УДК 340.13;342.35
DOI https://doi.org/10.32782/2524-0374/2020-4/56

СИСТЕМА ЗДІЙСНЕННЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ У США

SYSTEM OF LEGISLATIVE REGULATION OF CYBER SECURITY IN THE USA

Хом'яков Д.О., к.ю.н,
начальник науково-дослідної лабораторії проблем права воєнної сфери науково-дослідного центру
Військовий інститут
Київського національного університету імені Тараса Шевченка

Коропатнік І.М., д.ю.н., професор,
начальник кафедри правового забезпечення
Військовий інститут
Київського національного університету імені Тараса Шевченка

Сучасна ера є ерою інформаційного суспільства. Виробництво товарів і послуг, розподіл продукції, науково-технічні відкриття – все це відбувається за використання сучасних технологій оброблення й передавання інформації. Інформаційно-телекомунікаційні технології надають небачені раніше можливості в обміні інформацією: змінилися швидкість і якість передавання інформації, збільшилася кількість людей, що можуть одночасно дізнатися й передати інформацію, значно збільшилася кількість користувачів мережі Інтернет, спростився доступ до джерел інформації. Водночас кіберпростір від звичайного способу передавання інформації трансформується у новітній простір здійснення правовідносин і навіть розв'язання конфліктів. Ставлення до кіберпростору в сучасному світі зумовлює появлення нових думок, поглядів і концепцій як серед користувачів мережі, так і серед науковців. Українська держава лише починає формувати правове поле регулювання кіберпростору й правовідносин, які з ним пов'язані. Водночас у світі це питання почали досліджувати ще на початку 1980-х років XX сторіччя. Особлива увага приділяється питанням безпеки в кіберпросторі та кіберзахисту інформаційних ресурсів держав. Також важливим за останнє десятиріччя є питання здійснення кібероборони держав у кіберпросторі. У статті пропонується розглянути досвід здійснення правового регулювання кібербезпекових питань в одній з найбільш розвинених країн світу – Сполучених Штатах Америки. Адже саме Сполучені Штати Америки є найбільш інформаційно розвиненою державою світу, і мережа Інтернет починалася в цій державі. У статті досліджено підходи й порядок здійснення кіберзахисту у Сполучених Штатах Америки, практичне підґрунтя кібероборони, напрям політики держави щодо загроз у кіберпросторі та проаналізовано основні нормативно-правові акти, які регулюють різні аспекти забезпечення кібербезпеки як на рівні всієї держави, так і для захисту окремих громадян.
Ключові слова: кіберпростір, кіберзахист, правове регулювання кіберпростору, кібербезпека, Сполучені Штати Америки.

The modern era is the era of the information society. Production of goods and services, distribution of products, scientific and technical discoveries – all this is done using modern technologies for processing and transmission of information. Information and telecommunication technologies provide unprecedented opportunities in information exchange: the speed and quality of information transmission has changed, the number of people who can simultaneously learn and transmit information has increased, the number of Internet users has significantly increased, people's access to information sources has been simplified. At the same time, cyberspace, from the usual way of transmitting information, is transformed into the latest space for legal relations and even conflict resolution. The attitude to cyberspace in the modern world acquires new thoughts, views and concepts, both among network users and among scientists. The Ukrainian state is just beginning to form a legal framework for regulating cyberspace and related legal relations. At the same time, the world began to study this issue in the early 1980s of the twentieth century. Particular attention is paid to issues of security in cyberspace and the implementation of cyber protection of information resources of states. Also important in the last decade is the issue of cyber defense of states in cyberspace. This article proposes to consider the experience of legal regulation of cybersecurity issues in one of the most developed countries in the world – the United States. After all, the United States of America is the most information-developed country in the world, and the emergence of the Internet itself originates in this country. The article examines the approaches and procedures for cyber defense in the United States, the practical basis for cyber defense, the direction of state policy on threats in cyberspace and analyzes the basic regulations governing various aspects of cybersecurity, both at the state level and on the level of protection individual citizens.
Key words: cyberspace, cyberdefence, legal regulation of cyberspace, cybersecurity, United States.

