УДК 342.52

ПЕТРОВ С.Г., *кандидат юридичних наук.*
ORCID: https://orcid.org/0000-0001-7786-4657.

ЗАХИСТ ДЕРЖАВНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ

Анотація. *У статті здійснено аналіз напрямів удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів. Запропоновано внести зміни у кримінальне процесуальне законодавство України та Закон України "Про телекомунікації" задля імплементації положень Конвенції про кіберзлочинність, ввести кримінальну відповідальність за несанкціоноване втручання у роботу інформаційно-телекомунікаційних систем, в яких обробляються державні електронні інформаційні ресурси. Сформульовано низку пропозицій щодо удосконалення адміністративно-правових процедур, пов'язаних із захистом державних електронних інформаційних ресурсів, зокрема запропоновано запровадити ліцензування діяльності провайдерів Інтернет-послуг для органів державної влади, в яких обробляються державні електронні інформаційні ресурси та переглянути нормативні документи у сфері технічного і криптографічного захисту інформації.*

Ключові слова*: державні електронні інформаційні ресурси, кібербезпека, кіберзахист, удосконалення законодавства, інформаційно-телекомунікаційні системи.*

Summary. *The article deals with the issues of the directions for improvement of the current legislation of Ukraine with the purpose of the state electronic information resources protection. It is proposed to amend the criminal procedural legislation of Ukraine and the Law of Ukraine "On Telecommunications" in order to implement the provisions of the Convention on Cybercrime, to introduce criminal liability for unauthorized interference with the work of information and telecommunication systems in which state electronic information resources are processed. A number of proposals have been formulated to improve the administrative and legal procedures related to the protection of state electronic information resources, in particular, it is proposed to introduce licensing of activities of Internet service providers for public authorities in which state electronic information resources are processed and review technical and cryptographic information security regulations.*

Keywords*: state electronic information resources, cybersecurity, cyber defence, legislative improvements, information and telecommunication systems.*

Аннотация. *В статье осуществлен анализ направлений совершенствования действующего законодательства Украины с целью защиты государственных электронных информационных ресурсов. Предложено внести изменения в уголовное процессуальное законодательство Украины и Закон Украины "О телекоммуникациях" для имплементации положений Конвенции о киберпреступности, ввести уголовную ответственность за несанкционированное вмешательство в работу информационно-телекоммуникационных систем, в которых обрабатываются государственные электронные информационные ресурсы. Сформулирован ряд предложений по совершенствованию административно-правовых процедур, связанных с защитой государственных электронных информационных ресурсов, в частности предложено ввести лицензирование деятельности провайдеров Интернет-услуг для органов государственной власти, в которых обрабатываются государственные электронные информационные ресурсы и пересмотреть нормативные документы в сфере технической и криптографической защиты информации.*

Ключевые слова: *государственные электронные информационные ресурсы, кибербезопасность, киберзащита, совершенствование законодательства, информационно-телекоммуникационные системы.*

Постановка проблеми. Визначення шляхів формування безпечного функціонування електронних інформаційних ресурсів вищих органів державної влади, державних підприємств, установ та організацій є одним із пріоритетів для розвитку систем електронного урядування, реалізації концепції "держава у смартфоні" тощо. В Україні існує низка чинників, що впливають на регулювання, захист та розвиток системи обігу державних електронних інформаційних ресурсів. Поряд з безумовною відкритістю інформаційної сфери України загалом, досить часто нормативно-правові акти, що регулюють функціонування державних електронних інформаційних ресурсів, не враховують стратегічних орієнтирів, об'єктивних українських реалій, а також загроз, що виникають у зв'язку з протиправними посяганнями на електронні інформаційні ресурси і на державні зокрема. Виникають випадки, коли частина інформаційних відносин регулюється підзаконними нормативно-правовими актами, що не завжди узгоджуються із чинними законами України, зокрема Законом України "Про основні засади забезпечення кібербезпеки України", а також концептуальними документами, наприклад, "Стратегією кібербезпеки України".

