УДК 342.52

ПРОБЛЕМИ ЗАХИСТУ ДЕРЖАВНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ У КОНТЕКСТІ ЦИФРОВИХ ТРАНСФОРМАЦІЙ І ЦИФРОВІЗАЦІЇ В УКРАЇНІ

PROBLEMS OF THE STATE ELECTRONIC INFORMATION RESOURCES' PROTECTION ISSUES IN THE CONTEXT OF DIGITAL TRANSFORMATIONS AND DIGITALIZATION IN UKRAINE

Петров С.Г.,
кандидат юридичних наук

У статті досліджуються питання перегляду повноважень Держспецзв'язку України як одного із суб'єктів національної системи кібербезпеки, спрямованих на захист державних електронних інформаційних ресурсів.

Зроблено висновок про не повну відповідність повноважень Держспецзв'язку України євроінтеграційним напрямам розвитку держави, вказано на необхідність позбавлення Держспецзв'язку України невластивих функцій у окремих сферах, наприклад, у сфері захисту конфіденційної інформації в недержавному секторі, переходу від регулювання створення комплексних систем захисту інформації для електронних публічних сервісів до систем управління безпекою інформації та оцінки їх відповідності за міжнародними стандартами. Запропоновано на Держспецзв'язку України покласти функцію державного ринкового нагляду за засобами криптографічного захисту інформації.

Акцентовано увагу на необхідності упровадження сучасних ризик-орієнтованих механізмів захисту інформації на заміну комплексних систем захисту інформації, а також дерегулювання певних сфер, що віднесено до компетенції Держспецзв'язку України. Зокрема, запропоновано здійснити перехід від перевірок стану захисту інформації до його моніторингу, делегувати галузевим регуляторам функції визначення вимог щодо захисту та безпеки окремих категорій інформації. Обґрунтовано необхідність посилення функції Держспецзв'язку України стосовно розвитку організаційно-технічної моделі кіберзахисту, а також розвитку системи аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість.

За результатами науково-теоретичного аналізу сформульовано пропозиції щодо внесення змін до законів України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про ліцензування видів господарської діяльності», а також до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 та інших нормативно-правових актів.

Ключові слова: державні електронні інформаційні ресурси України, захист інформації, кібербезпека, кіберзахист, цифровізація.

The article deals with the issues of revision of the powers of the State Service of Special Communication and Information Protection of Ukraine as one of the member of the National Cybersecurity System aimed at the protection of state electronic information resources.

It is concluded that the powers of the the State Service of Special Communication and Information Protection of Ukraine are not fully consistent with the European integration of the state. The need to deprive inappropriate functions of the State Service of Special Communication and Information Protection of Ukraine is proved, particularly protection of confidential information in the private sector, the transition from regulating to monitoring of the integrated information protection systems, etc. It is proposed that the State Service of Special Communication and Information Protection of Ukraine assign the function of state market supervision over the of cryptographic protection of information hardware and software.

Based on the results of scientific and theoretical analysis, proposals have been formulated to amend the laws of Ukraine "On information protection in information and telecommunications systems", "On licensing of economic activities", as well as the Rules for information protection information and telecommunications systems, approved by the resolution of the Cabinet of Ministers of Ukraine of March 29, 2006 № 373 and other legal acts.

Keywords: State Electronic Information Resources of Ukraine, Information Security, Cybersecurity, Cyber Defense, Digitalization.

