УДК 004.056.5(477)(045)

Н. Б. Шуст
доктор соціологічних наук, професор,
професор кафедри цивільного права і процесу
Національного авіаційного університету

Т. С. Ярошенко
студентка
Національного авіаційного університету

А. В. Яценко
студентка
Національного авіаційного університету

ТЕОРЕТИКО-ПРАВОВІ ПИТАННЯ КІБЕРБЕЗПЕКИ У СФЕРІ ІНТЕРНЕТУ ТА ЇЇ СТАНУ В УКРАЇНІ, СПОСОБИ ЗАХИСТУ ВІД КІБЕРЗЛОЧИНІВ

Сьогодні неможливо оминути увагою зростаючу роль кібербезпеки. Щодня кожній людині доводиться стикатися з необхідністю користування інформаційними технологіями, починаючи від соціальних мереж і розміщення інформації про свої персональні дані в Інтернеті й до користування банкоматами, банківськими рахунками і т. п. У зв'язку із цим питання врегульованості цієї проблеми чинним законодавством і захисту від кіберзлочинців є актуальним і водночас вагомим як для українців, так і для всієї світової спільноти.

Водночас, незважаючи на зростаючий рівень технологічності нових викликів і кібернетичних атак, значна їх частина розрахована не на подолання складної системи кібернетичного захисту, а на рядового користувача, зокрема, на його недосвідченість і необізнаність у питаннях кібернетичної безпеки та захисту інформації. Стійкість системи до сучасних викликів і загроз визначається насамперед умінням кожного користувача розпізнавати атаки, спрямовані безпосередньо на нього, і протидіяти їм [1].

Серед науковців сутність і проблематику кібернетичної безпеки в Україні розглядали В.Б. Толубко, В.О. Хорошко, І.М. Сопілко та багато інших.

Так, О.А. Баранов у статті «Про тлумачення та визначення поняття «кібербезпека» визначає, що кібербезпека – це такий стан захищеності життєво важливих інтересів особистості, суспільства й держави в умовах використання комп'ютерних систем і/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через неповноту, невчасність і невірогідність інформації, що використовується [2, с. 44]. В.Н. Фурашов висловив таке ж твердження, але вже в спрощеному вигляді: кібербезпека – це стан здатності людини, суспільства й держави запобігати й уникати спрямованого (насамперед несвідомого) негативного впливу (управління) інформації.

У підручнику «Інформаційна та кібербезпека: соціотехнічний аспект» (В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко та С.В. Толюпа) зазначається, що стан кібернетичної безпеки досягається завдяки сукупності активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо ІР, ІКТ і ІТС.

С.В. Мельник, О.О. Тихомиров, О.С. Лєнков у праці «До проблеми формування понятійно-термінологічного апарату кібербезпеки» визначили, що в контексті нормативно-правового розуміння національної й інформаційної безпеки кібербезпека може визначатися як захищеність життєво важливих інтересів людини й громадянина, суспільства й держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем.

Метою статті є аналіз поняття кібербезпеки, особливості законодавчого регулювання цього питання в Україні, а також дослідження шляхів захисту персональних даних, дослідження питання покарання за кіберзлочинність і діяльність у цій сфері правоохоронних органів.

Правову основу кібернетичної безпеки України становлять Конституція України, Закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», інші закони, Конвенція Ради Європи про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, Доктрина інформаційної безпеки України, а також видані на виконання законів інші нормативно-правові акти [3, с. 312].

За роки незалежності України питання кібернетичної й інформаційної безпеки розвивалося за залишковим принципом. Нормативно-правові

документи з регулювання цієї сфери розроблялися безсистемно, нерідко базуючись на застарілих радянських нормах і вступаючи в протиріччя один з одним. Це призвело до гнітючого становища в системі кібернетичної безпеки й інформаційно-комунікаційних технологій узагалі. Україна кожен рік потрапляла в антирейтингові списки щодо піратства, розповсюдження шкідливого програмного забезпечення, DDoS-атак та ін. Так, відповідно до дослідження корпорації Майкрософт (Microsoft Corporation), на 86% комп'ютерів в Україні встановлене неліцензійне програмне забезпечення. У той же час у центральних органах державної влади України використовують 60% неліцензійного програмного забезпечення. Отже, використання неліцензійного програмного забезпечення – це прямий шлях для надання доступу хакерам до ресурсів систем, на яких воно встановлене [4].

Саме поняття «кібербезпека» можна визначити як стан захищеності кіберпростору держави в цілому чи окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним або національним інтересам [5, с. 15].

