масового застосування комп'ютерів проблема інформаційної та кібербезпеки набула особливої гостроти. Доступ до Інтернету зріс із неймовірною швидкістю: з 16 мільйонів користувачів у 1995 р. до понад 2 мільярдів сьогодні. Розширення мережевого світу є в інтересах усіх держав: за оцінками, на кожні 10 % зростання доступу до Інтернету припадає в середньому 1,3 % зростання глобального ВВП. Кожного року товарообіг в електронній комерції в усьому світі складає 8 трильйонів доларів США [3]. Віртуальний світ не знає державних кордонів. Відкритий кіберпростір розширює можливості людей, їх спільнот, держав, збагачує суспільство, сприяє світовому прогресу через обмін науковою та технічною інформацією, сприяє товарообміну та торгівлі.

З розвитком технічного прогресу, завдяки відсутності віртуальних кордонів між державами, у злочинців з'являється дедалі більше можливостей і вчиняти злочини, і приховувати їх сліди та перешкоджати пошуку злочинців. Стрімко зростає кількість та потужність кібератак, вмотивованих інтересами певних держав, злочинних груп та окремих осіб.

Світова спільнота, стурбована криміналізацією кіберпростору, розробляє заходи протидії кіберзлочинності. Так, 23 листопада 2001 року Рада Європи прийняла Конвенцію про кіберзлочинність (далі — Конвенція) [4]. Верховна Рада України ратифікувала Конвенцію із застереженнями та заявами 7 вересня 2005 року і вона набрала чинності для України 1 липня 2006 року. 28 січня 2003 року був прийнятий Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Додатковий протокол до Конвенції був ратифікований Верховною Радою України із застереженням 21 липня 2006 року, і він набрав чинності для України 1 квітня 2007 року.

2 грудня 2002 року Генеральна Асамблея ООН своєю резолюцією 57/239 затвердила "Елементи для створення глобальної культури кібербезпеки". Цей документ містить дев'ять основних вимог, яких мають дотримуватися і враховувати держави, створюючи власні системи кібербезпеки. Такими вимогами є: 1) обізнаність; 2) відповідальність; 3) реагування; 4) етика; 5) демократія; 6) оцінювання ризиків; 7) проектування і впровадження засобів забезпечення безпеки; 8) управління забезпеченням безпеки; 9) переоцінка [5].

Питання захисту кіберпростору є надзвичайно актуальними для України, яка стала жертвою воєнної агресії з боку Росії. Кібератакам, ініційованим російськими спецслужбами піддаються різні об'єкти критичної інфраструктури України: урядові органи, банківські установи, об'єкти енергетики та транспорту тощо. В Україні створений і діє державно-правовий механізм протидії кіберзлочинності, який включає законодавчі та інші нормативно-правові акти щодо забезпечення кібербезпеки, систему органів, що безпосередньо розробляють і реалізують заходи щодо кіберзахисту, форми та методи протидії кіберзагрозам. Розглянемо детальніше кожну із складових механізму протидії кіберзлочинності.

15 березня 2016 року Указом президента України № 96/216 була затверджена Стратегія кібербезпеки України (далі — Стратегія) — документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Основними завданнями держави у цьому напрямі, згідно зі Стратегією, є:

– створення національної системи кібербезпеки;

– посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;

– забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан

національної безпеки і оборони України (критична інформаційна інфраструктура) [6].

Кабінет Міністрів України розробляє та затверджує щорічні плани заходів з реалізації Стратегії кібербезпеки України, контролює їх виконання.

5 жовтня 2017 р. Верховна Рада України прийняла Закон України "Про основні засади забезпечення кібербезпеки України". Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [7].

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Закон України "Про основні засади забезпечення кібербезпеки України" та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Аналіз чинного законодавства та інших нормативно-правових актів України, що регламентують питання забезпечення кібербезпеки держави, дозволяє зробити висновок про відповідність їх основних положень рекомендаціям Конвенції про кіберзлочинність 2001 року та Додаткового протоколу до неї.