Постановка проблеми. Питання цифрового розвитку, цифрових трансформацій і цифровізації останніми роками набуває усе більшого практичного й наукового значення. Це пов'язано не лише із невпинним розвитком інформаційних технологій, а й з відповідним удосконаленням систем надання адміністративних послуг населенню, оптимізації державного управління у сфері застосування інформаційних технологій. Створення і функціонування Міністерства цифрової трансформації України [1] є позитивним чинником «реагування» держави на зміну суспільних інформаційних технологій. Крім того, у 2020 році у міністерствах, інших центральних органах виконавчої влади введено посади заступника керівника відповідного органу з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO) [2]. Відповідно, внесено зміни до постанови Кабінету Міністрів України від 30 січня 2019 р. № 56 «Деякі питання цифрового розвитку» [3], зокрема рекомендовано державним органам та органам місцевого самоврядування розглянути можливість утворення та забезпечення функціонування структурних підрозділів (спеціалістів) з питань цифрового розвитку, цифрових трансформацій і цифровізації, і встановлено, що заступники керівників центральних органів виконавчої влади, обласних, Київської та Севастопольської міських державних адміністрацій з питань цифрового розвитку, цифрових трансформацій і цифровізації отримують необхідну методичну допомогу та здійснюють відповідну взаємодію з Міністерством цифрової трансформації. Безумовно, подібні посадові особи органів виконавчої влади, обласних, Київської та Севастопольської міських державних адміністрацій мають основним своїм завданням здійснювати координацію впровадження новітніх інформаційних технологій у практику діяльності державних установ.

Поряд з позитивними ознаками розвитку державного управління у сфері цифро-

вого розвитку, цифрових трансформацій і цифровізації, існують випадки спрямованих кібератак на державні електронні інформаційні ресурси (далі – ДЕІР). Наприклад, 12 травня 2020 року слідчі Головного слідчого управління Національної поліції України розпочали кримінальне провадження за ч. 2 ст. 361 Кримінального кодексу України (Несанкціоноване втручання у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації) за фактами витоку персональних даних громадян імовірно із мобільного застосунку «Дія» [4].

Саме тому, потребують додаткового дослідження питання захисту державних електронних інформаційних ресурсів України у контексті цифрового розвитку, цифрових трансформацій і цифровізації, з урахуванням повноважень Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку України).

Результати аналізу наукових публікацій свідчать про те, що проблематика захисту державних електронних інформаційних ресурсів частково була предметом досліджень багатьох українських учених, а саме М.М. Галамби, О.Д. Довганя, О.О. Климчука, А.І. Марущака, В.В. Остроухова, В.М. Панченко, В.Г. Пилипчука, В.І. Польового, О.Б. Розвадовського, О.М. Юрченка та інших.

Окремі дослідники розкривали питання ефективності діяльності державних органів у сфері захисту інформаційного простору України [5], не розкриваючи однак особливостей правового статусу органів, відповідальних за захист ДЕІР. Крім того, питанням методології побудови класифікатора загроз державним інформаційним ресурсам присвятили свою монографію О.К.Юдін і С.С.Бучик [6].

Однак, проблема захисту державних електронних інформаційних ресурсів у контексті цифрових трансформацій і цифровізації в Україні була предметом наукових пошуків тільки частково.

Метою статті є розкриття правових проблем захисту державних електронних інформаційних ресурсів у контексті цифрових трансформацій і цифровізації в Україні у частині удосконалення повноважень Держспецзв'язку України.

Виклад основного матеріалу.

Серед завдань основних суб'єктів національної системи кібербезпеки Держспецзв'язку України має значну частину повноважень, спрямованих на захист ДЕІР. Цей орган зокрема забезпечує захист у кіберпросторі державних інформаційних ресурсів, кіберзахист об'єктів критичної інформаційної інфраструктури, здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформує про кіберзагрози та методи захисту від них, забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA тощо. Варто зазначити, що впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кібер-

захисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань [7, ст. 8]. Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC), створений у Держспецзв'язку України як центральний компонент і ядро національної системи кіберзахисту України, є платформою для взаємодії основних суб'єктів забезпечення кібербезпеки (Держспецзв'язку, СБУ, Нацполіції), яка підвищує ефективність і оперативність діяльності правоохоронних органів із протидії та розслідування кіберзлочинів [8].

Безумовно, значну частину заходів щодо забезпечення кібербезпеки здійснює Держспецзв'язку України поряд із забезпеченням функціонування й розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань [9, ст. 22].

