УДК 342.7

Шемчук В.В.
Кваліфікаційно-дисциплінарна комісія прокурорів

КІБЕРЗЛОЧИННІСТЬ ЯК ПЕРЕШКОДА РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ

У статті розкрито сутність кіберзлочинності, підходи до розуміння даного поняття, класифікації кіберзлочинів, інших протиправних діянь у даній сфері. Визначено проблеми, здобутки і перспективи протидії і боротьби з кіберзлочинністю на шляху розбудови громадянського інформаційного суспільства, входження України у світовий інформаційний простір,

Ключові слова: *інформаційне суспільство, кіберзлочинність, інформація, кіберзлочини, кібербезпека, законодавство.*

Постановка проблеми. В умовах гібридної війни, тотального використання засобів масової інформації та її комунікаційних складових частин особливої актуальності набуває попередження основних загроз кіберзлочинності. Як свідчать результати наукових досліджень, проблематика кіберзлочинності непокоїть не тільки державу в цілому, а й окремих господарюючих суб'єктів, практично кожну особу.

Кіберзлочинність – неминучий наслідок глобалізації інформаційних процесів і, як наслідок, є основною загрозою соціогуманітарної та інших компонентів. Зростаюча кількість кіберзлочинної діяльності на підприємствах, постійне вдосконалення інформаційних технологій і нові можливості «вдосконалення» інструментів їх скоєння створюють економічні загрози для глобальних інформаційних мереж.

Аналіз останніх досліджень та публікацій. Окремі аспекти розвитку та становлення інформаційних відносин, питання здійснення протидії кіберзлочинності розглядались провідними вітчизняними науковцями: М.О. Будаковим, В.М. Бутузовим, М.М. Галамбою, Р.А. Калюжним, Н.В. Камінською, В.В. Коваленко, Я.Ю. Кондратьєвим, Б.А. Кормичем, Ю.Є. Максименко, А.І. Марущаком, Г.В. Новицьким.

Метою статті є визначення праввої природи кіберзлочинності, особливостей даної категорії у вітчизняній науці та в контексті становлення і розвитку інформаційного суспільства в Україні. На цій оснві важливо визначити основні причини і форми її прояву, відповідні шляхи протидії.

Виклад основного матеріалу дослідження. Становлення інформаційного суспільства в Україні стримується низкою проблем нормативно-правового та організаційного векторів [1]. У період глобалізації швидкий розвиток інформаційних технологій, нових систем комунікацій і комп'ютерних мереж супроводжується зловживанням цими технологіями зі злочинною метою. Саме тому питання вивчення та запозичення позитивного міжнародного досвіду у сфері адміністративно-правових механізмів регулювання захисту інформації в сучасних умовах, протидії кіберзлочинності є актуальним і для забезпечення стратегічних намірів України щодо європейської і євроатлантичної інтеграції [2].

Поняття «кіберзлочинність» вперше з'явилось в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів відносно автоматизованих систем обробки даних. Поняття кіберзлочинності як сукупності злочинів поширюється на всі види злочинів, скоєних в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть виступати (бути) предметом (метою) злочинних посягань, середовищем, в якому відбуваються правопорушення, і засобом або знаряддям злочину.

Таким чином, кіберзлочинність може бути визначена як сукупність злочинів, скоєних у кіберпросторі за допомогою комп'ютерних систем чи комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [3].

О. Копатін та Є. Скулишин надають визначення поняття кіберзлочину як злочину, пов'язаного

з використанням кібернетичних комп'ютерних систем, та злочину в кіберпросторі. [4]. На думку В.М. Болгова, кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних, суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [2].

У теорії відсутня загальноприйнята правова дефініція досліджуваного поняття. Так, на доктринальному рівні можна зустріти низку аналогічних однорідних понять, зокрема: злочини, які вчиняються з використанням електронно-обчислювальної машин (ЕОМ), «комп'ютерний злочин», «злочин у сфері високих технологій», «комунікаційний злочин», «кіберзлочин», «злочин у сфері комп'ютерної інформації», «мережевий злочин» тощо. Зарубіжними дослідниками частіше вживаються поняття "high-tech crime", "cyber crime", "network crime", які, відповідно, перекладаються як «злочини у сфері високих технологій», «кіберзлочини», «злочини в комп'ютерних мережах» [5].

