УДК 343.9

В. В. Семенов
кандидат юридичних наук, доцент,
доцент кафедри кримінально-правових дисциплін
Національної академії внутрішніх справ

М. С. Дзігора
студентка
Національної академії внутрішніх справ

ДО ПИТАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

Хакерські атаки стають буденним явищем. У цьому переконуємось, ознайомившись з інформацією новин з мережі Інтернет за останні кілька місяців: з грудня 2016 року до лютого 2017 року відбулась хакерська атака на офіційний сайт Міністерства освіти і науки України, що призвела до тимчасового призупинення його роботи; від потужного кібернаступу постраждала Організація з безпеки та співробітництва в Європі (ОБСЄ), оскільки атака була спрямована на порушення її інформаційної безпеки та конфіденційність комп'ютерних мереж; сплеск хакерської активності спостерігався протягом усього часу виборів Президента у Сполучених Штатах Америки; у січні 2017 року масованої кібератаки зазнали збройні сили Швеції, що призвело до вимкнення комп'ютерної системи планування військових навчань; у лютому поточного року в Норвегії відбулись хакерські атаки на дев'ять скриньок електронної пошти кількох співробітників держслужб.

Варто підкреслити, що показником рівня розвитку будь-якого суспільства стає право не тільки на вільний доступ до інформації, а й на надійний захист даних з обмеженим доступом. Коли інформаційні технології впроваджені в усі сфери життя та діяльності суспільства, національна безпека прямо залежить від інформаційної безпеки, що, у свою чергу, гарантує стабільність суспільства, забезпечення прав і свобод громадян та правопорядку.

Якісну кібербезпеку в Україні неможливо уявити без створення, розвитку й успішної злагодженої реалізації законодавчої та інституційно-функціональної складових.

Аналіз останніх досліджень і публікацій. Вивченню питання кібербезпеки та кіберзлочинності в різних аспектах присвячені наукові праці К. Бєлякова, В. Білоус, В. Бутузова, А. Войціховського, О. Волеводза, Д. Гавловського, В. Голубєва, В. Гуславського, М. Литвинова, Е. Рижкова,В.Розовського,Т.Тропиної,В.Цимбалюк,О.Юхно.

Постановка завдання. Метою статті є висвітлення тих кроків, що вже були здійсненні в Україні з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави, що надасть змогу виявити позитивні аспекти цієї діяльності та ті прогалини, які ще варто заповнити.

Виклад основного матеріалу дослідження. Сьогодні як на міжнародному, так і на національному рівні відсутнє універсальне визначення «кіберзлочину».

Поняття «кіберзлочин» молоде й утворено сполученням двох слів: «кібер» і «злочин». Термін «кібер» має на увазі поняття кіберпростору (у спеціальній літературі частіше зустрічаються терміни «віртуальний простір», «віртуальний світ») та інформаційного простору, що моделюється за допомогою комп'ютерних засобів. Тобто кіберзлочини – це суспільно-небезпечні діяння, що так чи інакше пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами [1].

Поняття «кіберзлочинність» часто вживається поряд із поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». Кримінальний кодекс України оперує терміном «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед вищезазначених термінів поняття «кіберзлочинність» є найширшим та охоплює найбільше коло злочинних посягань у віртуальному середовищі, також його використання регулює міжнародне законодавство [2, с. 173].

23 листопада 2001 року Рада Європи прийняла Конвенцію про кіберзлочинність [3]. Тому вважаємо обґрунтованим вживання саме цього терміну. Україна стала стороною цієї Конвенції 07 вересня 2005 року, ратифікувавши її.

Конвенція про кіберзлочинність поділяє злочини в кіберпросторі на чотири групи. До першої групи (злочини, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем) належать: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів належить протизакон-

не використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не тільки комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених у статтях 2 – 5 Конвенції, а і паролі, коди доступу та їх аналоги, за допомогою яких можна увійти до комп'ютерної системи в цілому або до будь-якої її частини (з урахуванням злочинного наміру). Норми ст. 6 Конвенцій застосовуються тільки в тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на здійснення протиправних діянь.

До другої групи належать злочини, пов'язані з використанням комп'ютерних засобів: фальсифікація та шахрайство з використанням Інтернет-технологій (статті 7, 8 Конвенцій).

Третю групу складають злочини, пов'язані з контентом (змістом) даних.

До четвертої групи увійшли порушення авторського та суміжних прав.

Крім того, на початку 2002 р. до Конвенції ухвалено протокол про додання до переліку злочинів поширення інформації расистського й іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що ґрунтуються на расовій, національній, релігійній або етнічній приналежності.

