[13] Про судову практику в справах про злочини проти життя та здоров'я особи : постанова Пленуму Верховного Суду України від 7 лютого 2003 р. № 2 // Законодавство України : [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0002700-03

[14] Вирок Апеляційного суду Київської області від 15 липня 2010 р. (справа № 1-13/10) // Єдиний державний реєстр судових рішень : [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/52159660; Вирок Баштанського районного суду Миколаївської області від 25 червня 2015 р. (справа № 468/560/14-к) // Єдиний державний реєстр судових рішень : [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/39435618; Вирок Новокаховського міського суду Херсонської області від 18 грудня 2012 р. (справа № 2117/210/2012) // Єдиний державний реєстр судових рішень : [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/28182069

[15] Вирок Ленінського районного суду м. Миколаєва від 25 квітня 2014 р. (справа № 489/1363/14-к, провадження № 1-кп/489/178/14 // Єдиний державний реєстр судових рішень : [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/Review/38422019

Резюме

Андрушко А.В. **Проблеми кваліфікації захоплення заручників.**

У статті на підставі аналізу кримінального законодавства, доступної емпіричної бази і наукової літератури досліджено проблемні питання кваліфікації захоплення заручників (ст. 147 Кримінального кодексу України).

Ключові слова: злочини проти волі, честі та гідності особи, захоплення заручників, кримінально-правова кваліфікація.

Резюме

Андрушко А.В. **Проблемы квалификации захвата заложников.**

В статье на основании анализа уголовного законодательства, доступной эмпирической базы и научной литературы исследованы проблемные вопросы квалификации захвата заложников (ст. 147 Уголовного кодекса Украины).

Ключевые слова: преступления против свободы, чести и достоинства личности, захват заложников, уголовно-правовая квалификация.

Summary

Andrushko A. **Issue of legal denomination of the hostage-taking.**

The article analyzes criminal legislation, available empirical data and scholar literature in order to investigate problem issues of legal denomination of the hostage-taking (article 147 of the Criminal Code of Ukraine).

Key words: crimes against liberty, honor and dignity of a person, hostage-taking, criminal law denomination.

УДК 004.056.5:378.1 (045)

П.Д. БІЛЕНЧУК, Т.В. ОБІХОД

Петро Дмитрович Біленчук, *професор Київського університету права НАН України*

Тетяна Вікторівна Обіход, *старший науковий співробітник Інституту ядерних досліджень НАН України, юрист*

КІБЕРБЕЗПЕКА І ЗАСОБИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ Й КІБЕРТЕРОРИЗМУ

У наш час глобалізації і охоплення Всесвітньою мережею галузей науки, економіки, банківської сфери, політичного життя, систем електропостачання, розвитку систем телекомунікації, однією із нагальних проблем є проблема кібербезпеки.

Метою статті є аналіз сучасного стану кіберзлочинності в Україні і розгляд концептуальних безпекових засад формування стратегії розвитку України задля надійного захисту і успішного інноваційного розвитку нашої держави.

В Україні кібербезпеці приділяється багато уваги на законодавчому рівні. У Законі України «Про національну безпеку України»[1] акцентується увага на необхідності боротьби із тероризмом[2]. У рамках цього питання велику увагу приділено кібербезпеці. Визначено основи та принципи національної безпеки і оборони і підкреслено: «Стратегія кібербезпеки України – 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». Стаття 31 «Стратегія кібербезпеки України» є документом довгострокового планування, в якому визначаються:

– пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави,

– наявні та потенційні кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі,

– пріоритети національних інтересів України у сфері кібербезпеки,

– підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і розв'язання передбачених завдань, та основні напрями використання фінансових ресурсів.

Реалізація Стратегії кібербезпеки України здійснюється на основі національного оборонного, безпекового, економічного, інтелектуального потенціалу з використанням механізмів державно-приватного партнерства, а також із залученням міжнародної консультативної, фінансової, матеріально-технічної допомоги.

Закон України «Про основні засади забезпечення кібербезпеки України», який набрав чинності 9 травня 2018 р.[3], дає таке визначення кібербезпеки: «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 в кіберпросторі». Законом про кібербезпеку вперше встановлюється значна кількість понять, що є новими для правового поля України, а саме:

– кібербезпека;

– кіберзагроза;

– кіберпростір;

– кіберінцидент;

– кібершпигунство;

– кібертероризм

та інші поняття, які потребують подальшого узгодження з чинними законами і розмежування із суміжними поняттями.