Наступним елементом державно-правового механізму забезпечення кібербезпеки в Україні є система суб'єктів забезпечення кібербезпеки.

Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Робочим органом РНБО є Національний координаційний центр кібербезпеки, який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, що забезпечують кібербезпеку, вносить Президентові України пропозиції щодо вдосконалення Стратегії кібербезпеки України.

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки.

Суб'єктами, які безпосередньо здійснюють заходи із забезпечення кібербезпеки, є міністерства та інші центральні органи виконавчої влади, місцеві державні адміністрації, органи місцевого самоврядування, правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти

оперативно-розшукової діяльності, Збройні Сили України та інші військові формування, утворені відповідно до закону, Національний банк України, підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури, суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [7].

Серед державних органів, що розробляють і здійснюють заходи щодо забезпечення кібербезпеки держави, об'єктів критичної інфраструктури слід назвати, у першу чергу, спеціалізовані органи: Державна служба спеціального зв'язку та захисту інформації України, до складу якої входить Державний центр кіберзахисту та протидії кіберзагрозам; Національний координаційний центр кібербезпеки, який є робочим органом Ради національної безпеки і оборони України; кіберполіція у складі Національної поліції України (Департамент кіберполіції Національної поліції України та територіальні управління (Київське, Слобожанське, Донецьке, Придніпровське, Причорноморське, Карпатське, Поліське і Подільське управління)).

Державний центр кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України (далі — ДЦКЗ) — державна організація, створена для здійснення впровадження організаційно-технічної моделі кіберзахисту як складової Національної системи конфіденційного зв'язку України.

Серед завдань Державного центру кіберзахисту — забезпечення функціонування команди реагування на комп'ютерні надзвичайні події України CERT-UA, а також проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах органів державної влади. Крім того, ДЦКЗ відповідає за функціонування, безпеку та розвиток Національної системи конфіденційного зв'язку, функціонування та розвиток системи антивірусного захисту інформації для органів державної влади, забезпечення функціонування та модернізації Системи захищеного доступу до мережі Інтернет органів державної влади України та Захищеного вузла Інтернет-доступу Держспецзв'язку.

ДЦКЗ також займається впровадженням новітніх і перспективних технологій в інформаційно-телекомунікаційних системах, проведенням експертиз комплексних систем захисту інформації та засобів захисту інформації в органах державної влади, а також експертиз програмних, апаратних і програмно-апаратних засобів у сфері захисту інформації. Центр адмініструє та модернізує Реєстр інформаційно-телекомунікаційних систем державних органів [8].

У складі ДЦКЗ функціонує спеціалізований структурний підрозділ — Команда реагування на комп'ютерні надзвичайні події України (англ. Computer Emergency Response Team of Ukraine, CERT-UA) для забезпечення кіберзахисту та протидії кіберзагрозам. CERT-UA є акредитованим членом

FIRST (англ. Forum for Incident Response and Security Teams, FIRST) та активно взаємодіє з аналогічними командами в усьому світі.

2 лютого 2018 року у складі Державного центру кіберзахисту та протидії кіберзагрозам Держспецзв'язку відкрито новий підрозділ — Центр реагування на кіберзагрози (англ. Cyber Threat Response Centre — CRC). Основною діяльністю підрозділу є забезпечення кіберзахисту органів державної влади та об'єктів критичної інформаційної інфраструктури України [9].

Наведений вище перелік державних інституцій, що спеціалізуються на виявленні та протидії кіберзагрозам доповнюється структурними підрозділами банківських установ, об'єктів критичної інфраструктури різних форм власності, що спеціалізуються на виявленні та протидії кібератакам на відповідні об'єкти та усуненні їх шкідливих наслідків.