З урахуванням характеру загроз ДЕІР, а також розвитку правового регулювання у зарубіжних країнах, відзначимо, що повноваження Держспецзв'язку України видаються дещо застарілими і такими, що не відповідають євроінтеграційним напрямам розвитку держави, існує необхідність позбавлення Держспецзв'язку України невластивих функцій у окремих сферах, наприклад, у сфері захисту конфіденційної інформації в недержавному секторі (за винятком питань взаємодії держави та бізнесу), у сфері технічного та криптографічного захисту інформації – переходу від регулювання створення комплексної системи захисту інформації (далі – КСЗІ) для електронних публічних сервісів (у тому числі реєстрів) до систем управління безпекою інформації та оцінки їх відповідності за міжнародними стандартами (зокрема приєднання до міжнародних угод про визнання критеріїв оцінки інформаційної безпеки (Common Criteria), упровадження сучасних ризик-орієнтованих механізмів захисту інформації на заміну КСЗІ тощо. Особливої уваги заслуговують також питання упровадження у системах кіберзахисту та спеціального зв'язку засобів захисту інформації вітчизняного виробництва.

На сьогодні є необхідність здійснення дерегулювання певних сфер, що віднесено до компетенції Держспецзв'язку України, наприклад, переходу від перевірок стану захисту інформації до його моніторингу, зміна ліцензування залученням для виконання робіт зі створення та оцінки відповідності систем управління безпекою інформації підприємств-виконавців робіт з безпеки інформації, делегування галузевим регуляторам функцій визначення вимог щодо захисту та безпеки окремих категорій інформації тощо. При цьому має розвиватися функція Держспецзв'язку України стосовно розвитку організаційно-технічної моделі кіберзахисту та її масштабування на усю територію України; розвитку системи аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість.

У зв'язку з викладеним та з урахуванням Указу Президента України від 10.11.2019 р. № 837 «Про невідкладні заходи з прове-

дення реформ та зміцнення держави» [10] вважаємо за доцільне ініціювати наступні зміни до чинного законодавства України щодо правового статусу Держспецзв'язку. По-перше, у необхідно внести зміни до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373, у яких передбачити: вимоги з безпеки інформації за ризик-орієнтовним підходом; відповідно до вимог законодавства ЄС надати право галузевим регуляторам встановлювати вимоги з безпеки для персональних даних, банківської, лікарської таємниць, таємниці слідства тощо; запровадження Реєстру суб'єктів, що здійснюють діяльність у сфері захисту інформації.

По-друге, доцільно внести зміни до Закону України «Про ліцензування видів господарської діяльності» [11] щодо скасування ліцензування у галузі криптографічного та технічного захисту інформації та запровадження Реєстру суб'єктів, що здійснюють діяльність у сфері захисту інформації, встановлення кваліфікаційних вимог, порядку оцінки відповідності та порядку внесення (або виключення) фізичних та юридичних осіб до Реєстру, визначення видів робіт у сфері захисту інформації, що виконуються за умови внесення юридичних або фізичних осіб (виконавців робіт) до Реєстру. Відповідні зміни доцільно внести і до постанови Кабінету Міністрів України «Про затвердження переліку органів ліцензування та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України» [12], а також скасувати постанову Кабінету Міністрів України від 16.11.2016 р. № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України» [13].

По-третє, на Адміністрацію Держспецзв'язку доцільно покласти функцію державного ринкового нагляду за засобами криптографічного захисту інформації шляхом внесення відповідних змін до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», а також постанови Кабінету Міністрів України «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» [14] та постанови Кабінету Міністрів України від 28 грудня 2016 року № 1069 «Про затвердження переліку видів продукції, щодо яких органи державного ринкового нагляду здійснюють державний ринковий нагляд» [15].

Зазначені пропозиції сприятимуть підвищенню ефективності захисту ДЕІР у сучасних умовах з урахуванням міжнародної практики.

Висновки. Підсумовуючи викладене, зазначимо, що в умовах цифрових трансформацій і цифровізації, а також кібератак, спрямованих на ДЕІР, потребували перегляду повноваження Держспецзв'язку України, яка має значну частину завдань, порівняно з іншими суб'єктами національної системи кібербезпеки, спрямованих на захист ДЕІР.