Питання правового регулювання кібербезпекових аспектів функціонування держави стає дедалі актуальнішим й обговорюваним у всіх країнах світу. Причина такої зацікавленості – розвиток інформаційних технологій і швидка популяризація мережі Інтернет, що викликало необхідність здійснення правового регулювання цієї сфери; крім того, практика показала, що мережа Інтернет використовується не лише для задоволення потреб людей у спілкуванні й обміні інформацією, а також може використовуватися зловмисниками для спричинення шкоди як приватним особам, так і корпораціям, так і державам. З огляду на це гостро постає питання вживання саме кібербезпекових заходів для захисту інформаційних мереж держави та її громадян.

Тому перед правниками постає питання, яким чином та у яких обсягах необхідно здійснювати нормативно-правове регулювання у кіберпросторі.

Для України ця сфера є відносно новою. Лише у 2017 р. було прийнято закон України «Про основні засади забезпечення кібербезпеки України». Хоча цей закон і встановлює деякі основоположні засади щодо регулювання кібербезпеки та процесів, які відбуваються в кіберпросторі, водночас він отримав багато негативних відгуків у науковій спільноті через свою недосконалість і невизначеність термінологічного апарату. Таким чином, можна говорити про те, що в Україні процес розвитку нормативно-правової бази для регулювання процесів і відносин у кіберпросторі перебуває на початковій стадії. Можна також стверджувати, що розходяться й точки зору науковців у сфері інформаційного права щодо того, чи є кіберпростір окремим простором, який потребує регулювання, чи це просто ще один спосіб здійснення вже врегульованих взаємовідносин, як, наприклад, телефонія (тобто як ще один засіб обміну інформацією).

Метою цієї статті є проведення аналізу нормативно-правового регулювання відносин у кіберпросторі в одній із найбільш розвинених країн світу – Сполучених Штатах Америки.

Здійснення аналізу допоможе встановити, які саме сфери кіберпростору підлягають регулюванню та в який

спосіб. Також у статті здійснено огляд органів, до компетенції яких належить забезпечення кібербезпеки у Сполучених Штатах Америки. Аналіз допоможе визначити, на які аспекти кібербезпекових питань варто звернути увагу під час здійснення національного нормативно-правового регулювання кібербезпекових питань.

Сполучені Штати Америки (далі – США) є однією з найбільш розвинутих країн світу як в економічному аспекті, так і у сфері розвитку збройних сил. Тому вважаємо за необхідне розглянути систему нормативно-правового регулювання здійснення кіберзахисту саме в цій державі.

Розробки науковців показують, що першість у забезпеченні інформаційної безпеки у світі належить США. Так, навіть Японія, яка вважається Меккою виробництва цифрової техніки та використання найсучасніших ІТ-технологій, відстає від США більше ніж на п'ять років у сфері розповсюдження персональних комп'ютерів, кабельного телебачення, цифрової телефонії та в інших аспектах інформаційної політики [1, с. 34].

Спершу розглянемо, що є кібербезпекою в розумінні законодавства США. Кодекс Сполучених Штатів Америки, що є зведеною кодифікацією законодавства Сполучених Штатів Америки, у розділі 6 «Внутрішня безпека» визначає цілі забезпечення кіберзахисту: «Термін „мета кібербезпеки" означає мету захисту інформаційної системи або інформації, яка зберігається, обробляється в цій системі або переходить через неї від кібербезпекових загроз або порушень безпеки» [2].

Тобто, можливо зробити висновок, що кібербезпека мереж означає їхню захищеність і захищеність інформації, що проходить або зберігається в цих мережах від порушень, таких як втручання в мережу й незаконний доступ до інформації, яка є в цій мережі. Цікавим та вартим уваги в цьому акті є термін «контроль безпеки», що визначений як «управління, експлуатаційний і технічний контроль, що використовуються для захисту від несанкціонованих втручань з метою негативного впливу на конфіденційність, цілісність і доступність інформаційної системи або її інформації» [2].

Говорячи саме про інформаційну безпеку, складовою частиною якої є кібербезпека, ми можемо стверджувати, що сьогодні законодавство США у сфері забезпечення інформаційної безпеки складається з федеральних законів і законів штатів, які створили правову основу для формування єдиної державної політики в галузі захисту інформації для забезпечення інтересів національної безпеки. Це насамперед такі закони: «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997 р.), «Про комп'ютерне шахрайство та зловживання» (1986 р.), «Про свободу інформації» (1967 р.), «Про висвітлення діяльності уряду», «Про охорону особистих таємниць», «Про таємницю» (1974 р.), «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп'ютерних систем» (1987 р.) [3].