Основою кіберзлочинів, згідно з чинним законодавством України, є суспільно небезпечні діяння, що закріпленні в окремому розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України (далі – КК України). Із погляду кримінального права до кіберзлочинів належать тільки злочини, передбачені розділом XVI КК України, а в рамках криміналістики доцільно включити до цього поняття інші злочини, для скоєння яких використовується комп'ютер і Інтернет. Проте в розділі зовсім відсутні поняття, пов'язані з кібербезпекою, натомість є лише деякі поняття злочинів, які вчиняються за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Розділ складається з декількох статей:

– ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»;

– ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;

– ст. 361-2 «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. 362 «Викрадання, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем»;

– ст. 363 «Порушення правил експлуатації автоматизованих електронно-обчислювальних систем»;

– ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» [6].

Розглядаючи нормативно-правову базу у сфері регулювання кібербезпеки України, можна виділити деякі проблеми:

– відсутність єдиного понятійного апарату та норм щодо кваліфікації комп'ютерних злочинів;

– відсутність у державі розвинутих інститутів програмно-технічної та судово-кібернетичної експертизи як одного з головних механізмів у процесі документування та закріплення доказів «комп'ютерного» злочину та відповідних методик їх проведення;

– відсутність необхідного рівня координації та взаємодії між відповідними підрозділами правоохоронних структур під час проведення адекватних загрозам у зазначеній сфері запобіжних і правозастосовних заходів;

– малорозвинена загальнодержавна система протидії кіберзлочинності [7, с. 167].

Пріоритетами у вдосконаленні нормативно-правової бази сфери кібербезпеки є:

– розвиток і вдосконалення системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів із питань кібербезпеки та кіберзахисту;

– розроблення нових методів запобігання кібератакам, кіберінцидентам і поширенню інформації про них;

– здійснення захисту технологічних процесів на об'єктах критичної інфраструктури, в яких управління чи моніторинг здійснюється за допомогою інформаційно-комунікаційних технологій, від несанкціонованого втручання в їх роботу;

– удосконалення загальнодержавної системи протидії кіберзлочинності [8].

Нині в Україні чинний Указ Президента «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України», відповідно до якого передбачається створення національної системи кібербезпеки, посилення спроможностей суб'єктів сектора безпеки й оборони для забезпечення ефективної боротьби з кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом і кіберзлочинністю, поглиблення міжнародного співробітництва в 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 й оборони України (критична інформаційна інфраструктура) [9].

Також у майбутньому на нас чекає прийняття ЗУ «Про про основні засади забезпечення кібербезпеки України», який стане фундаментальною основою всього правового регулювання кібербезпеки України. Проте без практичного втілення ці нормативно-правові акти є лише текстовими носіями. Виникає запитання: чию діяльність вони будуть регулювати? Для цього в Україні створено відповідний правоохоронний орган – кіберполіцію. Основною метою створення кіберполіції стало реформування та розвиток підрозділів МВС України, що забезпечить підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних і слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності. Поетапне перетворення сучасної моделі створить новітній орган правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєво реагувати на кіберзлочини та кіберзагрози, а також відповідно до кращих світових стандартів проводитиме міжнародну співпрацю зі знешкодження транснаціональних злочинних угрупувань у цій сфері. До основних завдань кіберполіції відносять такі:

1) реалізація державної політики у сфері протидії кіберзлочинності;

2) протидія кіберзлочинам:

– у сфері використання платіжних систем:

– скімінг (шимінг) – незаконне копіювання вмісту треків магнітної смуги (чипів) банківських карток;

– кеш;

– трепінг – викрадення готівки з банкомату шляхом установлення на шатер банкомату спеціальної утримуючої накладки;

– кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів без підтвердження держателя;

– несанкціоноване списання коштів із банківських рахунків за допомогою систем дистанційного банківського обслуговування;

– у сфері електронної комерції та господарської діяльності:

– фішинг – виманювання в користувачів Інтернету їхніх логінів і паролів до електронних гаманців, сервісів онлайн-аукціонів, переказування або обміну валюти тощо;

– онлайн-шахрайство – заволодіння коштами громадян через Інтернет;

– аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

У сфері інтелектуальної власності:

– піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті;

– кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного ТВ;

– у сфері інформаційної безпеки:

-соціальна інженерія – технологія управління людьми в Інтернет-просторі;

– мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;

– протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства;

– рефайлінг – незаконна підміна телефонного трафіку [10].