У роботі доходимо висновку про не повну відповідність повноважень Держспецзв'язку України євроінтеграційним напрямам розвитку держави, вказано на необхідність позбавлення Держспецзв'язку України невластивих функцій у окремих сферах, на-

приклад, у сфері захисту конфіденційної інформації в недержавному секторі, переходу від регулювання створення КСЗІ для електронних публічних сервісів до систем управління безпекою інформації та оцінки їх відповідності за міжнародними стандартами. Запропоновано на Держспецзв'язку України покласти функцію державного ринкового нагляду за засобами криптографічного захисту інформації.

Акцентовано увагу на необхідності упровадження сучасних ризик-орієнтованих механізмів захисту інформації на заміну КСЗІ, а також дерегулювання певних сфер, що віднесено до компетенції Держспецзв'язку України. Зокрема, пропонується здійснити перехід від перевірок стану захисту інформації до його моніторингу, делегувати галузевим регуляторам функції визначення вимог щодо захисту та безпеки окремих категорій інформації тощо. При цьому обґрунтовано необхідність посилення функції Держспецзв'язку України стосовно розвитку організаційно-технічної моделі кіберзахисту, а також розвитку системи аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість.

За результатами науково-теоретичного аналізу сформульовано пропозиції щодо внесення змін до законів України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про ліцензування видів господарської діяльності», а також до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 тощо.

Подальшого розвитку потребують питання удосконалення повноважень інших суб'єктів національної системи кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856 «Питання Міністерства цифрової трансформації». Офіційний вісник України. 2019. № 80. Ст. 2736.
2. Постанова Кабінету Міністрів України від 3 березня 2020 р. № 194 «Деякі питання діяльності підрозділів з питань цифрового розвитку, цифрових трансформацій і цифровізації центральних та місцевих органів виконавчої влади та заступників керівників центральних органів виконавчої влади, обласних, Київської та Севастопольської міських державних адміністрацій з питань цифрового розвитку, цифрових трансформацій і цифровізації». Офіційний вісник України. 2020. № 23. Ст. 883.
3. Постанова Кабінету Міністрів України від 30 січня 2019 р. № 56 «Деякі питання цифрового розвитку». Офіційний вісник України. 2019. № 13. Ст. 473.
4. Нацполіція не підтвердила інформацію щодо витоку даних українців через мобільний застосунок «Дія». Url: https://diia.gov.ua/news/nacpoliciya-ne-pidtverdila-informaciyu-shchodo-vitoku-danih-ukrayinciv-cherez-mobilnij-zastosunok-diya.
5. Марущак А. І. Питання ефективності діяльності державних органів у сфері захисту інформаційного простору України. Інформація і право. 2017. № 4. С. 86-92.
6. Юдін О. К., Бучик С. С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія. К. : НАУ, 2015. 214 с.

7. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

8. Сайт Держспецзв'язку України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=286338&cat_id=284576.

9. Закон України «Про національну безпеку України» від 21.06.2018 р. Відомості Верховної Ради України. 2018. № 31. Ст. 241.

10. Указ Президента України від 10.11.2019 р. № 837 «Про невідкладні заходи з проведення реформ та зміцнення держави». Офіційний вісник Президента України. 2019. № 24. Ст. 1038.

11. Закон України «Про ліцензування видів господарської діяльності». Відомості Верховної Ради України. 2015. № 23. Ст. 158.

12. Постанова Кабінету Міністрів України від 5.08.2015 р. № 609 «Про затвердження переліку органів ліцензування та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України». Офіційний вісник України. 2015. № 68. Ст. 2232.

13. Постанова Кабінету Міністрів України від 16.11.2016 р. № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України». Офіційний вісник України. 2016. № 93. Ст. 3033.

14. Постанова Кабінету Міністрів України від 3.09.2014 р. №411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України». Офіційний вісник України. 2014. № 73. Ст. 2066.

15. Постанова Кабінету Міністрів України від 28.12.2016 р. № 1069 «Про затвердження переліку видів продукції, щодо яких органи державного ринкового нагляду здійснюють державний ринковий нагляд». Офіційний вісник України. 2017. № 50. Ст. 1550.