Якщо розглядати практичний аспект здійснення кіберзахисту у США, то донедавна головним виконавчим суб'єктом кіберзахисту США був створений у червні 2003 р. на базі Агенції національної безпеки (National Security Agency, NSA) (далі – АНБ), але підпорядкований Міністерству внутрішньої безпеки (далі – МВБ) Центр комп'ютерної безпеки (National Computer Security Center, NCSC). Нині його реорганізовано в Національний центр кібербезпеки й інтеграції зв'язку (National Cybersecurity and Communication Integration Center, NCCIC) (далі – NCCIC). До складу NCCIC входять Група екстреного реагування на комп'ютерні події в США (U. S. Computer Emergency Response Team, US-CERT) (далі – US-CERT), Група екстреного реагування на надзвичайні події в системах керування промисловістю (Industrial Control Systems Cyber Emergency Response Team, ICS-CERT) (далі – ICS-CERT) і Національний координаційний центр зв'язку (National Coordinating Center for Communications, NCC). US-CERT виявляє кібератаки на ІТС цивільних федеральних органів влади США, попереджає про них адміністраторів безпеки ІТС і координує дії з відновлення федеральних ІТС після кіберінцидентів. Відповідно ICS-CERT виявляє і запобігає здійсненню кібератаки на ІТС критично-важливих об'єктів промисловості США. 16 листопада 2018 р. указом президента США Д. Трампа NCCIC передано до нового Агентства з кібербезпеки й безпеки інфраструктури МВБ США [4, 9].

Тобто у 2018 р. створено новий орган – CISA (Cybersecurity and Infrastructure Security Agency), який на сьогодні є основним, центральним органом, що координує питання здійснення кіберзахисту інформаційно-телекомунікаційної мережі у США. CISA розбудовує національний потенціал для захисту від кібератак і працює з федеральним урядом для надання інструментів кібербезпеки, служб реагування на інциденти й можливостей оцінки для захисту мереж ".gov", які підтримують необхідні операції партнерських відомств й агентств.

CISA координує зусилля щодо безпеки та стійкості, використовуючи надійні партнерські відносини в приватному й державному секторах, і надає технічну допомогу й оцінку федеральним зацікавленим сторонам, а також власникам інфраструктури й операторам по всій країні [5].

Розглядаючи далі питання законодавчого забезпечення кібербезпеки, необхідно зазначити, що законодавство США у сфері зовнішньої інформаційної безпеки складається із сукупності федеральних законів, законів штатів і нормативних актів, які разом створюють правову основу для створення й здійснення державної політики у сфері інформаційної безпеки. Основні з них такі: «Національна стратегія захисту кіберпростору» (2003 р.), «Огляд з кібербезпеки» (Cyber Security Review, 2009 р.), «Ініціатива зі всеосяжної національної кібербезпеки» (2010 р.), Стратегія кібербезпеки США (2011 р.), Закон CISPA (2012 р.) (Cyber Intelliggence Sharring and Protection Act) [6].

У вересні 2018 р. у США була ухвалена Національна кіберстратегія (далі – Кіберстратегія). Основними завданнями цієї Кіберстратегії визначено:

– «захищати Батьківщину, захищаючи мережі, системи, функції та дані;

– сприяти процвітанню Америки шляхом розвитку безпечної, розвинутої цифрової економіки й сильних вітчизняних інновацій;

– зберегти мир і безпеку шляхом зміцнення спроможності США – узгоджено зі союзниками та партнерами – для стримування та, за необхідності, покарання тих, хто використовує кіберінструменти в шкідливих цілях;

– розширити американський вплив за кордоном, щоб розширити основні принципи відкритої, сумісної роботи, надійний і безпечний Інтернет».

Також ця Кіберстратегія визначає, що: «Адміністрація (президента США – *Д. Х.*) визнає, що США беруть участь у постійній конкуренції проти стратегічних супротивників, шахрайських держав і терористичних і злочинних мереж. Росія, Китай, Іран і Північна Корея використовують кіберпростір як засіб кинути виклик США, їхнім союзникам і партнерам, часто з необачністю, яку вони не проявляють в інших областях (просторах). Ці противники використовують кіберінструменти, щоб підірвати нашу економіку й демократію, красти нашу інтелектуальну власність і сіяти розбрат у наших демократичних процесах» [7].