Таким чином, державно-правовий механізм протидії кіберзлочинності в Україні вже створений, але констатувати наявність належного рівня кібербезпеки ще передчасно. Як свідчить статистика, рівень розкриття злочинів у кіберпросторі нижчий за 50 %. До того ж, слід урахувати, що до офіційної статистики потрапляє не більше чверті кібератак, які вчиняються щодо українських об'єктів. Три чверті вчинених кіберзлочинів — це латентна злочинність. Потерпілі від кіберзлочинів, особливо це стосується фінансово-банківських установ, вважають за краще приховати факт успішної кібератаки, ніж втратити ділову репутацію та клієнтуру через розголос події злочину. До того ж, має місце недовіра у суспільстві до правоохоронних органів, сумніви щодо професіоналізму та елементарної порядності їх працівників.

У міжнародних актах, чинному законодавстві України терміни "інформаційний простір", "віртуальний простір", "інформаційний злочин", "кіберзлочин", "кіберзлочинність", "кібератака", "кіберзагроза", "кібербезпека", "інформаційна безпека" тощо використовуються досить часто, але подекуди у ці поняття вкладають різний зміст.

У Конвенції про кіберзлочинність, незважаючи на таку її назву, відсутнє визначення понять "кіберзлочин" та "кіберзлочинність".

Зі змісту Преамбули Конвенції можна зрозуміти, що кіберзлочинами є дії, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними.

У II Розділі Конвенції (статті 2–10) визначений перелік правопорушень, що є кіберзлочинами. Такими, зокрема, є злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний умисний доступ до цілої комп'ютерної системи або її частини без права на це; умисне нелегальне перехоплення технічними засобами, без права на це, передач комп'ютерних даних, які не є призначеними для публічного користування, які проводяться з, на або всередині комп'ютерної системи, включаючи електромагнітні випромінювання комп'ютерної системи, яка містить в собі такі комп'ютерні дані; втручання у дані: навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; втручання у систему: навмисне серйозне перешкоджання функціонуванню

комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це; зловживання пристроями: навмисне вчинення, без права на це: a) виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином: 1) пристроїв, включаючи комп'ютерні програми, створених або адаптованих з метою вчинення кіберзлочинів; 2) комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення кіберзлочинів; та b) володіння цим пристроєм з наміром його використання для вчинення кіберзлочинів).

Кіберзлочинами, відповідно до статей 7–8 Конвенції, є й правопорушення, пов'язані з комп'ютерами (навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп'ютерних даних, яке призводить до створення недійсних даних з метою того, щоб вони вважались або відповідно до них проводилися б законні дії, як з дійсними, незалежно від того, можна чи ні такі дані прямо прочитати і зрозуміти; шахрайство, пов'язане з комп'ютерами: навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, без права на це, економічних переваг для себе чи іншої особи).

Злочинними також є діяння, пов'язані з протиправним змістом інформації, що розповсюджується (дитяча порнографія тощо) та з порушенням авторських і суміжних прав [4].

Аналіз ІІ розділу Конвенції та Додаткового протоколу до неї показує, що до кіберзлочинів відносяться як умисні протиправні дії, що становлять небезпеку в кіберпросторі, так і інші суспільно-небезпечні дії, де комп'ютер є лише знаряддям учинення злочинів (шахрайство, порушення авторських і суміжних прав, розповсюдження матеріалів порнографічного, расистського, ксенофобського характеру тощо).

У Кримінальному кодексі України (далі — КК) передбачена кримінальна відповідальність за порушення авторського права і суміжних прав (ст. 176 КК); за незаконний обіг дисків для лазерних систем зчитування, матриць, обладнання та сировини для їх виробництва (ст. 203-1 КК); за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК); несанкціоновані дії з інформацією, яка оброблюється в електронно-

обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК); Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК) [10].

Аналіз чинного Кримінального Закону України показує, що розділ XVI КК України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" містить 6 статей, які передбачають кримінальну відповідальність, переважно, за протиправне втручання в нормальну роботу комп'ютерних мереж та систем. Назва цього розділу КК не зовсім відповідає його змісту. Сфера використання комп'ютерів настільки широка, що охоплює усі без винятку сфери суспільного життя. Кіберпростір є "полем діяльності" торговців зброєю, людьми та наркотиками, різного роду шахраїв, творців шкідливого програмного контенту, комп'ютерних піратів тощо. Через комп'ютерні мережі поширюється контрафактна продукція, твори порнографічного змісту, лунають заклики до вчинення дій, що загрожують громадському порядку, до вчинення терористичних актів, чиняться адресні погрози політикам та підприємцям тощо.