Кіберзлочинність можна вважати об'єднуючим поняттям, що характеризує пов'язані кримінальні дії: кіберзалежні та кіберутворюючі злочини. Кіберзалежні – це злочини, які вчиняються з використанням комп'ютерів, комп'ютерних мереж чи інших комунікаційних форм (поширення вірусів та інших шкідливих програм, хакерство, зламування серверів для захоплення мережевої інфраструктури або веб-сторінок). Такі злочини спрямовані на пошкодження комп'ютерів та джерел мережі, мають наслідки у вигляді, наприклад, шахрайства. Кіберутворюючі злочини – це традиційні види злочинів, які стали кіберзлочинами через використання комп'ютерів, комп'ютерних мереж та інших видів комунікації. На відміну від кіберзалежних, вони можуть вчинятися і без застосування «комп'ютерного елементу» [6].

Прикладом кібертероризму, що посягнув на установлений розвиток інформаційних та інших відносин, може служити найбільша вірусна атака проти підприємства «Укртелеком» 16–19 листопада 2001 р. Дії вірусу Nimda (анаграма слова «admin») серйозно вплинули на працездатність обчислювальної мережі «Укртелекому», яка налічувала більше 700 комп'ютерів і десятки серверів. Це привело до тимчасового відключення комп'ютерів «Укртелекому» від мережі Інтернет, а також до виведення з ладу корпоративної системи електронної пошти. Вірусом виявилися заражені сотні комп'ютерів корпоративної мережі, порушена робота ряду серверів. Зокрема, було порушено функціонування сервера корпоративної електронної пошти Генеральної дирекції «Укртелеком» [7].

Інший приклад трапився 23 грудня 2015 р., коли хакери здійснили кілька потужних кібератак проти українських постачальників електроенергії Прикарпаття, атакувавши шість різних енергокомпаній одночасно. У результаті сталося відключення електроенергії в 103 населених пунктах України. Розслідування на території України проводили представники ФБР, Держдепартаменту, міністерства внутрішньої безпеки та міністерства енергетики США. За його результатами, було виявлено докази того, що за атакою на українську енергосистему стояла група добре підготовлених хакерів із Росії. А вже на початку 2016 року хакери знову атакували комп'ютерну систему «Укренерго» і розіслали вірусні повідомлення на електронні адреси підприємств електроенергетики [8].

Законом України «Про основні засади забезпечення кібербезпеки України» 2017 року визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України d 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. У законі поняття «кіберзлочин» («комп'ютерний злочин») трактується як суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України, а кіберзлочинність визначено як сукупність кіберзлочинів [9].

Ефективність протидії явищу кіберзлочинності вбачається у спільних діях державного і приватного секторів, вдосконаленні міжнародно-правових інструментів та національного законодавства, організації інституційного механізму боротьби з кіберзлочинами.

Так, Будапештська конвенція Ради Європи про злочинність у кіберпросторі 2001 р. є фундаментом

для розробки законодавства в боротьбі з кіберзлочинністю на різних рівнях територіальної організації влади [10]. Вона ратифікована 18 державами та підписана 25 країнами, серед яких є і Україна (7. 09.2005 р.) [11]. Згодом було ратифіковано додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (Додатковий протокол) [12].

Будапештська Конвенція, як основоположний документ у сфері боротьби з кіберзлочинністю, надає умовну класифікацію кіберзлочинів, що поділяються на такі категорії: 1) правопорушення проти конфіденційності, цілісності та доступності ікомп'ютерних даних і систем (так звані «CIA-злочини»); 2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, здійснені з використанням комп'ютерів; 3) правопорушення, пов'язані зі змістом інформації, зокрема дитяча порнографія, расизм та ксенофобія; 4) правопорушення, пов'язані з порушенням авторських і суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео і інших видів цифрової продукції, а також баз даних і книг.

Згідно з КК України поняття кіберзлочинності охоплює кримінальні правопорушення у сфері: використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем); обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; господарських відносин та приватної власності, яка включає в себе незаконні фінансові операції та заборонені види господарської діяльності, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж [13].