Також в огляді цієї Стратегії хотілося б звернути увагу на розділ «Визначення та встановлення неприйнятної поведінки в кіберпросторі». У цьому розділі зазначається: «Як США продовжують просувати консенсус щодо того, що становить відповідальну державну поведінку в кіберп-

росторі, ми також повинні працювати щодо гарантування наявності наслідків для безвідповідальної поведінки, яка завдає шкоди США й нашим партнерам. Усі інструменти національної влади доступні для запобігання, реагування та стримування зловмисної кібердіяльності проти США. Сюди входять дипломатичні, інформаційні, військові (як кінетична, так і кібер), фінансова, розвідувальна, публічна атрибуція та правоохоронні можливості. Сполучені Штати офіційно оформлять і здійснюватимуть співпрацю з однодумцями для визначення та стримування шкідливої кібердіяльності з інтегрованими наслідками, які дають швидкі, дорогі й прозорі наслідки, коли зловмисники шкодять США чи нашим партнерам [7].

Таким чином, можливо зробити висновок, що у Сполучених Штатах Америки значна увага приділяється викликам, які виникають у кіберпросторі, та розгляду кіберпростору як нової та значущої площини ведення протистояння.

Водночас, говорячи про кіберпростір, ми можемо говорити про декілька видів порушень, які можуть у ньому відбуватися. Тобто кіберпросторові порушення передбачають не лише порушення інтересів держави у кіберпросторі, але й ряд інших порушень, які також завдають чималої шкоди.

У США є окремі регулювання, що стосуються різних видів правопорушень у кіберпросторі. Федеральний акт з комп'ютерних крадіжок і зловживань № 1030 – це основний акт, що закріплює механізм розслідування кіберзлочинів і встановлює за них як кримінальні, так і цивільні покарання. Акт забороняє:

– неавторизований доступ до комп'ютерів й отримання національної секретної інформації;

– неавторизований доступ до комп'ютерів, які використовуються в торгівлі між штатами або з іншими країнами, та заволодіння інформацією з них;

– неавторизований доступ до непублічних комп'ютерів, які використовуються урядом Сполучених Штатів;

– зумисний доступ до захищених комп'ютерів без авторизації з наміром обману або отримання інформації, що на них міститься;

– знищення комп'ютера (з наміром або випадково);

– викрадення паролів;

– розповсюдження загроз вторгнення, а особливо загроз отримання інформації чи компрометування конфіденційності цієї інформації;

– кібервторгнення, пов'язане з бажанням заволодіти грошима чи власністю.

Залежно від специфіки конкретного вчиненого правопорушення покарання можуть варіюватися від одного до двадцяти років ув'язнення [8].

Іншим пов'язаним законом є Акт щодо захисту електронних комунікацій (Elecronic Communications Protection Act), який захищає інформацію у сховищах та в разі її передавання. Відповідно до цього акту й розділу 17 Кодексу Сполучених Штатів параграф 20702 є кримінальним порушенням навмисний доступ без авторизації чи в обхід авторизаційного доступу до потужностей, які надають сервіс електронної комунікації, що можуть включати, крім іншого, провайдерів імейл-сервісів чи навіть роботодавців, які надають імейл-адресу своїм робітникам. Водночас персональні комп'ютери не належать до потужностей, які надають сервіс електронної комунікації. Ці порушення є предметом покарань, які варіюються від одного року за вперше здійснене таке порушення без невиправданої (злочинної) цілі (також порушення, які вчиняються не з комерційною метою або щоб спричинити знищення інформації) і до 10 років за повторне порушення або здійснення з невиправданою (злочинною) метою [8].

Також необхідно зазначити, що законодавство США має окремі нормативні акти, що регулюють такі правопорушення, як хакерство (мається на увазі неавторизований доступ). Відповідно до цих актів покарання можуть бути до десяти років за доступ до національної секретної інформації або, наприклад, лише до одного року ув'язнення за просте отримання інформації, або до п'яти років, якщо є обтяжувальні фактори.

Наступним видом правопорушення є здійснення DOS-атаки, тобто атаки з метою відмови роботи сервісів. В залежності від того, які настають наслідки та яка нанесена шкода, термін ув'язнення може бути аж до десяти років. Ще одним видом правопорушення є фішинг. За різними законодавчими актами потенційний вирок може бути до двадцяти років ув'язнення.

Правопорушенням також є зараження комп'ютерної системи шкідливим програмним забезпеченням, наприклад таким, як шпигунські програми – так звані Троянпрограми й віруси. Такі дії також (відповідно до нормативно-правових актів США) можуть бути віднесені до злочину, але з урахуванням того, що порушення має бути здійснено навмисно й заподіяно шкоду. Покарання може бути до десяти років ув'язнення.