У Законі України "Про основні засади забезпечення кібербезпеки України" (далі — Закон) зроблена спроба на законодавчому рівні дати визначення основних понять, що стосуються кібербезпеки.

Кіберзлочин (комп'ютерний злочин) — суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [7, п. 8, ст. 1].

Вказане визначення не конкретизує об'єкт посягання, яким можуть бути будь-які суспільні відносини, тобто під це поняття можна підвести якщо не всі, то більшість злочинів Особливої частини КК. Через Інтернет здійснюються, наприклад, фінансові операції, легалізуються злочинні доходи, приховуються чи перекручуються відомості про екологічний стан і безліч інших злочинних дій, для вчинення яких використовується окремий комп'ютер чи їх мережа. Бажано було б вказати в якості об'єкта цього виду злочинів суспільні відносини щодо забезпечення діяльності об'єктів критичної інфраструктури.

Не витримує критики і наведене у Законі визначення поняття "кіберзлочинність": кіберзлочинність — сукупність кіберзлочинів [7, п. 9, ст. 1].

У наведеному вище визначенні поняття “кіберзлочин” вказується, що кіберзлочин вчиняється у кіберпросторі або з його використанням. Далі дається наступне визначення цього поняття: кіберпростір — середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [7, п. 11, ст. 1]. Це визначення є не тільки неконкретним. а й використовує для тлумачення терміни, ще складніші для розуміння, ніж поняття “кіберпростір”.

У Законі дається також визначення терміна “кібербезпека”: кібербезпека — 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. У першій частині визначення йдеться про життєво важливі інтереси людини і громадянина, а в кінці — забезпечується своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз тільки національній безпеці України.

Доводиться констатувати, що рівень кібербезпеки в Україні вкрай низький. І це стосується не тільки окремої людини чи суб’єкта господарювання, а й об’єктів критичної інфраструктури, від нормального функціонування яких залежить безпека держави. Так, наприклад, у 2017 році в Україні від кібератаки вірусом NotPetya постраждали понад 80 % підприємств. Відбуваються постійні кібератаки на об’єкти енергетики та транспорту України. Кількість таких кібератак зросла з часу військового конфлікту між Україною та Російською Федерацією. Окрім наземних бойових дій ведеться війна у кіберпросторі, так як за більшістю кібератак на українські об’єкти стоять спецслужби Росії.

Уразливість об’єктів критичної інфраструктури України від кібератак обумовлюється рядом обставин, серед яких виділяють правові, організаційно-технічні та криміналістичні проблеми забезпечення кібербезпеки.

До правових проблем, насамперед, слід віднести недосконаліть чинного Кримінального Закону України. Більшість статей XVI розділу КК України, які передбачають кримінальну відповідальність за вчинення кіберзлочинів, можуть бути застосовані лише в разі заподіяння злочином певної шкоди (витік, втрата. підробка, блокування інформації, порушення чи припинення роботи електронно-обчислювальних машин тощо). Доцільно у диспозиції цих статей передбачити формальний склад злочину і передбачити кримінальну відповідальність за злочинні діяння у кіберпросторі незалежно від реального настання шкідливих наслідків.

Низький рівень розкриття виявлених кіберзлочинів зумовлений також відсутністю окремих криміналістичних методик розслідування кіберзлочинів.

Слідчі не мають у своєму розпорядженні ні науково обґрунтованих рекомендацій щодо виявлення та розслідування злочинів цього виду, ні практичного досвіду, ні належної фахової підготовки.

У Кримінальному процесуальному кодексі України в статті 99 зазначається, що документами в якості речових доказів можуть бути електронні носії інформації, проте немає конкретних вказівок, що слід під ними розуміти, не визначені умови допустимості таких доказів, тобто не враховуються особливості кіберпростору як сфери вчинення кіберзлочинів.