Водночас тенденції розвитку суспільних відносин в Україні протягом останніх років демонструють такі найбільш поширені кіберзлочини: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем із метою одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам); інші злочини. За інформацією Національного банку України, в банківській системі України розповсюдженими є такі види кіберзлочинів: 1) банкоматне шахрайство (скіминг, використання «білого пластику» для «клонування» (підробки) платіжної картки та зняття готівки в банкоматах; Transaction Reversal Fraud; Cash Trapping); 2) шахрайство в торгівельно-сервісних мережах; 3) шахрайство в мережі Інтернет; 4) шахрайство в системах дистанційного банківського обслуговування (ДБО) [10; 14]

Не залишаються осторонь такиі негативні явища, що перешкоджають життєдіяльності інформаційного громадянського суспільства і міжнародних правоохоронних організацій. Зокрема, на основі взаємодії в боротьбі з комп'ютерними злочинами було розроблено робочою групою Інтерполу кодифікатор, за яким усі кіберзлочини класифіковані таким чином: QA – несанкціонований доступ і перехоплення (QAH – комп'ютерний абордаж (несанкціонований доступ)); QAI – перехоплення за допомогою спеціальних технічних засобів; QAT – крадіжка часу (ухилення від плати за користування); QAZ – інші види несанкціонованого доступу та перехоплення); QD – зміна комп'ютерних даних (QDL – логічна бомба; QDT – троянський кінь; QDV – комп'ютерний вірус; QDW – комп'ютерний черв'як; QDZ – інші види зміни даних); QF – комп'ютерне шахрайство (QFC – шахрайство з банкоматами; QFF – комп'ютерна підробка; QFG – шахрайство з ігровими автоматами; QFM – маніпуляції з програмами введення-виведення; QFP – шахрайства з платіжними засобами; QFT – телефонне шахрайство; QFZ – інші комп'ютерні шахрайства); QR – незаконне копіювання (QRG – комп'ютерні ігри; QRS – інше програмне забезпечення; QRT – топологія напівпровідникових пристроїв; QRZ – інше незаконне копіювання); QS – комп'ютерний саботаж (QSH – з апаратним забезпеченням (порушення роботи ЕОМ); QSS – із програмним забезпеченням (знищення, блокування інформації); – інші види саботажу); QZ – інші комп'ютерні злочини (QZB – із використанням комп'ютерних дошок оголошень; QZE – розкрадання інформації, що становить комерційну таємницю; QZS – передача інформації, що підлягає судовому розгляду; QZZ – інші комп'ютерні злочини) [15].

Постають питання: в який спосіб слід протидіяти комп'ютерній та іншій злочинності в даній сфері? Чи є вже певні здобутки на даному шляху і т.д.?

Безумовно є, але, на жаль, на наше переконання, вони є дещо несвоєчасними і несистем-

ними. При цьому відзначимо, що відповідно до Плану заходів на 2018 рік із реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 11 липня 2018 р. № 481-р, будуть реалізовані такі завдання:

1. Підготовка пропозицій стосовно врегулювання на законодавчому рівні питання щодо: розмежування кримінальної відповідальності за злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; підвищення рівня відповідальності посадових осіб державних органів, установ та організацій за порушення вимог щодо інформування в установленому порядку про несанкціоновані дії (кібератаки) стосовно державних інформаційних ресурсів; визначення Держспецзв'язку органом, відповідальним за збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів; встановлення обов'язкового погодження з ним завдань (проектів) Національної програми інформатизації, проектів (завдань) створення і розвитку інформаційно-телекомунікаційних систем державних органів, підприємств, установ та організацій державної форми власності

2. Врегулювання питання щодо: заборони державним органам, підприємствам, установам та організаціям державної форми власності, крім закордонних дипломатичних установ України, закуповувати послуги (укладати договори) з доступу до Інтернету в операторів (провайдерів) телекомунікацій, в яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації; впровадження обов'язкових вимог стосовно здійснення державними органами, підприємствами, установами та організаціями державної форми власності ідентифікації та автентифікації джерел отриманих оновлень до програмного забезпечення, яке використовується для обробки державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, та встановлення цілісності таких оновлень; застосування посадовими (службовими) особами державних органів, підприємств, установ та організацій державної форми власності електронного цифрового підпису під час використання електронної пошти для виконання посадових (службових) обов'язків; визначення порядку передачі, збереження і доступу до резервних копій інформації та відомостей державних електронних інформаційних ресурсів для потреб державних органів, насамперед суб'єктів сектору безпеки і оборони, фінансового, енергетичного, транспортного секторів; формування переліку об'єктів критичної інформаційної інфраструктури; визначення порядку формування та забезпечення функціонування їх державного реєстру; визначення вимог до проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