Кіберзлочинність визначається як злочин, у якому комп'ютер є об'єктом злочину (хакерство, фішинг, спам) або використовується як інструмент для вчинення злочину (дитячої порнографії, злочини на ґрунті ненависті).

Необхідно виділити наступні типи кібератак:

– яка використовує шкідливе програмне забезпечення і порушує роботу мережі за допомогою окремої виноски або небезпечного посилання і вкладення електронної пошти за допомогою фішинга. Після такої атаки зловмисник може встановити програмне забезпечення для обробки всієї конфіденційної інформації жертви: дані кредитної карти і логіну;

– атаки підслуховування (Man-in-the-middle (MitM));

– проводити атаки з розподіленою відмовою (DdoS);

– SQL(Structured Query Language)-ін'єкції зі шкідливим кодом на сервері;

– проводити операцію із нульовим днем після оголошення про мережеву уразливість до того, як буде реалізований патч або рішення.

Один із найвідоміших квантових хакерів у світі Вадим Макаров звертає увагу на те, що нині існує понад 20 способів зламати квантовий зв'язок. Найпростіший спосіб, на думку Макарова, це підключитися до лінії зв'язку в момент передачі фотона і спробувати виміряти його стан. Квантова система зв'язку не знаходиться завжди в ідеальному стані, на сьогоднішній день багато функцій захисту поки просто не працюють. При цьому уразливості системи дають змогу перехоплювати ключ під час його передачі непомітно для обох сторін. Для цього потрібна лише добра оптична лабораторія вартістю до $ 1 млн.

Таким чином, кіберзлочинність охоплює широкий спектр видів діяльності, але їх можна розподілити на дві основні категорії:

1. Злочини, які націлені на комп'ютерні мережі або пристрої. До таких видів злочинів належать віруси і атаки типу «відмова в обслуговуванні» (DoS).

2. Злочини, які використовують комп'ютерні мережі для просування іншої злочинної діяльності. До таких видів злочинів належать кібер-штурм, фішинг і шахрайство або крадіжка особистих даних.

Відомо, що з кіберзлочинністю пов'язане поняття кібертероризму, який визначається Федеральним бюро розслідувань США як навмисний напад на комп'ютерну систему, комп'ютерні дані, програми та іншу інформацію з єдиною метою насильства щодо підпільних агентів і субнаціональних груп. Головна мета кібертероризму – заподіяти шкоду і руйнування[4,5].

Вважаємо, що кібертероризм можна в цілому класифікувати за трьома основними категоріями:

простий – це основні атаки, які включають злом окремої системи;

додатковий – це більш складні атаки, які можуть включати злом декількох систем і/або мереж;

комплексний – це скоординовані атаки, які пов'язані із великомасштабним впливом і використанням складних інструментів.

Основними галузями загроз від кібертероризму є наступні:

– галузі електропостачання;

– системи телекомунікацій;
– дії Кабінету Міністрів і адміністрації Президента.

Сучасний ринок кіберзлочинності є наступним:
– наркотики;
– промисловість;
– банківські послуги;
– речовий ринок;
– ринок ІТ технологій;
– фармацевтичний ринок.

Його особливості пов'язані із відсутністю певного місця як джерела загрози і глобалізмом масової загрози. Тому боротьба із цим соціальним злом є вкрай необхідною, важливою та з позиції забезпечення безпеки людини, суспільства, держави, цивілізації є загальнообов'язковою.

Статистичні дані органів правосуддя засвідчують, що кількість і багатосторонність кібератак сьогодні є вражаючою. Перелічимо лише декілька з них:

– Атаки на промислові об'єкти, енергетичні системи.

США. Операція «NightKnight» (нічний лицар). У 2011 р. компанія McAfee оприлюднила детальну доповідь про виявлену нею потужну операцію кібершпигунства.

Саудівська Аравія. Операція «Shamoon» та однойменний вірус були виявлені в 2012 році.

Україна. Кібератака на енергетичні компанії України в грудні 2015 року. Найбільше постраждали споживачі «Прикарпаттяобленерго»: було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин.

– Системи управління технологічними процесами.

Австралія. У березні-квітні 2000 р. відбулась низка невдалих кібератак (не менше 45) на систему управління нещодавно побудованої водоочисної системи в графстві Маручі, Квінсленд, Австралія. Нарешті, із 46-ї спроби зловмисникові, Вайтеку Боудену, вдалось вивести систему управління з ладу, в навколишнє середовище (парки, річки) Маручідору вилилось близько 800 тис. м³ стічних вод.

Іран. Операція «Олімпійські ігри» з використанням комп'ютерного хробака Стакснет – спроба саботувати ядерну програму Ірану.

– Об'єкти інфраструктури.

США. Наприкінці листопада 2016 р. інформаційна система міського громадського транспорту (автобуси та трамваї) Сан-Франциско була вражена здирницьким програмним забезпеченням (англ. ransomware).

США. 15 березня 2018 р. американський уряд оприлюднив спільну доповідь CERT-US, ФБР та Міністерства національної безпеки, в якій звинуватили Російську Федерацію у здійснені хакерських атак на державні установи, об'єкти критичної інфраструктури, енергетичні та ядерні об'єкти, приватні підприємства.

– Кібервійни.

Естонія-Росія. Кібератаки проти Естонії (2007 р.) – перші відомі масовані кібератаки, спрямовані проти національної безпеки країни. Зловмисникам вдалось вчинити «дефейс» деяких сайтів, урядові та банківські сервери і служби були виведені з ладу внаслідок масованих атак на відмову в обслуговуванні.

Грузія-Росія. Кібератаки проти Грузії (2008 р.), які відбувались спільно зі збройною агресією Російської Федерації проти країни. Перевага була віддана атакам на відмову в обслуговуванні урядових веб-сайтів та засобів масової інформації. Під час другої хвилі вже відбувались діфейси різних сайтів, а також DoS-атаки проти ширшого кола сайтів (великих приватних підприємств, тощо).

Україна-Росія. Російсько-українська кібервійна з 2014 року. Перші атаки на інформаційні системи приватних підприємств та державні установи України фіксували іще під час масових протестів у 2013 році. Повідомлення вірусу Petya, що показується після завершення шифрування головної таблиці файлів файлової системи NTFS (Україна, червень 2017 р.)[6].

Бангладеш Хакерська крадіжка золотовалютних резервів Бангладеш – спроба викрасти невстановленими особами в 2016 р. майже $ 1 млрд з рахунку Банку Бангладеш у Федеральному резервному банку Нью-Йорка, з яких вдалося вивести лише $101 млн.

Про актуальність боротьби із кіберзлочинністю можна більш детально дізнатися із сайту URL: https://korrespondent.net/tag/38906/, який є лише відображенням останньої інформації із теми «Кібератака» в інтернеті наприкінці 2018 року.

Згідно з дослідженням «Глобальний індекс кібербезпеки» (Global Cybersecurity Index), який щорічно проводиться Міжнародним союзом електрозв'язку (ITU), у 2017 р. Україна зайняла «почесне» 59 місце в рейтингу з 193 можливих. Слід зазначити, що рівень кібербезпеки держав-респондентів оцінювався за п'ятьма основними показниками:

Legal (законодавча база);
Technical (технологічна база);
Organization (методологічна база);
Capacity Building (нарощування потенціалу);
Cooperation (розвиток взаємодії).

З перерахованих вище показників в Україні в «зеленій зоні» опинилися тільки «Legal» і «Cooperation». Відомо, що навіть багаторазове прочитання вголос законів і нормативних документів дуже мало допоможе в

практичному вирішенні означеної проблеми. Наші найнижчі показники фактично пов'язані із практичною площиною. Очевидно, що нам сьогодні бракує як високих технологій, так і належних світових стандартів і методологій з кібербезпеки. Сьогодні фактично відсутня імплементація реальних заходів кіберзахисту в ІТ-інфраструктурах, слабий процес навчання і підвищення обізнаності в питаннях кібербезпеки. Очевидно, що закони – це не якась окрема від всіх нас сутність. Їх виконання – це наш головний обов'язок.

Для України у сфері кібербезпеки існують тільки дві основні проблеми: внутрішня і зовнішня:

а) внутрішня проблема полягає в тому, що комерційні структури і фізичні особи не є обізнаними із кіберпроблемами. Передусім потрібно працювати над взаємодією між силовими структурами і тими комерційними організаціями, які можуть забезпечити цей сервіс із подолання проблем при атаках, хаках і т.д. Крім того, повинні бути реформи у сфері освіти задля достатньої інформаційної професійної грамотності випускників вузів. Очевидно, що фахівці із кібербезпеки зможуть пояснювати необхідність кіберзахисту, і відповідно будуть розвивати послуги з кібербезпеки. Вважаємо, що наявність таких спеціалістів є важливою з позиції захисту державних об'єктів, державної таємниці, у зв'язку з низьким рівнем впровадження інноваційних технологій у сферу захисту інформації державної важливості;

б) якщо вести мову про зовнішню політику в цьому плані, то захист державних об'єктів і державної таємниці також повинен підтримуватися з інформаційних засадничих положень. Безумовно, існує дуже хороша наукова школа СБУ і т.д. Але треба звернути увагу на те, що існує технічна недосконаліть на підприємствах, а технології, як відомо, постійно розвиваються. У цій сфері теж потрібні постійні оновлення.

Тому не випадково, що тема кібератак увійшла до порядку денного саміту ЄС (17–18 жовтня 2018 р.) у зв'язку з кібератакою на Організацію по забороні хімічної зброї (ОЗХЗ), в якій звинувачують російські спецслужби. У зв'язку з цим 18 жовтня 2018 р. глави держав і урядів 28 країн Європейського Союзу звернули увагу Брюсселя на заходи по боротьбі з кібератаками за допомогою встановлення відповідних санкцій. Про це повідомила прес-служба Ради ЄС за підсумками дводенного саміту. Представник прес-служби даного форуму акцентував увагу на тому, що: «Саміт тільки що погодив роботу над боротьбою з кібератаками за допомогою обмежувальних заходів»[7,8,9].

Отже, можемо зробити такі висновки, а також надати пропозиції та рекомендації. Задля запобігання кіберзлочинності та кібертероризму реакція Уряду України на кіберзагрози, очевидно, що повинна бути наступною:

1) карантин на смартфони;

2) стандартні методи захисту;

а) морально-етичні засоби. До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін.;

б) правові засоби захисту, які вимагають удосконалення карного і цивільного законодавства, а також судочинства. Вони повинні бути пов'язаними із підвищенням жорсткості кримінальних законів щодо комп'ютерних злочинців. Наприклад, у Гонконгу максимальне покарання за такий злочин – 10 років позбавлення волі, а у Кримінальному кодексі України незаконне втручання в роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк;

в) адміністративні (організаційні) засоби захисту інформації. які регламентують процеси функціонування ІС, використання її ресурсів;

г) засоби фізичного (технічного) захисту інформації – це різного роду механічні, електро- або електронно-механічні пристрої для захисту від несанкціонованого доступу і викрадень інформації;

д) програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів із використанням біометричного захисту інформації;

3) розробка автоматизованих систем, мереж і комп'ютерів, повинні бути добре захищеними проти зламу.

---

[1] Про національну безпеку України : Закон України // Відомості Верховної Ради (ВВР). – 2018, № 31. – Ст. 241.

[2] *Біленчук П.Д.* Розвиток ядерної криміналістики для протидії міжнародному тероризму / П.Д. Біленчук, Т.В. Обіход // Сучасні правові системи світу в умовах глобалізації: реалії та перспективи: матеріали міжнародної наук.-практ. конференції (м. Київ, 11–12 березня 2016 р.). – К.: Центр правових наукових досліджень, 2016. – С. 128–130; *Обіход Т.В.* Загроза ядерного тероризму та боротьба з ним за допомогою ядерної криміналістики / Т.В. Обіход // Безпека людини, суспільства, держави: правові, криміналістичні і психофізіологічні засади : зб. матеріалів Міжнародної наук.-практ. конференції (м. Київ, 17 листопада 2015 р.). – С. 33–38; *Біленчук П.Д.* Правове регулювання та національна програма України в галузі ядерної криміналістики П.Д. Біленчук, Т.В. Обіход // Часопис Київського університету права. – 2016. – № 1. – С. 260–264; *Биленчук П.Д., Обиход Т.В.* Современные реалии и развитие ядерной криминалистики. – С. 20–25; Напрями реформування кримінального провадження в Україні: процесуальні та криміналістичні аспекти // Збірник матеріалів VI Міжнародної науково-практичної конференції (27 травня 2016 р.) / редкол. Ю.Л. Бошицький, Г.С. Семаков, П.Д. Біленчук, У.Б. Андрусів та ін. – Л.: Галицька видавнича спілка, 2016. – 196 с.; *Біленчук П.Д., Обіход Т.В.* Створення ядерної криміналістики як протидії ядерному тероризму // Сучасний стан криміналістичного забезпечення досудового розслідування : Збірник матеріалів конференції / редкол.: Кобилянський О.Л., Свобода Є.Ю. – К.: Навчально-науковий інститут № 2 Національної академії внутрішніх справ, 2017. – 476 с. – С. 39–45; *Біленчук П.Д.* Правове і криміналістичне забезпечення протидії ядерному тероризму / П.Д. Біленчук, Т.В. Обіход // Часопис Київського університету права. – 2017. – № 1. – С. 292–296; *Біленчук П.Д.* Ядерна безпека: сучасний стан правового

забезпечення / П.Д. Біленчук, Т.В. Обіход // Правове забезпечення безпеки в сучасному вимірі: матеріали наук.-методологічного семінару (м. Київ, 18 травня 2017 р.). – К. : КУП НАН України, 2017. – С. 3; *Біленчук П.* Ядерна безпека і ядерна криміналістика: стратегія наукового забезпечення / П. Біленчук, Т. Обіход // Юридичний вісник України. – 2017. – № 21 (1141). – С. 14–15.

[3] Про основні засади забезпечення кібербезпеки України: Закон України // Відомості Верховної Ради (ВВР). – 2017. – № 45. – Ст. 403.

[4] NASA Mariner 1NSSDC ID: MARIN1 Passwords revealed by sweet deal – BBC News.

[5] *Richardson R.* (2010). 2009 CSI Computer Crime & Security Survey. Computer Security Institute. «A General Framework for Formal Notions of Secure Systems». – B. Pfitzmann, M. Waidner, Hildesheimer Informatik-Berichte.

[6] *Кім Зеттер*, Wired (17 березня 2016). Хакерська атака Росії на українську енергосистему: як це було : [Електронний ресурс]. – Режим доступу: http://texty.org.ua/pg/article/newsmaker/read/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak

[7] *Біленчук П.Д.* Електронна цивілізація: інноваційне майбутнє України: монографія / П.Д. Біленчук, М.М. Близнюк, О.Л. Кобилянський, М.І. Малій, Ю.О. Пілюков, О.В. Соболєв; за заг. ред. П.Д. Біленчука. – К.: УкрДГРІ, 2018. – 284 с.

[8] *Біленчук П.* Конвергенція квантового майбутнього: правове, освітнє, наукове і ресурсне забезпечення / П. Біленчук // Юридичний вісник України. – 2018. – № 42–43. – С. 16–17.

[9] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України № 96/2016.

Резюме

Біленчук П.Д., Обіход Т.В. **Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму.**

Розглянуто законодавче забезпечення і основні поняття кібербезпеки і кіберзлочинності. Наведено основні типи кібератак і галузі загроз від кібертероризму. Підкреслено глобалізм, велику небезпеку і масовість наслідків кібертероризму. Проаналізовано недоліки боротьби із кіберзлочинністю. Запропоновано внутрішні й зовнішні засоби подолання проблем боротьби із кібертероризмом в Україні.

Ключові слова: кібербезпека, кіберзлочинність, кібертероризм, національна безпека, кіберзагроза.

Резюме

Биленчук П.Д., Обиход Т.В. **Кибербезопасность и методы предотвращения и противодействия киберпреступности и кибертерроризму.**

Рассмотрено законодательное обеспечение и основные понятия кибербезопасности и киберпреступности. Приведены основные типы кибератак и разновидности угроз, связанных с кибертерроризмом. Подчеркнуты глобализм, большая опасность и массовость последствий кибертерроризма. Проанализированы недостатки борьбы с киберпреступностью. Предложены внутренние и внешние средства преодоления проблем борьбы с кибертерроризмом в Украине.

Ключевые слова: кибербезопасность, киберпреступность, кибертерроризм, национальная безопасность, киберугроза.

Summary

Bilenchuk P., Obikhod T. **Cybersecurity and means of preventing and combating to cybercrime and cyberterorrism.**

In this article legislative support and basic concepts of cybersecurity and cybercrime are considered. The main types of cyberattacks and the types of threats associated with cyberterrorism are given. Globalism, great danger and mass consequences of cyberterrorism are underlined. The shortcomings of the fight against cybercrime are analyzed. Internal and external means of overcoming of the problems of fighting again cyberterrorism in Ukraine are proposed.

Key words: cybersecurity, cybercrime, cyberterrorism, national security, cyber threat.