Не останнє місце серед детермінант кіберзлочинності відіграє віктимна поведінка потенційних жертв злочинів. Насамперед, це повсюдне використання неліцензійного програмного забезпечення. Пірати наповнили кіберпростір різноманітними програмами зі зламаним захистом, кодами, паролями тощо. Одночасно в таких програмах інстальовані шкідливі програми у вигляді вірусів, троянів, хробаків тощо. Така, на перший погляд, "безкоштовна" програма, інфікована вірусом чи іншою шкідливою програмою завдає значної шкоди користувачу, надаючи доступ до комп'ютера стороннім особам, викрадаючи паролі, рахунки, знищуючи чи спотворюючи важливу інформацію, блокуючи чи сповільнюючи роботу комп'ютера тощо.

Значна частина користувачів комп'ютерної техніки легковажно ставиться до її антивірусного захисту. Використовує малоефективні безкоштовні, або знову ж таки "зламані", а тому не без "сюрпризів" антивірусні програми.

На багатьох об'єктах, у тому числі й на об'єктах критичної інфраструктури не тільки використовують неліцензійне програмне забезпечення, а й довіряють технічне обслуговування комп'ютерних мереж та їх захист від кібератак недостатньо компетентним або з невисокими морально-етичними якостями працівникам. Як свідчить статистика, значна частина кібератак чи витік конфіденційної інформації вчиняється безпосередньо чи за сприянням таких осіб.

Слід враховувати також ту обставину, що значна частина вузькоспеціалізованого програмного забезпечення, яке використовується в Україні на важливих з погляду національної безпеки об'єктах, розроблялася в Російській Федерації. Немає впевненості, що безпосередньо в цих програмах чи програмах їх оновлення програмісти на завдання відповідних російських спецслужб не заклали якийсь шкідливий "бонус". Відомий випадок з американо-іракської війни, коли всі літаки "Міраж", продані Іраку Францією, "раптом випадково" не змогли піднятися в повітря для ведення бойових дій. У літаків одночасно відмовила вся електроніка. Хто, звідки й який подав сигнал, який вивів з ладу авіацію Хусейна, можна лише здогадуватися. Тому слід негайно відмовитися від використання такого програмного забезпечення, яке у критичний момент виведе з ладу об'єкти критичної інфраструктури держави.

Висновки і перспективи подальших досліджень у даному напрямі. З метою забезпечення належного рівня кіберзахисту різних об'єктів, а

особливо об'єктів критичної інфраструктури, на наш погляд, необхідно здійснити такі заходи:

1) внести зміни до чинного законодавства України, зокрема до Кримінального та Кримінального процесуального кодексів України, які б враховували особливості кіберпростору як "місця" вчинення кіберзлочинів;

2) розробити окремі криміналістичні методики розслідування кіберзлочинів, використовувати їх у процесі виявлення. розкриття та розслідування злочинів у кіберпросторі;

3) розробити власне, вітчизняне програмне забезпечення різного виду та призначення, стимулювати його використання різними користувачами взамін неліцензійного, чи розробленого спеціалістами з недружніх держав;

4) налагодити систему підготовки та перепідготовки спеціалістів з питань кібербезпеки;

5) здійснити перерозподіл функцій та повноважень між правоохоронними органами держави щодо запобігання, виявлення, розкриття, розслідування кіберзлочинів, протидії та усунення шкідливих наслідків кібератак;

6) налагодити тісну взаємодію правоохоронних та інших органів держави щодо забезпечення ефективного кіберзахисту;

7) забезпечити розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, зокрема щодо видів кібератак та ефективних способів протидії цим злочинам.

У подальших дослідженнях у даному напрямі автор розгляне результати діяльності органів держави, що спеціалізуються на забезпеченні кібербезпеки та протидії кіберзлочинності з метою виявлення проблем і недоліків у їх діяльності та формулювання обґрунтованих пропозицій щодо її покращення.