Ще одним видом порушення є використання програмного забезпечення чи інших інструментів для вчинення кіберзлочинів. Але необхідно зазначити, що виявлення таких злочинів є достатньо складним і їх важко розслідувати, але якщо буде встановлено саме злочинний намір, таке порушення також може бути віднесено до кримінального злочину.[8]

Наступним злочином є викрадення особистості або обман особистості. Але такий злочин має бути пов'язаним із доступом до пристроїв. Такий злочин може підпадати під дію федерального законодавства, а також і під велику кількість законів різних штатів і теж буде вважатися кримінальним злочином.

Також необхідно звернути увагу на злочин, який в Україні не є достатньо розповсюдженим. Це електронна крадіжка, тобто порушення безпеки чинного або колишнього працівника або кримінальне порушення прав інтелектуальної власності, тобто прав копірайту. Відповідно до деяких умов і законодавчих актів це правопорушення може також містити складові частини крадіжки інтелектуальної власності та комерційних секретів відповідно до законодавства США. Правопорушення буде вважатися злочином якщо, по-перше, доступ до мережі було здійснено без відповідної авторизації, а по-друге, торгові секрети були надані з користю для іноземного уряду, а також якщо така крадіжка може спричинити економічні вигоди для інших або вона несе шкоду ринку, на якому здійснено крадіжку [8].

Таким чином, із проведеного аналізу ми можемо зробити висновок, що законодавство сполучених Штатів Америки є достатньо розгалуженим й об'ємним у питаннях здійснення кіберзахисту й забезпечення кібербезпеки.

Загальним рівнем є федеральний рівень законодавства й політика США у цьому питанні. Тут ми можемо зробити висновок, що на федеральному рівні закладено важливість питання забезпечення кібербезпеки як усієї держави, так і її установ і громадян та виражено позицію нетерпимості щодо порушення кібернетичної незалежності США та їхніх партнерів і рішучість щодо здійснення протистоянні у цьому полі. До цього питання належить і здійснення кібероборони держави. І, як ми можемо пересвідчитися з проведеного аналізу, у США створено потужну систему державних органів, що забезпечують кібербезпеку держави й протистоять викликам у кіберпросторі.

Наступним є рівень регулювання діяльності в кіберпросторі на федеральному рівні та рівні штатів. У цьому випадку окремі правопорушення віднесено до злочинів на рівні всієї держави, що врегульовано Кодексом США та відповідними Актами, як діють по всій території США. Третім рівнем є регулювання на рівні кожного окремого

штату. Але проведений аналіз норм показав, що майже неможливо знайти правопорушення, які віднесені до злочинів лише у певних штатах.

Таким чином, ми можемо зробити висновок, що законодавство Сполучених Штатів Америки є розвиненим і врегульовує значну кількість правопорушень, які можуть виникати в кіберпросторі. Основне регулювання здійснено на рівні всієї держави. Також чітко вбачається розмежування різних видів правопорушень, які стосуються забезпечення кібербезпеки всієї держави, і великої кількості правопорушень, які стосуються безпеки громадян у кіберпросторі.

ЛІТЕРАТУРА

1. Брижко В. До питання сучасної інформаційної політики. *Вісник Академії управління Міністерства внутрішніх справ*. 2009. № 2. С. 32–36.

2. Кодекс Сполучених Штатів Америки (U. S. Code) URL: https://www.law.cornell.edu/uscode/text/6/1501.

3. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України / вебсайт Центру досліджень соціальних комунікацій НБУВ. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350.

4. Корченко О., Логінов І., Скворцов С. Стаціонарні системи виявлення і попередження кібератак в інтересах кіберзахисту та кіберконтррозвідки (на прикладі США). *Безпека інформації*. 2019, Т. 25. Вип. 1, С. 5–12. URL: http://jrnl.nau.edu.ua/index.php/Infosecurity.

5. Official website of the Department of Homeland Security URL:https://www.cisa.gov/about-cisa.

6. Ничипорчук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2018. № 1. С. 66–71. URL: http://nbuv.gov.ua/UJRN/mvckrc_2018_1_13.

7. National Cyber Strategy of the United States of America / офіційний вебсайт Білого дому Сполучених Штатів Америки. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

8. The International comparative Legal Guides and the International Bussiness reports / вебсайт Global Legal Group URL: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa.