УДК 343.3

НАПРЯМИ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ ПРОТИ ВЛАСНОСТІ

Юрій ПІЦИК,
здобувач
Міжрегіональної академії управління персоналом

АНОТАЦІЯ

У статті проведено дослідження основних напрямів у сфері протидії злочинам проти власності, що вчиняються у кіберпросторі. З цією метою проаналізовано сучасний стан проблеми та запропоновано систему заходів щодо протидії кіберзлочинам проти власності в Україні.

Ключові слова: кіберзлочини, кіберзлочини проти власності, злочини у сфері інформаційних відносин, кіберзлочинність, комп'ютерні злочини.

AREAS OF RESISTANCE AGAINST CYBERCRIME AGAINST PROPERTY

Yurii PITSYK,
Applicant of the Interregional Academy of Personnel Management

SUMMARY

The article deals with the study of the main areas in the field of counteraction to property crimes committed in cyberspace. To this end, the current state of the problem is analyzed and a system of measures to combat cybercrime against property in Ukraine is proposed.

Key words: cybercrime, cybercrime against property, crimes in the field of information relations, cybercrime, computer crimes.

Постановка проблеми. Забезпечення оптимального рівня кібербезпеки є необхідною умовою розвитку сучасного інформаційного суспільства. В умовах розвитку інформаційних процесів, їх інтеграції в різні сфери суспільного життя людство приділяє посилену увагу створенню й удосконаленню ефективних систем захисту від зовнішніх і внутрішніх загроз кібернетичного характеру. У переважній більшості розвинених країн світу вже сформовані загальнодержавні системи кібербезпеки, здатні за невеликий проміжок часу акумулювати сили та засоби різних державних (у т. ч. правоохоронних) органів для протидії кіберзагрозам.

У нашій державі також відбувається процес формування системи кібербезпеки. Зокрема, її правову основу становлять Конституція України, Закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади кібербезпеки України» та ін. Доцільно у цьому аспекті згадатий Конвенцію Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Стратегію кібербезпеки України тощо.

Стан дослідження. Вивченню питання кіберзлочинності в різних аспектах присвячені наукові праці К. Бєлякова, В. Білоус, В. Бутузова, А. Войціховського, О. Волеводза, Д. Гавловського, В. Голубєва, В. Гуславського, Ю. Дорохіної, М. Литвинова, Е. Рижкова, В. Розовського, Т. Тропиної, В. Цимбалюк, О. Юхно.

Метою статті є аналіз напрямів у сфері протидії злочинам проти власності, що вчиняються у кіберпросторі.

Виклад основного матеріалу. Розповсюдження кіберзлочинів, у т. ч. шахрайства з пластиковими платіжними картками, крадіжки коштів із банківських рахунків, викрадення комп'ютерної інформації – це далеко не повний перелік кіберзлочинів проти власності. Такі злочини характеризуються певними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, завданням шкоди в особливо великих розмірах навіть у разі вчинення одиничного злочину.

Взагалі кіберзлочини можна класифікувати на два види: традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету, та нові злочини, що стали можливими завдяки новітнім комп'ютерним технологіям. Так, за оцінками експертів, в останні місяці в управлінні з боротьби з кіберзлочинністю тільки в Києві фіксується до двадцяти випадків кіберкрадіжки грошей через клієнт-банк, де суми збитку становлять від 20 тис. до 40 млн грн.

Вивчивши історію виникнення кіберзлочинності в Україні та інших країнах, визначивши основні види кіберзлочинів проти власності, виявивши їх основні причини й умови, можна сформувати систему заходів протидії кіберзлочинів проти власності в Україні, зокрема спрямованих на:

1) виявлення, усунення або послаблення і нейтралізацію причин кіберзлочинності проти власності;

2) виявлення й усунення ситуацій, що безпосередньо мотивують або провокують на вчинення злочинів проти власності в кіберпросторі;

3) виявлення осіб підвищеного кримінального ризику і зниження цього ризику;

4) виявлення осіб, поведінка яких вказує на реальну можливість вчинення кіберзлочинів проти власності, і розробка шляхів стримуючого і коригуючого впливу на них.

За способом протидії ці заходи слід розділити на дві основні групи: правові та кримінологічні.

