Інформаційна і національна безпека

УДК 342.52

МАРУЩАК А.І., *доктор юридичних наук, професор.*
ORCID 0000-0003-0069-3727.
ПЕТРОВ С.Г., *кандидат юридичних наук.*
ORCID 0000-0001-7786-4657.

СУЧАСНИЙ СТАН РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ (НА ПРИКЛАДІ СБ УКРАЇНИ ТА ДЕРЖСПЕЦЗ'ВЯЗКУ УКРАЇНИ)

Анотація. *У статті здійснено аналіз сучасного стану розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецз'вязку України). Сформульовано висновок про необхідність врегулювання окремих відносин, пов'язаних з розвитком національної системи кібербезпеки, з урахуванням міжнародної практики. Зокрема, підтримано необхідність врегулювання процедури віднесення до об'єктів критичної інфраструктури, а також незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури. Відзначено, що з визначенням процедури віднесення до об'єктів критичної інфраструктури має запрацювати цілісний правовий механізм як кіберзахисту, так і контррозвідувального забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури.*

Ключові слова*: національна система кібербезпеки, державні електронні інформаційні ресурси, кібербезпека, кіберзахист, інформаційно-телекомунікаційні системи.*

Summary. *The article deals with the issues of the current state of development of the National Cybersecurity System (on the example of the Security Service of Ukraine and the State Special Service of Ukraine). The conclusion is formulated on the need to regulate certain relations of the National Cybersecurity System development, taking into account international practice. For instance, the need to regulate the procedure for defining critical infrastructure facilities, as well as the independent audit of information security at critical infrastructure facilities, was supported. With the definition of the procedure for classifying objects of critical infrastructure, a holistic legal mechanism should work for both cyber defense and counterintelligence support of cyber security for objects of critical information infrastructure.*

Keywords*: National Cybersecurity System, state electronic information resources, cybersecurity, cyber defence, information and telecommunication systems.*

Аннотация. *В статье осуществлен анализ современного состояния развития национальной системы кибербезопасности (на примере СБ Украины и Госспецсвязи Украины). Сформулирован вывод о необходимости урегулирования отдельных отношений, связанных с развитием национальной системы кибербезопасности, с учетом международной практики. В частности, поддержано необходимость урегулирования процедуры отнесения к объектам критической инфраструктуры, а также независимого аудита информационной безопасности на объектах критической инфраструктуры. Отмечено, что с определением процедуры отнесения к объектам критической инфраструктуры должен заработать целостный правовой механизм как киберзащиты, так и контрразведывательного обеспечения кибербезопасности объектов критической информационной инфраструктуры.*

Ключевые слова: *национальная система кибербезопасности, государственные электронные информационные ресурсы, кибербезопасность, киберзащита, информационно-телекоммуникационные системы.*

Постановка проблеми. Служба безпеки України (далі – СБУ) і Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку) є одними з основних суб'єктів Національної системи кібербезпеки разом з Національною поліцією України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами, Національним банком України [1, ст. 8]. Ці два державні органи мають спільну історію у минулому. На даному ж етапі розвитку української державності актуалізуються питання взаємодії СБУ і Держспецзв'язку, зокрема у межах Національної системи кібербезпеки з метою здійснення заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. У цьому контексті науково-теоретична оцінка сучасного стану та перспектив розвитку Національної системи кібербезпеки на прикладі діяльності СБУ та Держспецз'вязку вбачається нагальною.

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

Частково питання сучасної безпекової політики, зокрема щодо обов'язкового включення до неї питань протидії кіберзброї розкриває Форест Харе [2]. Розвитку національних стратегій кібербезпеки присвячує своє дослідження Петрісор Патраску [3], а найбільш вдало, на нашу думку, компаративістське дослідження стратегій кібербезпеки країн ЄС та НАТО здійснено дослідниками Даріусом Стілісом, Паулісом Пакутінскасом та Інгою Малінаускайте [4]

Однак у цілому питання сучасного стану та перспективи розвитку Національної системи кібербезпеки було предметом наукових досліджень лише фрагментарно.

Метою статті є розкриття сучасного стану розвитку Національної системи кібербезпеки, здійснене на прикладі СБУ та Держспецз'вязку, з акцентом на питання взаємодії зазначених суб'єктів.

Виклад основного матеріалу. Розпочнемо з аналізу норм Закону України "Про Службу безпеки України", які передбачають взаємодію СБ України з державними органами, підприємствами, установами, організаціями та посадовими особами, які сприяють виконанню покладених на неї завдань, а також громадянами України та їх об'єднаннями, іншими особами, які сприяють законній діяльності СБ України на добровільних засадах [5, ст. 8]. Закон України "Про основні засади забезпечення кібербезпеки України" деталізує сприяння Службі безпеки України як суб'єкту національної системи кібербезпеки: державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків [1].

Закон України "Про телекомунікації" також передбачає підстави для взаємодії СБ України з операторами і провайдерами телекомунікацій, закріплюючи обов'язок останніх за власні кошти встановлювати на своїх телекомунікаційних мережах технічні

засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення; оператори телекомунікацій зобов'язані також забезпечувати захист зазначених технічних засобів від несанкціонованого доступу [6].

Частково питання взаємодії суб'єктів національної системи кібербезпеки передбачені у Правилах надання та отримання телекомунікаційних послуг, наприклад стосовно обов'язків споживачів: не допускати дій, що можуть перешкоджати безпечній експлуатації телекомунікаційних мереж, підтримці цілісності та взаємодії таких мереж, захисту їх інформаційної безпеки, електромагнітної сумісності радіоелектронних засобів, ускладнювати чи унеможливлювати надання послуг іншим споживачам; не здійснювати несанкціонованого втручання в роботу та/або використання телекомунікаційних мереж [7], а також у Порядку підключення до глобальних мереж передачі даних [8], Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [9].

Безпосередньо правові підстави для взаємодії суб'єктів сектору безпеки і оборони, зокрема щодо захисту державних електронних інформаційних ресурсів (далі – ДЕІР), визначає Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах [10]. Зокрема, органи виконавчої влади з метою захисту державних інформаційних ресурсів в ІТС:

визначають перелік інформаційних та телекомунікаційних систем, які містять ДЕІР (у тексті документа використовується термін "державні інформаційні ресурси", скорочення авторів), та погоджують його з Адміністрацією Держспецзв'язку (далі – Адміністрація);

здійснюють згідно з вимогами нормативно-правових актів з питань захисту інформації під методичним керівництвом Адміністрації заходи щодо захисту ДЕІР в інформаційно-телекомунікаційних системах (далі – ІТС), у тому числі підключених до глобальних мереж передачі даних;

збирають, узагальнюють та аналізують інформацію про вчинення несанкціонованих дій і здійснюють заходи щодо усунення їх наслідків;

невідкладно (протягом доби) інформують Адміністрацію про спробу вчинення чи вчинення несанкціонованих дій;

надають на запит Адміністрації інформацію про технічні та програмні засоби, що використовуються для надання мережних послуг, а також про зміни у способах або видах підключення до глобальних мереж передачі даних;

оновлюють за рекомендаціями Адміністрації антивірусні програмні засоби, використовуючи при цьому лише ті з них, які пройшли державну експертизу.

У свою чергу Адміністрація: здійснює методичне керівництво та координує діяльність органів виконавчої влади, пов'язану із запобіганням, виявленням, реагуванням та усуненням наслідків несанкціонованих дій щодо ДЕІР в ІТС, надає в разі потреби допомогу у здійсненні заходів щодо запобігання порушенню цілісності, доступності та конфіденційності зазначених ресурсів; надає органам виконавчої влади відомості про антивірусні програмні засоби, які можуть застосовуватися для захисту ДЕІР в ІТС, та проводить перевірку їх оновлення; накопичує та аналізує дані про вчинення та/або спроби вчинення несанкціонованих дій щодо ДЕІР в ІТС, а також про їх наслідки, інформує правоохоронні органи для вжиття заходів із запобігання та

припинення злочинів у зазначеній сфері, оцінює стан захищеності цих ресурсів та надає відповідні рекомендації [10].

З метою організації координації діяльності з питань запобігання вчиненню порушень безпеки інформації в ІТС, виявлення та усунення наслідків інших несанкціонованих дій щодо ДЕІР в ІТС, а також впровадження єдиної процедури надання суб'єктами координації інформації про вчинення та/або спроби вчинення несанкціонованих дій щодо ДЕІР в ІТС розроблено Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо ДЕІР в ІТС [11]. Відповідно до цього Порядку суб'єкти координації у разі виявлення спроби вчинення та/або вчинення несанкціонованих дій вживають заходів щодо: блокування, усунення або локалізації їх негативних наслідків власними силами відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та інших нормативно-правових актів у сфері ТЗІ; збереження (фіксації) ознак несанкціонованих дій, у тому числі на матеріальних носіях інформації; захисту ДЕІР відповідно до рекомендацій, наданих адміністратору безпеки ІТС електронною поштою, телефоном, факсом чи іншим способом; надсилання до Адміністрації Держспецзв'язку України письмового повідомлення тощо. Адміністрація Держспецзв'язку при цьому взаємодіє з органами державної влади, провайдерами та операторами телекомунікацій, установами, підприємствами та організаціями усіх форм власності України; для організації своєчасного обміну інформацією про несанкціоновані дії використовує веб-сторінку www.cert.gov.ua і електронні поштові адреси cert@cert.gov.ua та cert@dsszzi.gov.ua; здійснює міжнародне співробітництво з питань, що належать до компетенції Держспецзв'язку; з метою своєчасного запобігання та припинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж вживає заходів щодо своєчасного інформування правоохоронних органів України, зокрема і СБ України (*додано Авт.*) про виявлені суб'єктами координації несанкціоновані дії [11].

Правові та організаційні засади проведення оцінки стану захищеності ДЕІР в ІТС державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форм власності визначені Порядком оцінки стану захищеності ДЕІР в ІТС [12]. Порядком визначається, що оцінка стану захищеності здійснюється з метою виявлення існуючих загроз ДЕІР в ІТС і є складовою частиною заходів із захисту інформації. Об'єктом оцінки стану захищеності є ДЕІР, які обробляються в ІТС, незалежно від наявності в таких ІТС комплексної системи захисту інформації (далі – КСЗІ). В ІТС, де створено КСЗІ з підтвердженою відповідністю, оцінка стану захищеності здійснюється з метою виявлення нових загроз ДЕІР, які виникли у процесі експлуатації КСЗІ та які не враховані у КСЗІ.

У разі виявлення в ІТС, де створено КСЗІ з підтвердженою відповідністю, додаткових загроз державним інформаційним ресурсам, які виникли за період експлуатації КСЗІ, інформація про таку КСЗІ надається Держспецзв'язку згідно з Положенням про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, затвердженим постановою Кабінету Міністрів України від 03 серпня 2005 року № 688 [13]. У цьому напрямку правового регулювання нормативно-правові акти містять застарілі конструкції, відповідні

відносини потребують правового регулювання з урахуванням міжнародної практики, зокрема у частині запровадження аудиту інформаційної безпеки, про що йдеться нижче.

З метою здійснення оцінки стану захищеності Держспецзв'язку: створює комісію з оцінки стану захищеності (далі – комісія); здійснює планування проведення оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності; визначає перелік документів, що стосуються функціонування ІТС та підлягають аналізу під час проведення оцінки стану захищеності; визначає та оприлюднює на офіційному веб-сайті Держспецзв'язку у мережі Інтернет перелік спеціалізованого ПЗ та програмно-апаратних засобів, які використовуються для проведення оцінки захищеності тощо. Державні органи, органи місцевого самоврядування, військові формування, підприємства, установи і організації незалежно від форм власності, в яких здійснюється оцінка стану захищеності: надають комісії всі необхідні документи, що стосуються функціонування ІТС; надають комісії доступ до ІТС; повідомляють Держспецзв'язку про стан виконання рекомендацій, зазначених в Акті [12]. При здійсненні таких перевірок (насамперед, позапланових) особливо важлива взаємодія Держспецзв'язку і СБУ. Адже наявні в обох органах на сьогодні технологічні можливості щодо виявлення кібератак та кіберінцидентів дають змогу спільно виявляти вразливості тієї або іншої ІТС, що обробляє ДЕІР.

Одним із механізмів посягань на ДЕІР є втручання в роботу офіційних веб-ресурсів органів державної влади. На сьогодні правові та організаційні засади проведення сканування на предмет вразливості ДЕІР, розміщених в Інтернеті, встановлює відповідний Порядок, який таке сканування передбачає як форму проведення оцінки стану захищеності інформації в ІТС. Сканування полягає у дистанційному виявленні уразливих місць програмно-апаратних засобів (місць, використовуючи які зловмисник може порушити цілісність, доступність, конфіденційність інформації або спостережність системи), які забезпечують функціонування ДЕІР, розміщених в Інтернеті. Об'єктом сканування є ІТС або її окремі елементи, в яких обробляються ДЕІР, розміщені в Інтернеті, незалежно від наявності в таких ІТС побудованої КСЗІ. До зазначених інформаційних ресурсів, зокрема, належать Інтернет-ресурси органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій державної форми власності.