3. Удосконалення взаємодії між суб'єктами забезпечення кібербезпеки шляхом: створення єдиної інтерактивної бази даних про кіберінциденти для потреб Міноборони, Держспецзв'язку, СБУ, Національної поліції, Національного банку, розвідувальних органів; організації обміну інформацією про кібератаки на об'єкти критичної інфраструктури (насамперед енергетики, транспорту, банків).

4. Узгодження проектів (завдань) Національної програми інформатизації, виконання яких передбачено у 2018 році, з Адміністрацією Держспецзв'язку та Державним агентством із питань електронного урядування.

5. Удосконалення нормативно-правової бази шляхом: подальшого впровадження норм міжнародних стандартів, стандартів ЄС та НАТО у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки; імплементації Директиви (ЄС) 2016/1148 Європейського Парламенту та Ради ЄС від 6 липня 2016 р. щодо заходів з підвищення загального рівня безпеки мереж та інформаційних систем в ЄС.

6. Розроблення механізму залучення фізичних і юридичних осіб до виконання завдань кіберзахисту державних електронних інформаційних ресурсів у рамках державно-приватного партнерства на умовах аутсорсингу.

7. Розвиток Національної телекомунікаційної мережі, врегулювання питань порядку надання послуг та їх тарифікації.

8. Проведення модернізації ситуаційних центрів із кібербезпеки Держспецзв'язку та СБУ шляхом залучення допомоги НАТО в рамках реалізації Трастового фонду Україна – НАТО з кібербезпеки.

9. Забезпечення розвитку організаційно-технічної моделі кіберзахисту, зокрема утворення центру реагування на кіберзагрози, а також розвиток системи захищеного доступу державних органів до Інтернету.

10. Опрацювання питання щодо утворення тренінгового кіберцентру в інтересах суб'єктів забезпечення кібербезпеки.

11. Удосконалення механізму взаємодії з Національною академією наук та її профільними установами з метою проведення наукових досліджень та спільних науково-практичних робіт у галузях кібербезпеки та кіберзахисту критичної інфраструктури.

12. Забезпечення діяльності Центру кіберзахисту Національного банку, вдосконалення кіберзахисту і кібербезпеки банківської системи України та у сфері переказу коштів.

13. Розроблення методики формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик.

14. Участь у заходах щодо зміцнення міжнародного співробітництва шляхом утворення спільних двосторонніх або багатосторонніх груп для здійснення розслідувань кіберзлочинів, а також проведення спільних операцій, обміну інформацією та досвідом

15. Організація та проведення конференцій, семінарів, форумів, засідань круглих столів, тренінгів, навчань із питань кібербезпеки та кіберзахисту на державному і міжнародному рівнях.

16. Розвиток системи підготовки кадрів у сфері кібербезпеки, зокрема: підготовка фахівців тактичного та оперативно-тактичного рівня за напрямом «Кібербезпека»; підготовка, атестація, переатестація та підвищення кваліфікації фахівців у сфері кіберзахисту для потреб державних органів, військових формувань і правоохоронних органів.

17. Проектування захищеного дата-центру (центру обробки даних) для потреб державних органів, насамперед суб'єктів сектору безпеки і оборони, фінансового, енергетичного, транспортного секторів.

18. Здійснення заходів щодо утворення Національного центру оперативно-технічного управління телекомунікаційними мережами України [18].

Висновки. Вважаємо, що для комплексної протидії кіберзлочинності з метою зміцнення економічних основ функціонування безпеки підприємств, установ і організацій слід активізувати проведення вищеперелічених заходів. Враховуючи транскордонний характер кіберзлочинності, потребує налагодження співробітництво правоохоронних органів у розслідуванні кіберзлочинів на оперативному рівні; створення і забезпечення функціонування механізму вирішення юрисдикційних питань у кіберпросторі. У сучасному інформаційному суспільстві, де поширені і будуть надалі поширюватись кіберзагрози, важливо постійно і системно, своєчасно вживати ефективних заходів із протидії кіберзлочинності, а також удосконалення її методів і форм її попередження. Це стосується практично всіх сфер суспільного і державного життя, підприємницького і соціогуманітарного середовища.

З огляду на курс України на входження у світовий інформаційний простір ми переконані, що потребує побудови національна модель забезпечення кібербезпеки підприємств, установ і організацій, включаючи неурядових; координація зусиль та взаємодія правоохоронних органів, спецслужб, судової системи, а також належне їх кадрове і матеріально-технічне забезпечення, обмін інформацією про попередження і боротьбу з кіберзлочинністю.

Список літератури:

1. Бойченко О.В. Угрозы информационных ресурсов государственного самоуправления. Проблемы и особенности влияния международной информации на экономические и общественно-политические процессы Материалы Междунар. научно-практ. конфер. Симферополь: ИСВА МСУ, 2007.9. Сідак В.С., Артемов В.Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: навч. посіб. Київ: КНТ, 2007. 160 с.

2. Болгов В., Гадіон Н., Гладун О. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. К.: Національна академія прокуратури України, 2015. 202 с.

3. Кіберзлочинність: проблеми боротьби і прогнози. URL: http://anticyber.com.ua/article_detail.php?id=140.

4. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. К.: Аванпост- Прим, 2012. 214 с.

5. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: монография. М.: Норма, 2004. 432 с.

6. Dr. Mike McGuire and Samantha Dowling Cybercrime: A review of the evidence Summary of key findings and implications. Home Office Research Report 75. University of Surrey, October, 2013. P. 29.

7. Фесик А.В. Роль органів державної влади у протидії кіберхлочинності. Вісник Кримінологічної асоціації України. 2013. № 4.

8. Маркарян М.В. До питання про реформування законодавства України у сфері кіберзлочинності. Київ.

9. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.2017. URL: http://zakon5.rada.gov.ua/laws/show/2163-19.

10. Кіберзлочинність та відмивання коштів. Дані Департаменту фінансових розслідувань Державної служби фінансового моніторингу України. К., 2013.

11. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV. Відомості Верховної Ради України. 2006. № 5. С. 128. Ст. 71.

12. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Закон України від 21 липня 2006 року № 23-V. Відомості Верховної Ради України. 2006. № 39. С. 1384. Ст. 328.

13. Кримінальний кодекс України. URL: http://zakon3.rada.gov.ua/ laws/show/2341-14/page.

14. Кіберзлочинність: проблеми боротьби і прогнози. URL: http://anticyber.com.ua/article_detail.php?id=140.

15. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: ООО Издательство «Юрлитин- форм», 2001.

16. План заходів на 2018 рік з реалізації Стратегії кібербезпеки України, затверджений розпорядженням Кабінету Міністрів України від 11 липня 2018 р. № 481-р. URL: http://zakon.rada.gov.ua/laws/show/481-2018-%D1%80.

КИБЕРПРЕСТУПНОСТЬ КАК ПРЕПЯТСТВИЕ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА В УКРАИНЕ

В статье раскрыта сущность киберпреступности, подходы к пониманию данного понятия, классификации киберпреступлений, других противоправных действий в данной сфере. Определены проблемы, достижения и перспективы противодействия и борьбы с киберпреступностью на пути развития гражданского информационного общества, вхождения Украины в мировое информационное пространство.

Ключевые слова: *информационное общество, киберпреступность, информация, киберпреступления, кибербезопасность, законодательство.*

CYBERCRIME AS AN OBSTACLE THE DEVELOPMENT OF THE INFORMATION SOCIETY IN UKRAINE

The article reveals the essence of cybercrime, approaches to the understanding of this concept, classification of cybercrime and other illegal acts in this sphere. Defined problems, achievements and prospects of combat and combat cybercrime on the way to build civil society, Ukraine joining into the global information space.

Key words: *information society, cybercrime, information, cybersecurity, legislation.*