В Україні стан кібербезпеки залишається досить складним. Через те, що питанню кібербезпеки довгий час не приділялася увага, наразі маємо високі показники піратства в мережі Інтернет, слабку нормативну базу, застарілі види відповідальності за кіберзлочини в Кримінальному кодексі, слабку систему захисту даних державного значення, велику кількість кібератак тощо. Проте останнім часом у зв'язку зі змінами в країні та виходом на новий рівень європейського розвитку кібербезпека стала чи не найактуальнішим питанням, на якому зосередилися всі представники державної влади. Розвиток кібербезпеки України став пріоритетним у державній політиці. Наразі необхідно розширювати нормативно-правову базу, чітко її структурувати, уникаючи виникнення колізій у законодавстві. Потребує змін і доповнень Кримінальний кодекс України в XVI розділі, необхідно внести до нього поняття кіберзлочину та його видів. Ураховуючи те, що кіберполіція є досить новим структурним підрозділом Міністерства внутрішніх справ України, необхідно залучати міжнародний досвід діяльності відповідних органів розвинених країн світу, щоб робота кіберполіції була ефективною та злагодженою.

Україна знаходиться на етапі становлення найвищих європейських цінностей, і розвиток кібербезпеки на її теренах є одним із найактуальніших питань сьогодення.

Література

1. Щоденні кіберзагрози. Офіційний веб-сайт Міністерства оборони України. URL:http://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi.html.

2. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки: зб. матер. наук.-практ. конф. «Актуальні проблеми управління інформаційною безпекою держави». К.: Вид-во НА СБ України, 2011. Ч. 2. С. 43–48.

3. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Наук.-практ. журнал «Боротьба з

організованою злочинністю і корупцією (теорія і практика)». К.: 2012. 324 с.

4. Кібербезпека як ключовий елемент протидії гібридній агресії. URL: https://defence-ua.com/index.php/statti/1359-kiberbezpeka-yak-klyuchovyy-element-protydiyi-hibrydniy-ahresiyi.

5. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. К.: ДУТ, 2015. 288 с.

6. Кримінальний кодекс України: чинне законодавство зі змінами та допов. станом на 1 вересня 2016 р. К.: ПАЛИВОДА А.В., 2016. 212 с.

7. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2. С. 162–169.

8. ІТ-законодавство, проблеми, пріоритети, напрями розвитку. URL: http://aphd.ua/publication-98/.

9. Про Стратегію кібербезпеки України: Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 р. URL: http://zakon0.rada.gov.ua/laws/show/96/2016.

10. Кібербезпека в Україні, Одеса, 21 жовтня 2016 р. URL: http://www.academia.edu/30615672/Кібербезпека_в_Україні_Одеса_21.10.2016

Анотація

Шуст Н. Б., Ярошенко Т. С., Яценко А. В. **Теоретико-правові питання кібербезпеки у сфері Інтернету та її стану в Україні, способи захисту від кіберзлочинів.** – Стаття.

У статті досліджується загальна характеристика, розкривається суть кібербезпеки, її стан в Україні, розкрито актуальні проблеми, а також аналізуються перспективи розвитку цієї сфери діяльності. Розглядаються такі поняття, як кібербезпека, кіберзлочин, кіберзахист, кібератака, кіберполіція.

Ключові слова: кібербезпека, кіберзлочин, кіберполіція, Стратегія кібербезпеки в Україні.

Аннотация

Шуст Н. Б., Ярошенко Т. С., Яценко А. В. **Теоретико-правовые вопросы кибербезопасности в сфере Интернета и ее состояния в Украине, способы защиты от киберпреступлений.** – Статья.

В статье исследуется общая характеристика, раскрывается суть кибербезопасности, ее состояние в Украине, раскрыты актуальные проблемы, а также анализируются перспективы развития этой сферы деятельности. Рассматриваются такие понятия, как кибербезопасность, киберпреступление, киберзащита, кибератака, киберполиция.

Ключевые слова: кибербезопасность, киберпреступление, киберполиция, Стратегия кибербезопасности в Украине.

Summary

Shust N. B., Yaroshenko T. S., Yatsenko A. V. **Theoretical and legal aspects of cybersecurity in the field of Internet and its status in Ukraine, methods of protection against cybercriminals.** – Article.

The article examines the general characteristics, reveals the essence of cyber security, the situation in Ukraine, revealed current problems and analyzes the development prospects of this scope. We consider such concepts as cybersecurity, cyber-crime, cyber, cyber attacks, cyber police.

Key words: cybersecurity, cyber-crime, cyber police, Strategy of cyber security in Ukraine.