Результати аналізу наукових публікацій свідчать про те, що питання забезпечення кібернетичної і інформаційної безпеки держави були предметом досліджень багатьох українських учених, а саме Довганя О.Д., Климчука О.О., Марущака А.І., Остроухова В.В., Панченко В.М., Пилипчука В.Г., Польового В.І., Розвадовського О.Б., Хлевицького В.Б., Юрченка О.М.та інших.

У попередніх дослідженнях [1] автор частково розкриває організаційні питання діалогу суб'єктів Національної системи кібербезпеки і представників ІТ-бізнесу з метою підвищення довіри між приватними суб'єктами та державними органами, а відповідну платформу для обговорення пропонує організувати на базі Апарату РНБО України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Частково питання методології побудови класифікатора загроз для державних інформаційних ресурсів розкривають дослідники технічних наук Юдін О.К.та Бучик С.С. [2]; у контексті електронного урядування принципи організації національних електронних інформаційних ресурсів, зокрема у частині державних електронних інформаційних ресурсів аналізує Приймак Ю. [3, с. 130]. Стратегічну проблему забезпечення інформаційної безпеки в контексті глобалізації у своїй монографії розкриває Довгань О.Д. [4].

Однак у цілому питання удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів було предметом наукових досліджень лише фрагментарно. Саме тому у сучасний період у системі функціонування електронних інформаційних ресурсів держави свого вирішення потребують науково-теоретичні проблеми удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів.

Метою статті є визначення окремих напрямів удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів.

Виклад основного матеріалу. Насамперед, звернемо увагу на відсутність Державної цільової програми, яка б передбачала заходи із забезпечення кіберзахисту України, зокрема і в частині захисту державних електронних інформаційних ресурсів. У цьому контексті підтримуємо позиції експертів щодо необхідності передбачення у програмі першочергових заходів: запровадження міжнародних стандартів безпеки, підвищення рівня обізнаності населення з загрозами кібербезпеки, впровадження системи навчання з кібербезпеки і визнання міжнародної сертифікації з кібербезпеки ІТ-аудиту [5]. Дійсно, Закон України "Про основні засади забезпечення кібербезпеки України"

передбачає, що функціонування національної системи кібербезпеки забезпечується зокрема шляхом програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту [6, ст. 8]. Відповідно, правові передумови для прийняття Державної цільової програми кіберзахисту України існують і вони актуалізуються сучасними загрозами кібербезпеці держави. Існують також приклади прийняття і реалізації подібних програм в провідних іноземних країнах, зокрема у Сінгапурі, де впроваджено Національну програму з кібербезпеки [7]. Тому вважаємо за необхідне прийняти Державну цільову програму кіберзахисту України.

У розвиток позиції Марущака А.І. щодо імплементації у вітчизняне законодавство статей 16 – 18 Конвенції про кіберзлочинність [8] (далі – Конвенція) відзначимо також, що від належного нормативно-правового регулювання відносин щодо повноважень правоохоронних органів залежить ефективність їх діяльності щодо захисту державних електронних інформаційних ресурсів від кіберінцидентів та кібератак. Норми Конвенції мають імплементуватися у законодавство нашої держави, зокрема у частині доповнення Кримінального процесуального кодексу України статтями щодо електронних доказів у кримінальному провадженні у частині визначення поняття цифрових (електронних) доказів (ст. 14 Конвенції: "…кожна Сторона застосовує повноваження і процедури, передбачені до… збору доказів у електронній формі стосовно кримінального правопорушення" [9]), порядку обмеження (блокування) інформаційного ресурсу (інформаційного сервісу) і впровадження термінової фіксації інформації в цифровій (електронній) формі та її збереження (ст. 16 Конвенції: "1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання можливості своїм компетентним органам видавати ордери або іншим подібним шляхом спричиняти термінове збереження визначених комп'ютерних даних, включаючи дані про рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема у випадку, коли існують підстави вважати, що такі комп'ютерні дані особливо вразливі до втрати чи модифікації. 2. Якщо Сторона застосовує пункт 1 вище шляхом видачі ордеру особі, яким така особа зобов'язується зберігати визначені комп'ютерні дані, які зберігаються і знаходяться у власності або під контролем такої особи, вона вживає такі законодавчі та інші заходи, які можуть бути необхідними для того, щоб зобов'язати таку особу зберігати і підтримувати цілісність таких комп'ютерних даних протягом такого періоду, який буде необхідним для того, щоб компетентні органи мали можливість отримати дозвіл на їхнє розкриття, з максимальним терміном у 90 днів [9]), специфіки проведення обшуку і арешту з метою розширення дії на цифрові (електронні) докази, в тому числі можливість копіювати необхідні дані (ст. 19 Конвенції "Обшук і арешт комп'ютерних даних, які зберігаються" [9]).

У зв'язку з викладеним та з урахуванням положень Конвенції необхідно також передбачити у Законі України "Про телекомунікації" (ст. 39) [10] обов'язок суб'єктів ринку телекомунікації, які надають послуги доступу до Інтернет, забезпечити ідентифікацію власних абонентів за ПІБ, IP-адресою, фізичною адресою надання послуг, а також зберігати дані щодо спожитих ними послуг, форм оплати та інформацію щодо з'єднань абонентів протягом 90 днів.

Наступна пропозиція удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів стосується врегулювання проблемних питань протидії кіберзлочинності, зокрема і спрямованої на такі державні ресурси. Так, кримінальне законодавство України не виокремлює злочини щодо державних електронних інформаційних ресурсів, що не дає змоги віднести їх досудове

розслідування до підслідності слідчих СБ України, хоча це передбачено положеннями Стратегії кібербезпеки України [11]. На нашу думку, необхідно ввести відповідальність за несанкціоноване втручання у роботу інформаційно-телекомунікаційних систем, в яких обробляються державні електронні інформаційні ресурси. Адже останнім часом фіксується збільшення кібератак, зорієнтованих на спричинення шкоди національним інтересам держави, на такі ресурси, відповідні інформаційно-телекомунікаційні системи, а також на об'єкти критичної інформаційної інфраструктури. Протидія ж органами СБ України зазначеним загрозам ускладнюється через відсутність належного кримінально-правового захисту інтересів держави. Адже на сьогодні предмет, об'єктивна та суб'єктивна сторони злочинів, передбачених статтями 361 та 362 КК України [12] не повною мірою охоплюють діяння, спрямовані на порушення сталої роботи державних електронних інформаційних ресурсів.

Наступні пропозиції для удосконалення законодавства України стосуються зміни адміністративно-правових процедур, пов'язаних із захистом державних електронних інформаційних ресурсів. Так, рішенням РНБО України від 29 грудня 2016 р. [13], Кабінету Міністрів України було доручено врегулювати питання щодо заборони державним органам, підприємствам, установам і організаціям державної форми власності закуповувати послуги (укладати договори) з доступу до мережі Інтернет у операторів (провайдерів) телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам у сфері захисту інформації. Відповідне рішення до цього часу не втілилося в окремий нормативно-правовий акт, оскільки суб'єкти ринку Інтернет-послуг та їх об'єднання блокують його прийняття на стадії громадського обговорення. Однак, з 2018 року оператори (провайдери) телекомунікацій отримують в Держспецзв'язку України атестати відповідності щодо забезпечення захисту інформації згідно з вимогами нормативних документів системи технічного захисту інформації в Україні, які дозволяють їм надавати послуги з доступу до мережі Інтернет – "Захищений вузол Інтернет-доступу" – державним органам, підприємствам, установам і організаціям державної форми власності.

У цьому напрямі пропонуємо запровадити ліцензування діяльності провайдерів Інтернет-послуг для органів державної влади, в яких обробляються державні електронні інформаційні ресурси.

На сьогодні законодавство України також не передбачає адміністративної відповідальності за невиконання законних вимог посадових осіб СБ України. У контексті наділення СБ України додатковими повноваженнями здійснювати контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, протидіяти кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідувати кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечувати реагування на кіберінциденти у сфері державної безпеки [6]. За такого стану правового регулювання відсутність адміністративної відповідальності за невиконання законних вимог посадових осіб СБ України суттєво знижуватиме ефективність реалізації зазначених вище повноважень, передбачених Законом України "Про основні засади забезпечення кібербезпеки України".

Саме тому вважаємо, що пропозиція внести зміни до Кодексу України про адміністративні правопорушення шляхом включення статті 185-14 "Невиконання законних вимог посадових (службових) осіб Служби безпеки України або перешкоджання

здійсненню Службою безпеки України визначених законом функцій або повноважень" [14] є цілком обґрунтованою і сприятиме, серед іншого, належному виконанню органами СБ України повноважень щодо розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, боротьбу з кібертероризмом та кібершпигунством.

Потребують також перегляду нормативні документи у сфері технічного і криптографічного захисту інформації (НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі", НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі"), відповідно до яких здійснюється побудова комплексних систем захисту інформації. Зокрема, згідно з чинним законодавством [15] при проведенні перевірки інформаційно-телекомунікаційних систем визначається відповідність комплексних систем захисту інформації вимогам нормативно-правових актів та нормативних документів системи технічного захисту інформації. Тобто, видається, що перевіряється виключно технічна документація з впровадження таких систем без вивчення реального стану справ із захисту державних електронних інформаційних ресурсів. Такий підхід вважаємо застарілим і таким, що не відповідає як провідним міжнародним практикам, так і реаліям сучасних загроз у кіберпросторі, а тому має бути переглянутий у напрямку запровадження міжнародних апробованих підходів щодо виявлення вразливостей для завантаження шкідливого програмного забезпечення, порядку проведення регулярного аудиту захисту державних електронних інформаційних ресурсів тощо.

Ще однією проблемою практичного характеру, яка негативно впливає на стан захищеності державних електронних інформаційних ресурсів, є використання співробітниками державних органів, в яких обробляються такі ресурси, джерел розважального характеру, сторонніх поштових сервісів, соцмереж тощо. Це призводить до формування додаткових вразливостей для державних електронних інформаційних ресурсів.

З метою зниження рівня відповідного ризику для державних електронних інформаційних ресурсів, пропонуємо передбачити розпорядчим документом Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, ведення Реєстру ресурсів, доступ до яких абонентів телекомунікаційних мереж – органів державної влади України обмежений. До такого реєстру доцільно включати ресурси розважального характеру, сторонні поштові сервіси, соцмережі, анонімайзери доступу, тор-браузери тощо.

Насамкінець відзначимо, що незважаючи на рішення Ради національної безпеки і оборони України "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" від 29 грудня 2016 р. введеного в дію Указом Президента України від 13.02.17 р. № 32 [16], на даний час не сформовано перелік інформаційно-телекомунікаційних систем об'єктів критичної інформаційної інфраструктури (відповідно до постанови Кабінету Міністрів України від 23.08.16 р. № 563 [17]), що суттєво ускладнює протидію загрозам безпечному функціонуванню інформаційно-телекомунікаційних систем, в яких обробляються державні електронні інформаційні ресурси. Тому вважаємо, що є усі підстави для пришвидшення формування зазначеного переліку.

Висновки.

Підсумовуючи викладене, зазначимо, що здійснений аналіз дав підстави для формулювання напрямів удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів.

Набули подальшого розвитку питання імплементації норм Конвенції про кіберзлочинність у кримінальне процесуальне законодавство України у частині порядку обмеження (блокування) інформаційного ресурсу (інформаційного сервісу) і впровадження термінової фіксації інформації в цифровій (електронній) формі та її збереження, проведення обшуку і арешту з метою розширення дії на цифрові (електронні) докази. Відповідно, доцільно також передбачити у Законі України "Про телекомунікації" обов'язок суб'єктів ринку телекомунікації, які надають послуги доступу до Інтернет, забезпечити ідентифікацію власних абонентів, а також зберігати дані щодо спожитих ними послуг протягом 90 днів.

Обґрунтовано необхідність введення відповідальності за несанкціоноване втручання у роботу інформаційно-телекомунікаційних систем, в яких обробляються державні електронні інформаційні ресурси, з метою кримінально-правового захисту інтересів держави.

Сформульовано низку пропозицій щодо удосконалення адміністративно-правових процедур, пов'язаних із захистом державних електронних інформаційних ресурсів, а саме запропоновано:

прийняти Державну цільову програму кіберзахисту України;

запровадити ліцензування діяльності провайдерів Інтернет-послуг для органів державної влади, в яких обробляються державні електронні інформаційні ресурси;

внести зміни до Кодексу України про адміністративні правопорушення шляхом включення статті щодо відповідальності за невиконання законних вимог посадових (службових) осіб Служби безпеки України або перешкоджання здійсненню Службою безпеки України визначених законом функцій або повноважень;

переглянути нормативні документи у сфері технічного і криптографічного захисту інформації у напрямку запровадження міжнародних апробованих підходів щодо виявлення вразливостей для завантаження шкідливого програмного забезпечення, порядку проведення регулярного аудиту захисту державних електронних інформаційних ресурсів тощо;

передбачити розпорядчим документом Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації ведення Реєстру ресурсів, доступ до яких абонентів телекомунікаційних мереж – органів державної влади України обмежений.

Перспективами подальших наукових пошуків визначаємо питання правових механізмів для розбудови мережі ситуаційних центрів кібербезпеки в Україні.

Використана література

1. Петров С.Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України. *Інформація і право*. № 4(31)/2019. С. 107-112.

2. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія. Київ: НАУ, 2015. 214 с.

3. Приймак Ю. Розвиток електронного урядування в Україні: організація національних електронних інформаційних ресурсів. URL: http://www.visnyk.academy.gov.ua/wp-content-/upload/2013/11/2011-4-18.pdf

4. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія. Київ: Видавничий дім "АртЕк", 2015. 386 с.

5. Котвицкий І. Що потрібно зробити Україні для власної кібербезпеки. URL: https://www.glavnoe.ua/articles/a12228-scho-potribno-zrobiti-ukraini-dlja-vlasnoi-kiberbezpeki

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

7. The National Cybersecurity R&D Programme. URL: https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme

8. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності. *Інформація і право*. № 1(24)/2018. С. 127-132.

9. Про кіберзлочинність: Конвенція РЄ від 23 листопада 2001 року. *Офіційний вісник України*. 2007. № 65. Ст. 253.

10. Про телекомунікації: Закон України від 18.11.03 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.

11. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899.

12. Кримінальний кодекс України: Закон України від 05.04.01 р. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131.

13. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації": Указ Президента України від 13.02.17 р. № 32. URL: https://www.president.gov.ua/documents/322017-21282

14. Про внесення змін до Закону України "Про Службу безпеки України": проект закону щодо удосконалення організаційно-правових засад діяльності Служби безпеки України від 10.03.20 р. № 3196. URL: https://www.http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68347

15. Про затвердження Положення про державний контроль за станом технічного захисту інформації: Наказ Адміністрації Держспецзв'язку України від 16.05.07 р. № 87. *Офіційний вісник України*. 2007. № 50. Ст. 2037.

16. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації": Указ Президента України від 13.02.17 р. № 32/2017. *Офіційний вісник України*. 2017. № 16. Ст. 464.

17. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23.08.16 р. № 563. *Офіційний вісник України*. 2016. № 69. Ст. 2332.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~