Таким чином, перший розділ Конвенції присвячено видам діянь, які підлягають криміналізації. Її другий розділ освітлює процесуальні аспекти боротьби з кіберзлочинністю [4].

У криміналістичній науці також надається класифікація кіберзлочинів. Це питання є доволі дискусійним.

З точки зору кримінального права, до кіберзлочинів належать тільки правопорушення, передбачені розділом XVI КК України, а в рамках криміналістики доцільно включити до цього поняття й інші злочини, для скоєння яких застосовуються комп'ютерні засоби та використовується Інтернет.

У вітчизняній криміналістиці існують різні точки зору щодо класифікації кіберзлочинів.

На сьогодні поширеними є два основні напрями наукової думки. Одна частина дослідників відносять до кіберзлочинів дії, у яких комп'ютер є об'єктом або засобом посягання. Дослідники іншої групи такими правопорушеннями вважають тільки протизаконні дії у сфері автоматизованої обробки інформації. Тобто об'єктом посягання є інформація, що обробляється в комп'ютерній системі, а засобом скоєння злочину є комп'ютер. Можна погодитись із В. Вєховим, який пропонує давати різні визначення комп'ютерних злочинів (з точки зору кримінально-правової науки). Очевидно, що остання група більш широка. Відповідно до її визначення кіберзлочин можна характеризувати як діяння, в яких комп'ютер, програмне забезпечення є предметом, знаряддям або засобом скоєння злочину. Виокремлення цієї групи, в першу чергу, пов'язане зі специфікою методики розслідування. Проте назвати діяння кіберзлочином можна тільки за умови, коли комп'ютерні засоби та технології відіграють основну, центральну роль у скоєнні злочину.

Особливості механізму вчинення кіберзлочинів зумовлюють необхідність залучення до їх розслідування і розкриття фахівців відповідної спеціалізації та кваліфікації, застосування і використання сучасних комп'ютерних технологій. Це пов'язано з необхідністю пошуку, фіксації, вилучення та збирання доказів в електронній формі. Також комп'ютерні технології широко використовуються під час здійснення оперативно-розшукових заходів [1].

Свідченням того, що кібербезпека в Україні є однією зі складових національної безпеки, є те, що у 2016 році Указом Президента України [5], було введено в дію рішення Ради Національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України» («Рішення») [6], а також затверджено Стратегію кібербезпеки України («Стратегія») [7].

Надзвичайно цікавим із точки зору розуміння внутрішньої політики України в напрямі забезпечення кібербезпеки є зміст положень Стратегії. У цьому документі чітко визначено її мету – створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави [7].

Для досягнення такої мети необхідним є: створення національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби з кіберзагрозами військового характеру, кібершпигунством, кібертероризмом і 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, і порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки та оборони України (критична інформаційна інфраструктура) [7].

Надзвичайно позитивним, на нашу думку, є визначення у Стратегії тих чинників, що є провідними для порушення кібербезпеки в Україні та які варто усунути. Мова йде про: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень безпеки критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз; безсистемність заходів кіберзахисту критичної ін-

формаційної інфраструктури; недостатній розвиток організаційно-технічних аспектів кібербезпеки та кіберзахисту критичної інформаційної інфраструктури і державних електронних інформаційних ресурсів; недостатня ефективність суб'єктів сектору безпеки та оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кіберзахисту [7].

Очевидним є те, що втілення закріплених у Стратегії ідей вимагає здійснення практичних заходів, що мають бути чіткими, логічними та взаємоузгодженими. Їх план затверджується Кабінетом Міністрів України.

Так, розпорядженням Уряду від 24 червня 2016 року № 440-р було затверджено відповідний план заходів, що включає двадцять чотири завдання, які мали бути виконані протягом 2016 року за наступними напрямками:

– нормативно-правове забезпечення діяльності у сфері «кібербезпеки» (гармонізація законодавства із захисту державних інформаційних ресурсів, упровадження системи незалежного аудиту інформаційної безпеки об'єктів критичної інфраструктури тощо);

– створення технологічної складової національної системи кібербезпеки;

– налагодження тісного співробітництва з міжнародними партнерами України;

– налагодження процесу підготовки кадрів у сфері кібербезпеки [8].

Звіт про виконання протягом 2016 року заходів із метою реалізації Стратегії станом на лютий 2017 року відсутній, а тому надати об'єктивну оцінку тому, що вдалось або невдалось, зробити неможливо.