Правові заходи спрямовані на одну з основних умов майнової кіберзлочинності – недосконаліть законодавства. Вони включають пропозиції щодо вдосконалення законодавства про кримінальну відповідальність за кіберзлочини проти власності. Такі заходи нерозривно пов'язані з організаційними, оскільки вони забезпечують їх виконання на законодавчому рівні. Без належного правового регу-

лювання більшість організаційних заходів будуть неефективними.

Кримінологічні заходи включають пропозиції щодо протидії таким детермінантам майнової кіберзлочинності, як анонімність злочинців, екстериторіальність злочинів проти власності, відсутність культури цифровий безпеки у населення і наявність субкультури хакерів.

Кримінологічні заходи містять пропозиції щодо профілактики інформаційної безпеки серед окремих груп населення, пропозиції щодо вдосконалення інформаційних технологій, а також пропозиції щодо кваліфікації злочинів проти власності, вчинених у кіберпросторі. Оскільки всі кіберзлочини проти власності за способом їх вчинення й об'єктом посягання можна поділити на дві самостійні групи (кіберзлочини проти власності, що вчиняються шляхом впливу на людину, і кіберзлочини проти власності, що вчиняються шляхом впливу на обладнання), то і заходи протидії кіберзлочинам проти власності за об'єктом протидії можна розділити на соціальні і технічні.

Соціальні заходи спрямовані на розвиток соціальних якостей громадян (користувачів кіберпростору): розвиток культури інформаційної безпеки й інформаційної грамотності, а також викорінення субкультури хакерів. Соціальні заходи щодо способу протидії можна розділити на правові та кримінологічні.

Відсутність чітко визначених кордонів у кіберпросторі створює безліч труднощів у притягненні винних до кримінальної відповідальності, і єдине рішення проблеми транскордонності кіберзлочинів проти власності, на нашу думку, полягає в розвитку тісного міжнародного співробітництва.

Україна бере активну участь у міжнародному співробітництві у боротьбі з кіберзлочинами, в т. ч. і з кіберзлочинами проти власності. За останні п'ятнадцять років Україна уклала десятки угод про співпрацю у цій сфері, у яких держави домовляються про співпрацю щодо протидії кіберзлочинам (у т. ч. і кіберзлочинами проти власності), про встановлення кібербезпеки, а також щодо ефективного захисту кіберпростору.

Однак міждержавні угоди, на наш погляд, є лише першим етапом реального міжнародного співробітництва щодо протидії кіберзлочинності. На цьому етапі вводяться основні правила і принципи протидії, визначаються терміни і поняття, встановлюються напрями такої роботи.

Проте, ґрунтуючись на проведеному нами дослідженні, можна зробити висновок, що вітчизняний законодавець не приділяє належної уваги протидії кіберзлочинам проти власності. Лише в одній статті VI розділу Особливої части КК України (ч. 3 ст. 190 КК України) встановлено спеціальний спосіб вчинення кіберзлочину проти власності – шляхом незаконних операцій із використанням електронно-обчислювальної техніки.

На наш погляд, необхідно визнати використання кіберпростору з метою вчинення злочину обставиною, що підвищує його суспільну небезпеку. Тому пропонуємо ввести в основний склад ст. 189 КК України «Вимагання» таку ознаку, як вчинення вказаного злочину: «під загрозою видалення, блокування або модифікації комп'ютерної інформації, а так само під загрозою іншого втручання у функціонування засобів зберігання, обробки або передачі комп'ютерної інформації або інформаційно-телекомунікаційних мереж, яке може завдати істотної шкоди правам чи законним інтересам потерпілого або його близьким».

Основні кримінологічні засади протидії кіберзлочинам закріплені у Стратегії кібербезпеки України, розробленій на виконання Стратегії національної безпеки України від 2015 р., затвердженій рішенням Ради національної безпеки і оборони України (далі – РНБО) та введеній у дію Указом Президента України 27 січня 2016 р. Провідним розробником Стратегії кібербезпеки України виступила Державна служба спеціального зв'язку та захисту інформації (далі – Держспецзв'язок). У роботі над документом брали активну участь представники Громадської Ради при Держспецзв'язку, представники приватного бізнесу, експерти НАТО, ОБСЄ, RAND corporation. Документ ретельно узгоджувався з усіма іншими державними структурами, що мають відношення до кібербезпеки, доопрацьовувався в Кабінеті Міністрів, у РНБО.

Стратегія кібербезпеки базується на положеннях Конвенції Ради Європи про кібрзлочинність та має на меті створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Для цього передбачається: створення національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного 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 перебувають під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки й оборони України (критична інформаційна інфраструктура).