До початку сканування підрозділ Держспецзв'язку: розробляє загальну програму та методику сканування; письмово погоджує із розпорядником ДЕІР, розміщеного в Інтернеті, та власником ІТС (якщо розпорядник ДЕІР не є власником ІТС, у якій обробляється відповідний ресурс) строки, обсяг та зміст проведення сканування; не пізніше ніж за три робочих дні письмово інформує Службу безпеки України про об'єкт, строки та методи проведення сканування. Передбачається також термінове інформування за допомогою електронної пошти. Крім того, Держспецзв'язку протягом п'яти календарних днів з моменту виявлення під час сканування випадків порушення правил обробки та захисту інформації, які можуть спричинити розголошення службової інформації або інформації, що становить державну таємницю, інформує про них Службу безпеки України [14].

Посадовим особам Держспецзв'язку, що безпосередньо проводять сканування, а також співробітникам Служби безпеки України, яким відповідно до визначених законодавством повноважень стали відомі результати сканування, забороняється використовувати виявлені вразливості для одержання доступу до змісту інформації, зокрема персональних даних, а також розголошувати результати сканування [14]. Цією

нормою встановлюються важливі правові гарантії захищеності відповідної інформації з обмеженим доступом.

Наведені вище приклади взаємодії між двома суб'єктами національної системи кібербезпеки передбачені адміністративними процедурами у сфері ТЗІ та перевірки відповідності захисту ДЕІР в ІТС, а також розміщеного в Інтернеті контенту, встановленим нормативним вимогам.

Відзначимо також, що Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (далі – Загальні вимоги), затверджені 19 червня 2019 р., вперше на загальнодержавному рівні (не враховуючи Постанову Правління Національного банку України від 28.09.2017 № 95 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України" [16]) визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури. Відповідно до Загальних вимог власник та/або керівник об'єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу ДКІБ СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єктів критичної інформаційної інфраструктури [16].

Новелою Загальних вимог є використання державними органами основного та резервного захищеного дата-центру збереження ДЕІР Державного центру кіберзахисту з метою створення резервних копій своїх інформаційних ресурсів та їх оперативного відновлення у разі пошкодження або знищення [16]. З урахуванням чисельних кібератак та кіберінцидентів, що виявляються як Держспецзв'язку, так і СБУ створення резервних копій ДЕІР є важливою передумовою збереження їх доступності і цілісності.

Зазначені вище нормативно-правові акти не враховують вимоги Закону України "Про основні засади забезпечення кібербезпеки України" у частині запровадження аудиту інформаційної безпеки. Тому у контексті розвитку державно-приватного партнерства підтримуємо необхідність врегулювання на рівні постанови Кабінету Міністрів України саме проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, проект якої було оприлюднено у квітні 2020 року [17]. Позитивним вважаємо включення до проекту регуляторного акта як вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, так і порядку проведення такого незалежного аудиту.

Висловлюємо припущення, що зазначений правовий механізм (Загальні вимоги і незалежний аудит) має небагато шансів на успішне функціонування у межах держави без належного визначення переліку об'єктів критичної інфраструктури. А тому актуалізуємо необхідність прийняття такого акта. Позитивно відзначаємо, що на момент завершення цього дослідження, а саме 25 травня 2020 року Держспецзв'язку оприлюднив проект постанови Кабінету Міністрів України "Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури" [18]. Заслуговують на підтримку сформовані з урахуванням зарубіжного досвіду відповідної діяльності перелік секторів (підсекторів), основних послуг критичної інфраструктури, а також методика категоризації об'єктів критичної інфраструктури.

Насамкінець зазначимо, що проект закону про внесення змін до Закону України "Про Службу безпеки України" щодо удосконалення організаційно-правових засад діяльності Служби безпеки України [19] частково коригує статус СБУ як суб'єкта національної системи кібербезпеки. Хоча, на нашу думку, потребує термінологічних

правок. Зокрема, у зазначеному проекті закону використана редакція із Закону України "Про національну безпеку України", який визначив СБ України державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина:

1) протидію розвідувально-підривній діяльності проти України;

2) боротьбу з тероризмом;

3) контррозвідувальний захист… кібербезпеки… та інформаційної безпеки держави, об'єктів критичної інфраструктури [20, ст. 31].