При цьому такий звіт у найближчий час має з'явитись, оскільки в пункті 2 Рішення визначено обов'язок Кабінету Міністрів України разом зі Службою безпеки України, Службою зовнішньої розвідки України та за участю національного інституту стратегічних досліджень інформувати щопівроку про стан реалізації Стратегії [6].

Варто також звернути увагу, що в пункті 3 Рішення визначено необхідність утворення, згідно зі статтею 14 Закону України «Про Раду національної безпеки і оборони України», Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України [6].

Правовий статус Національного координаційного центру кібербезпеки («Центр») закріплено в Положенні про Національний координаційний центр кібербезпеки, що затверджено Указом Президента України від 07 червня 2016 року № 242/2016 («Положення № 242») [9].

Згідно з пунктом 10 Положення № 242, рішення Центру є обов'язковими для розгляду органами державної влади, місцевого самоврядування, військовими формуваннями, утвореними відповідно до Законів України, підприємствами, установами, організаціями [9]. Отже, рішення Центру не є обов'язковими для виконання. Це характеризує Центр радше як координаційний, а не виконавчий орган. Отже, доходимо висновку, що створення Центру не вирішило проблему відсутності в Україні єдиного виконавчого органу щодо кіберзахисту.

Незважаючи на те, що в пункті 3 Стратегії наведено перелік основних суб'єктів забезпечення кібербезпеки, серед яких уже згадана Рада національної безпеки і оборони України, а також Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, все ж доводиться констатувати, що кожен із цих органів за можливості вирішує питання кіберзахисту, проте досі вони не роблять цього системно.

СБУ і МВС в особі Управління боротьби з кіберзлочинністю опинилися на вістрі війни з «кіберами». На жаль, їхніх зусиль замало. Загальною проблемою є як недостатня кількість судових експертів у галузі комп'ютерно-технічної експертизи, так і складнощі з введенням у правове поле досліджень фахівців недержавних організацій. Практика показує, що термін здійснення комп'ютерно-технічних експертиз становить від півроку і вище через високу завантаженість профільних державних установ [1].

Надзвичайно важливим у боротьбі з кіберзлочинністю є забезпечення розслідування завдяки наданню науково обґрунтованих криміналістичних рекомендацій.

Значну роль у протидії кіберзлочинності та реалізації вище перелічених заходів може відіграти широкий спектр засобів сучасної криміналістики, спрямованих на:

1) масштабну інтеграцію до криміналістики знань із галузі інформатики та розроблення окремої криміналістичної теорії (вчення) про електронний слід, у межах якої необхідно визначити теоретичні основи електронного слідознавства, вивчити закономірності виникнення електронних слідів, що відображають механізм злочину, розробити рекомендації із застосування методів і засобів їх виявлення, фіксації, вилучення й аналізу з метою встановлення обставин, що мають істотне значення для розкриття, розслідування та попередження злочинів;

2) модернізацію навчального курсу з криміналістики у напрямку поглибленого вивчення: прийомів і методів процесуально-коректного виявлення, фіксації та вилучення різних електронних слідів, а також трансформації виявлених інформаційних масивів у процесуальні форми, доступ-

ні для сприйняття всіма учасниками провадження, техніко-криміналістичного забезпечення й огляду комп'ютерної техніки, а також вилучення електронних документів; вимог до кваліфікації слідчого, понятих і спеціалістів, що залучаються до участі в названих та інших слідчих (розшукових) діях; форм взаємодії з адміністраторами мережевої безпеки і заходів з нейтралізації технічної протидії слідству, спрямованої на знищення електронних слідів; можливостей сучасної експертизи з дослідження слідів зазначеного виду та методичних рекомендацій із забезпечення експертизи репрезентативним обсягом об'єктів дослідження. Формування професійних навичок з об'єктивного, повного та всебічного встановлення обставин розслідуваного злочину потребує набуття знань щодо здійснення аналізу та синтезу даних, отриманих із галузі високих технологій, з «класичною криміналістичною слідовою картиною», виявленою за допомогою традиційних криміналістичних методик.

3) подальший розвиток методики дослідження комп'ютерної техніки та програмних продуктів, а також телекомунікаційних систем і засобів, у межах яких шляхом дослідження електронних слідів вирішується широке коло діагностичних та ідентифікаційних завдань. Особливості механізму утворення і трансформації цифрових слідів повинні враховуватись під час здійснення і широкого кола інших криміналістичних експертиз, наприклад: технічної експертизи документів для встановлення документа, виготовленого шляхом монтажу із застосуванням копіювально-розмножувальної та комп'ютерної техніки; ідентифікації особи, яка надрукувала текст із використанням комп'ютерної техніки, виготовила зображення відтиску печатки з використанням програмного забезпечення за особливостями навичок виконавця; установленні типу та ідентифікації комп'ютерної техніки за виготовленим за її допомогою документом; експертизи відеозвукозапису та фототехнічної експертизи для вирішення завдань ідентифікації знімальної апаратури за електронними файлами фото / відеозаписів, ідентифікації осіб, предметів, приміщень та ділянок, відображених на записах, у тому числі за допомогою геоінформаційних систем, відновлення первісних зображень у фото / відео файлах тощо [10, с. 19 – 20].