Головними перевагами цієї Стратегії є:

– дотримання європейського підходу до забезпечення кібербезпеки як до спільної відповідальності усіх ключових стейкхолдерів;

– орієнтація на стандарти ЄС та НАТО в сфері забезпечення кібербезпеки замість застосування пострадянських або виключно радянських стандартів;

– відмова від пріоритету «захисту національного сегмента Інтернету», який є притаманним російському та китайському підходам до кібербезпеки.

Стратегія закладає загальну архітектуру національної системи кібербезпеки та розподіляє завдання і повноваження між основними суб'єктами забезпечення кібербезпеки (РНБО, Міністерством оборони, Генеральним штабом Збройних Сил, Державною службою спеціального зв'язку та захисту інформації, Службою безпеки, Національною поліцією, Національним банком, розвідувальними органами України), передбачає створення умов для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян. Ухвалення Стратегії є важливим кроком у розбудові системи національної кібербезпеки, вкрай необхідним, але недостатнім, адже Стратегія не пропонує відповідної термінології та не передбачає внесення змін до чинних нормативно-правових актів. Ці питання планувалося врегулювати під час написання Закону України про кібербезпеку, який і було прийнято у другому читанні 05 жовтня 2017 р.

Профілактика кіберзлочинності, підвищення інформаційної досвідченості громадян – такі ідеологічні заходи протидії кіберзлочинності є цілим комплексом методів і засобів протидії, спрямованих на усунення в певних групах і у певних індивідів антигромадських установок, а також на вироблення негативного суспільного ставлення до кіберзлочинців.

До них можна віднести діяльність традиційних та Інтернет-ЗМІ, заняття в школах і вищих навчальних закладах, заняття на курсах підвищення кваліфікації тощо.

Однак конкретні заходи будуть найбільш ефективні лише для конкретної аудиторії. Оскільки простежується тенденція до зниження середнього віку кіберзлочинця і його жертви, збільшення загального числа неповнолітніх кіберзлочинців, найбільш ефективним методом ідеологічного впливу на них буде інформування про кіберзлочини та кримінальну відповідальність за їх вчиненняу кіберпросторі.

Популярність різних соціальних мереж серед неповнолітніх є необхідною умовою ефективної профілактики кіберзлочинності, а якщо врахувати, що понад 75% дітей мають профіль у соціальних мережах, майже третина мають більше одного профілю в різних соціальних мережах і відвідують їх майже щодня, то така профілактика буде максимально ефективною. Крім того, оскільки користуватися комп'ютером і «Інтернетом» починають вже з малих років (5–6 років), то культуру інформаційної безпеки необхідно закладати вже з цього віку.

Необхідно виробити у користувачів кіберпростору стійку звичку перевіряти свій комп'ютер на віруси, встановлювати захисні програми і вчасно оновлювати їх. Звісно ж, така корисна звичка повинна бути прищеплена в дитинстві, як звичка чистити зуби або мити руки. Необхідно уберегти користувачів кіберпростору від безконтрольного поширення персональних даних. Так само, як на вулиці не можна заводити розмови з незнайомцями, так і в соціальних мережах або по електронній пошті це робити не бажано. Більш того, у такому спілкуванні необхідно бути більш пильним, ніж у живому, хоча б тому, що ви не бачите свого співрозмовника.

Побудова дієвої системи забезпечення кібербезпеки вимагає від державних органів України чіткого визначення державної політики у цій сфері та випереджального реагування на стрімкі зміни, що відбуваються у світі в сфері забезпечення кібербезпеки. Вибір конкретних засобів і шляхів забезпечення кібербезпеки України зумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру та масштабам реальних і потенційних кібернетичних загроз життєво важливим інтересам людини і громадянина, суспільства і держави.

Організаційне забезпечення системи кібербезпеки також можна розглядати як цілеспрямовану діяльність суб'єкта забезпечення кібербезпеки, пов'язану зі:

– створенням і впорядкуванням (розвитком) організаційних структур, найбільш доцільних для забезпечення безпеки у кіберпросторі;

– впорядкуванням (налагодженням) процесу управління у сфері забезпечення безпеки у кіберпросторі, забезпеченням найліпших умов для прийняття та реалізації відповідних управлінських рішень [1].