Однак, словосполучення "контррозвідувальний захист кібербезпеки" при визначенні відповідної функції СБ України видається не зовсім коректним. Вважаємо, що кращим для використання і позначення функції СБ України буде термін "контррозвідувальне забезпечення кібербезпеки". Адже поняття "захист кібербезпеки" є етимологічно і змістовно не правильним.

Висновки.

Підсумовуючи викладене, зазначимо, що здійснений аналіз дав підстави для висновку про необхідність врегулювання окремих відносин, пов'язаних з розвитком національної системи кібербезпеки, з урахуванням міжнародної практики.

Зокрема, підтримано необхідність врегулювання на рівні постанов Кабінету Міністрів України:

процедури віднесення до об'єктів критичної інфраструктури з визначенням секторів (підсекторів) і методики категоризації об'єктів критичної інфраструктури;

незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури.

З визначенням процедури віднесення до об'єктів критичної інфраструктури має запрацювати цілісний правовий механізм як кіберзахисту, що здійснюється Держзспецзв'язку, так і контррозвідувального забезпечення СБУ кібербезпеки об'єктів критичної інформаційної інфраструктури.

Акцентовано також увагу на важливості взаємодії Держспецзв'язку і СБУ, зокрема при здійснені перевірок суб'єктів, що оперують ІТС, в яких обробляються ДЕІР, з урахуванням наявних в обох органах технологічних можливостей щодо виявлення кібератак та кіберінцидентів.

Перспективами подальших наукових пошуків визначаємо питання правових механізмів для врегулювання питань державно-приватного партнерства у сфері кібербезпеки в Україні.

Використана література

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

2. Hare, FB. Precision cyber weapon systems: An important component of a responsible national security strategy? Contemporary security policy. Т. 40. Вип. 2. С. 193-213. DOI: 10.1080/13523260. 2018.1529369.

3. Patrascu, P. The Appearance and Development of National Cyber Security Strategies. Proceedings Paper: 14th International Scientific Conference on eLearning and Software for Education - eLearning Challenges and New Horizons. 2018. Vol 4. Стр. 53-59. DOI: 10.12753/2066-026X-18-222.

4. Stitilis, D, Pakutinskas, P, Malinauskaite, I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*. 2017. № 30. С. 1151-1168.

5. Про Службу безпеки України: Закон України від 25.03.92 р. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382.

6. Про телекомунікації: Закон України. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155. Ст. 39.

7. Про затвердження Правил надання та отримання телекомунікаційних послуг: Постанова Кабінету Міністрів України від 11.04.12 р. № 295. *Офіційний вісник України*. 2012. № 29. Ст. 1074, п. 36.

8. Про затвердження Порядку підключення до глобальних мереж передачі даних: Постанова Кабінету Міністрів України від 12.04.02 р. № 522. *Офіційний вісник України*. 2002. № 16. Ст. 864.

9. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29.03.06 р. № 373. *Офіційний вісник України*. 2006. № 13. Ст. 878.

10. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах: Постанова Кабінету Міністрів України від 16.11.02 р. № 1772. *Офіційний вісник України*. 2002. № 47. Ст. 2155.

11. Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Наказ Адміністрації Держспецзв'язку від 10.06.08 р. № 94. *Офіційний вісник України*. 2008. № 52. Ст. 1753.

12. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Наказ Адміністрації Держспецзв'язку від 02.12.14 р. № 660. *Офіційний вісник України*. 2015. № 12. Ст. 323.

13. Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління: Постанова Кабінету Міністрів України від 03.08.05 р. № 688. URL: https://zakon.rada.gov.ua/laws/show/688-2005-%D0%BF

14. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті: Наказ Адміністрації Держспецзв'язку від 15.01.16 р. № 20. *Офіційний вісник України*. 2016. № 17. Ст. 695.

15. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Правління Національного банку України від 28.09.17 р. № 95. *Офіційний вісник України*. 2017. № 84. Ст. 2575.

16. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518. *Офіційний вісник України*. 2019. № 50. Ст. 1697, п. 50.

17. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури: проект постанови Кабінету Міністрів України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=320263&cat_id=38837

18. Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури: проект постанови Кабінету Міністрів України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=321031&cat_id=38837

19. Про внесення змін до Закону України "Про Службу безпеки України" щодо удосконалення організаційно-правових засад діяльності Служби безпеки України: проект закону. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68347

20. Про національну безпеку України: Закон України від 21.06.18 р. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

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