На національному рівні для розслідування кіберзлочинів потрібен добре підготовлений штат співробітників і вдосконалене національне законодавство з метою формування ефективної правової основи для забезпечення слідчої, оперативно-розшукової діяльності правоохоронних органів і спецслужб у боротьбі з такими злочинами.

Позитивним кроком у напрямку реалізації кібербезпеки в Україні є прийняття Верховною Радою України 20 вересня 2016 року Проекту Закону «Про основні засади забезпечення кібербезпеки в Україні» № 2126а від 19 червня 2015 року [11].

На підставі вищевикладеного доходимо висновку, що створення основ інституційно-організаційного, законодавчого та наукового забезпечення кібербезпеки в Україні розпочалось у 2016 році та вже має позитивні результати.

У той же час важливо розуміти, що проблема профілактики та боротьби з кіберзлочинністю в Україні є комплексною. Сьогодні закони повинні відповідати вимогам, висунутим сучасним рівнем розвитку комп'ютерних технологій. Пріоритетним напрямком є також організація взаємодії та координація зусиль правоохоронних органів, спецслужб, судової системи як на національному, так і на міжнародному рівні.

Література

1. Довбиш М. Кіберзлочинність в Україні. – [Електронний ресурс]. – Режим доступу: https://www.science-community.org/ru/node/16132.

2. Іванченко О. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні // Актуальні проблеми вітчизняної юриспруденції. – 2016. – № 3. – С. 172 – 177.

3. Конвенція про кіберзлочинність від 23 листопада 2011 року. – [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_575/print1453722395322329.

4. Орлов О., Онищенко Ю. Організаційні та нормативно-правові засади боротьби з кіберзлочинністю // Державне управління: удосконалення та розвиток. – 2014. – № 5. – [Електронний ресурс]. – Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=715.

5. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року № 96/2016. – [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/96/2016.

6. Про стратегію кібербезпеки України: Рішення Ради національної безпеки і оборони України від 27 січня 2016 року. – [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/n0003525-16/paran2#n2.

7. Стратегія кібербезпеки України. – [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/96/2016#n11.

8. Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України від 24 червня 2016 року № 440-р. – [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/440-2016-%D1%80.

9. Про національний координаційний центр кібербезпеки: Указ Президента України від 07 червня 2016 року № 242/2016. – [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/242/2016.

10. Білоус В. Роль засобів криміналістики у протидії кіберзлочинності // Міжнародні стандарти з кібербезпеки та їх застосування в Україні (матеріали «круглого столу» м. Харків, 19 квіт. 2016 р.) / за ред. А. Гетьмана, Б. Головкіна. – Х.: Право, 2016. – 88 с.

11. Про основні засади забезпечення кібербезпеки України: Проект Закону № 2126а від 19 червня 2015 року. – [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

Анотація

Семенов В. В., Дзігора М. С. **До питання боротьби з кіберзлочинністю в Україні.** – Стаття.

У статті розглянуто заходи, вжиті у законодавчій, інституційній сфері в Україні, напрями науково-криміналістичного забезпечення, спрямовані на боротьбу з кіберзлочинністю.

Ключові слова: кіберзлочин, кібербезпека, класифікація кіберзлочинів, суб'єкт забезпечення кібербезпеки.

Аннотация

Семенов В. В., Дзигора М. С. **К вопросу борьбы с киберпреступностью в Украине.** – Статья.

В статье рассмотрены меры, принятые в законодательной и институционной сфере в Украине, направления научно-криминалистического обеспечения, обращенные на борьбу с киберпреступностью.

Ключевые слова: киберпреступность, кибербезопасность, классификация киберпрестпулений, субъект обеспечения кибербезопасности.

Summary

Semenov V. V., Dzihora M. S. **The question as to struggle against cybercrime in Ukraine.** – Article.

This article is about the measures which were taken in the domestic legislative, institutional spheres in Ukraine and scientific – criminalistic guarantee with the aim to struggle the cybercrime.

Key words: cybercrime, cybersecurity, cybercrimes classification, subject who provided the cybersecurity.