Література:

1. Кіберзлочинність виявилася для світової економіки збитковішою від наркоторгівлі [Електронний ресурс]. — Режим доступу : https://ua.korrespondent.net/business/web/1587043-kiberzlochinnist-viyavilasya-dlya-svitovoyi-ekonomiki-zbitkovishoyu-vid-narkotorgivli
2. Генеральна прокуратура України [Електронний ресурс]. — Режим доступу: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113281&libid=100820&c=edit&_c=fo
3. Вільям Хейг: ніхто не контролює Інтернет, і ми не можемо залишити майбутнє напризволяще [Електронний ресурс]. — Режим доступу : https://gurt.org.ua/news/recent/12223/
4. Конвенція про кіберзлочинність від 23 листопада 2001 р. / Рада Європи // Офіційний вісник України. — 2007. — № 65. — Ст. 2535.

5. Елементи для створення глобальної культури кібербезпеки від 20 грудня 2002 р. [Електронний ресурс]. — Режим доступу: http://zakon.rada.gov.ua/laws/show/995_b42
6. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України” : Указ від 15 березня 2016 р. / Президент України // Офіційний вісник України. — 2016. — № 23. — Ст. 899.
7. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. / Верховна Рада України // Відомості Верховної Ради України. — 2017. — № 45. — Ст. 403.
8. У Держспецзв’язку створено Державний центр кіберзахисту та протидії кіберзагрозам [Електронний ресурс]. — Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=156473&cat_id=119123
9. Державний центр кіберзахисту та протидії кіберзагрозам [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%B8%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%82%D0%B0_%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0%D0%BC
10. Кримінальний кодекс України : Закон України від 5 квітня 2001 р. // Відомості Верховної Ради України. — 2001. — № 25–26. — Ст. 131.

References:

1. Kiberzlochynnist' vyiavylasia dlia svitovoi ekonomiky zbytkovishoiu vid narkotorhivli [Elektronnyj resurs]. — Rezhym dostupu : https://ua.korrespondent.net/business/web/1587043-kiberzlochinnist-viyavilasya-dlya-svitovoyi-ekonomiki-zbitkovishoyu-vid-narkotorgivli
2. Heneral'na prokuratura Ukrainy [Elektronnyj resurs]. — Rezhym dostupu: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113281&libid=100820&c=edit&_c=fo
3. Vil'iam Khejh: nikhto ne kontroliuie Internet, i my ne mozhemo zalyshyty majbutnie napryzvoliasche [Elektronnyj resurs]. — Rezhym dostupu : https://gurt.org.ua/news/recent/12223/
4. Konventsiia pro kiberzlochynnist' vid 23 lystopada 2001 r. / Rada Yevropy // Ofitsijnyj visnyk Ukrainy. — 2007. — № 65. — St. 2535.
5. Elementy dlia stvorennia hlobal'noi kul'tury kiberbezpeky vid 20 hrudnia 2002 r. [Elektronnyj resurs]. — Rezhym dostupu: http://zakon.rada.gov.ua/laws/show/995_b42
6. Pro rishennia Rady natsional'noi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku “Pro Stratehiiu kiberbezpeky Ukrainy” : Ukaz vid 15 bereznia 2016 r. / Prezydent Ukrainy // Ofitsijnyj visnyk Ukrainy. — 2016. — № 23. — St. 899.

7. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 5 zhovtnia 2017 r. / Verkhovna Rada Ukrainy // Vidomosti Verkhovnoi Rady Ukrainy. — 2017. — № 45. — St. 403.
8. U Derzhspetszv'iazku stvoreno Derzhavnyj tsentr kiberzakhystu ta protydii kiberzahrozam [Elektronnyj resurs]. — Rezhym dostupu: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=156473&cat_id=119123
9. Derzhavnyj tsentr kiberzakhystu ta protydii kiberzahrozam [Elektronnyj resurs]. — Rezhym dostupu: https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%B8%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%82%D0%B0_%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B0%D0%BC
10. Kryminal'nyj kodeks Ukrainy : Zakon Ukrainy vid 5 kvitnia 2001 r. // Vidomosti Verkhovnoi Rady Ukrainy. — 2001. — № 25–26. — St. 131.