Висновки. Підсумовуючи вищенаведене, доцільно вказати, що позитивним моментом є те, що переважна більшість країн світу розпочали просування проектів стратегій кібербезпеки, у т. ч. і Україна. Система національної кібербезпеки є її спеціальною підсистемою національної системи безпеки, мета функціонування якої полягає у забезпеченні її функціонування та розвитку. Національну систему кібербезпеки пропонується розглядати як сукупність суб'єктів забезпечення кібербезпеки, які взаємодіють з метою забезпечення відсутності безпеки для індивіда, суспільства і держави.

Очевидною є необхідність створення Національної системи кібербезпеки, якою займатимуться відповідні підрозділи СБУ, ДСТСЗІ та МВС. Координацію й ефективну взаємодію забезпечуватиме відповідний підрозділ РНБО.

У зв'язку з цим доцільно вказати, що в нашій державі продовжується робота та розвиток основних засад протидії у досліджуваній сфері. Так, за інформацією, наданою прес-службою Держспецзв'язку, 02 лютого 2018 р. за участі Секретаря РНБО України Олександра Турчинова відбулося відкриття Центру реагування на кіберзагрози Держспецзв'язку.

Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC) створено Держспецзв'язку як центральний компонент і ядро національної системи кіберзахисту України. CRC побудовано на базі найновітніших досягнень у сфері кібербезпеки провідних вітчизняних і світових ІТ-компаній. Розроблені на рівні кращих світових аналогів, сучасні технологічна й аналітична системи CRC закономірно претендують на звання найпотужніших у європейському співтоваристві.

Систему CRC можна порівняти з розбудовою кордону захисту держави в кіберпросторі, зі створенням першої лінії її оборони від кіберагресій, а сам Центр є своєрідним «генеральним штабом» для сил кіберзахисту України.

«Україна активно розбудовує національну систему кібербезпеки, і сьогодні для цього зроблено черговий потужний ривок», – зазначив Голова Держспецзв'язку Леонід Євдоченко. Завдяки втіленим у CRC унікальним технологічним рішенням, Держспецзв'язку здатна з високим ступенем точності здійснювати у режимі «24/7» раннє виявлення аномальних активностей і потенційно небезпечних подій у системах і мережах, підключених до Інтернет. Час реагування на кіберзагрози та сповіщення про них скоротився в десятки разів. «Сьогодні принципово змінюється тактика кіберзахисту. Від реагування постфактум, тобто вже після масштабного заподіяння шкоди інформаційним ресурсам і системам, як це відбувалося під час останніх кібератак минулого року, ми переходимо до дій на випередження та максимальної локалізації можливих уражень», – звертаючись до присутніх зауважив О. Турчинов. CRC – це ще й технічна платформа взаємодії основних суб'єктів забезпечення кібербезпеки (Держспецзв'язку, СБУ, Нацполіції), що на порядок підвищує ефективність і оперативність діяльності правоохоронних структур із протидії та розслідування кіберзлочинів. Це ефективний механізм координації зусиль усіх учасників кіберзахисту державного та приватного секторів, який є однією з ключових ланок прийняття оперативних рішень Національним центром кібербезпеки РНБО України.

Можна без перебільшення сказати, що CRC Держспецзв'язку вже сьогодні здатен забезпечити один із найвищих в ЄС рівнів кіберзахисту контуру безпеки державних інформаційних ресурсів, державних реєстрів та елементів критичної інфраструктури [2].

Утім, незважаючи на те, що необхідний комплекс організаційно-правових і технічних заходів щодо протидії кіберзлочинності взагалі та майнової кіберзлочинності (кіберзлочинам проти власності) зокрема ще перебуває на етапі створення, його розробка має відбуватися з активним, проте оптимальним запозиченням зарубіжного досвіду.

Список використаної літератури:

1. Діордіца І.В. Поняття та зміст національної системи кібербезпеки. URL: http://goal-int.org/ponyattyata-zmist-nacionalnoi-sistemi-kiberbezpeki/.

2. У Держспецзв'язку відбулося відкриття найпотужнішого в ЄС Центру реагування на кіберзагрози. URL: http://www.dsszzi.gov.ua/dsszzi/ control/uk/publish/article?art_id=286338&cat_id=284576.

ІНФОРМАЦІЯ ПРО АВТОРА

Піцик Юрій Миколайович – здобувач Міжрегіональної академії управління персоналом

INFORMATION ABOUT THE AUTHOR

Pitsyk Yurii Mykolaiovych – Applicant of the Interregional Academy of Personnel Management