УДК 342.951

ГУРЖІЙ С.В., провідний науковий співробітник Українського науково-дослідного Інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-3642-4975.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ НАЦІОНАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ, КОМУНІКАЦІЙНИХ ТА ТЕХНОЛОГІЧНИХ СИСТЕМ, ЩО ЗАБЕЗПЕЧУЮТЬ ФУНКЦІОНУВАННЯ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Анотація. *Визначено ризики та загрози несанкціонованого доступу до державних інформаційних ресурсів, комунікаційних та технологічних систем. Деталізовано порядок та умови адміністрування державних інформаційних ресурсів, що розміщуються на хмарних ресурсах та центрах обробки даних, які розташовані за межами України. Проаналізовано сукупність нормативно-правових актів, схвалених Урядом України з метою посилення кіберстійкості національних інформаційних ресурсів, висвітлено процедуру реагування на кіберінциденти та кібератаки, порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Узагальнено нормативні акти, прийняті Адміністрацією Держспецзв'язку протягом 2023 року з метою посилення кіберстійкості державних інформаційних ресурсів, автоматизованих систем управління технологічними процесами, адміністрування державного реєстру об'єктів критичної інформаційної інфраструктури. Розкрито зміст методичних рекомендацій, присвячених проблематиці реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Окреслено подальші шляхи удосконалення процесів управління вразливостями як важливої складової системи забезпечення кіберстійкості національних інформаційних ресурсів, комунікаційних та технологічних систем, що забезпечують функціонування органів державної влади.*

Ключові слова: *кіберстійкість, кіберзагрози, кібербезпека, національні інформаційні ресурси, технологічні системи, російська військова агресія, правовий режим воєнного стану, релокація державних інформаційних ресурсів, критична інформаційна інфраструктура, автоматизована система.*

Summary*. Risks and threats of unauthorized access to state information resources, communication and technological systems are identified. The procedure and conditions for the administration of state information resources hosted on cloud resources and data processing centers located outside of Ukraine are detailed. The set of regulatory acts approved by the Government of Ukraine with the aim of strengthening the cyber resilience of national information resources was analyzed, the procedure for responding to cyber incidents and cyber attacks, the procedure for searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, and electronic communication networks was regulated. The regulatory acts adopted during 2023 by the Administration of the State Service of Special Communications and Information Protection with the aim of strengthening the cyber resilience of state information resources, automated systems for managing technological processes, administration of the state register of critical information infrastructure objects are summarized. The content of methodological recommendations devoted to the issue of responding by cyber security entities to various types of events in cyberspace, increasing the level of cyber protection of electronic document management systems, and strengthening the protection of critical infrastructure objects has been revealed. It is concluded that the process of managing*

vulnerabilities is aimed at their constant detection, which can be corrected by implementing patches and configuring security parameters. Further directions of improving vulnerability management processes as an important component of the system of ensuring cyber resilience of national information resources, communication and technological systems that ensure the functioning of state authorities are outlined.

Keywords: *cyber resilience, cyber threats, cyber security, national information resources, technological systems, russian military aggression, martial law, relocation of state information resources, critical information infrastructure, automated system.*

Постановка проблеми. Забезпечення кіберстійкості національних інформаційних ресурсів, комунікаційних та технологічних систем, що забезпечують функціонування органів державної влади, є важливою складовою національної кібербезпеки будь-якої країни. Застосування російською федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протистояння. Комплексний характер загроз національній безпеці в інформаційній та кібернетичній сферах потребує інноваційних підходів до формування та захисту інформаційного простору. В умовах повномасштабної війни саме кібератаки російських хакерів на замовлення військово-політичного керівництва кремля є частиною злочинів російської армії, які спрямовані на знищення та пошкодження, у тому числі, й інформаційної інфраструктури державних органів центральної та місцевої влади. Військова агресія рф провокує та актуалізує питання виживання держави та її основних інституцій, що вбачається неможливим без гарантованого та надійного рівня кіберстійкості, у першу чергу, національної інформаційної інфраструктури. Кіберстійкість державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури безпосередньо залежить не тільки від передумов, які має створити держава, а й від ефективного та надійного кіберзахисту, який має бути побудований на рівні кожної державної організації та установи державного чи приватного сектора.

В цих складних умовах протягом останніх років Україна зробила важливі та поступальні кроки: завершила процеси визначення переліку об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури; створила і забезпечила належне функціонування державного реєстру об'єктів критичної інформаційної інфраструктури з урахуванням сучасних міжнародних стандартів з питань кібербезпеки; запровадила на постійній основі комплексну оцінку стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановила обов'язковість та періодичність проведення такої оцінки з урахуванням категорій наявної критичності об'єктів.

Незважаючи на отримані здобутки, державні органи та підприємства, які знаходяться під перманентною загрозою кібератак російського походження, можуть зазнати різних економічних, фінансових та політичних втрат. Крім того, є ризик зупинки роботи та виведення з ладу критичної інфраструктури в результаті кібератак на ці об'єкти, що гіпотетично може мати масштабні наслідки. Наприклад, в банківській сфері загрозою може бути атака з метою отримання конфіденційної інформації про клієнтів, а в залізничному транспорті – атака на систему автоматичного управління рухом потягів тощо.

Щоб запобігти таким негативним та руйнівним наслідкам, державні органи мають опановувати та впроваджувати на постійній основі комплексну програму управління вразливостями. Державні органи повинні мати можливість оцінювати всі можливі шляхи та контури кібератак, які можуть використати зловмисники або хакери для

проникнення в ту чи іншу автоматизовану або операційну систему. При оцінці поверхні атаки, важливо враховувати всі типи інформаційних активів: сервери, мережі, веб-додатки, бази даних, програмне забезпечення та інші, оскільки кожен з них може бути вразливим та ризикує стати точкою входу для зловмисників. Оцінювання вразливостей всіх активів та їх зв'язків дозволяє збільшити точність визначення потенційних загроз, які можуть виникнути в результаті атак, що допомагає встановлювати пріоритети щодо усунення вразливостей та схвалювати ефективні рішення з питань кібербезпеки та посилення стану кіберстійкості.

Вказані питання, особливо в умовах правового режиму воєнного стану, набувають актуальності та потребують предметного висвітлення на науковому рівні.

Результати аналізу наукових публікацій. Питання, присвячені кіберстійкості досліджували у своїх працях: М. Костроміна, Л. Гарнатко [1], О. Федієнко [2], В. Шиповський [3]. Актуальні проблеми забезпечення кіберстійкості об'єктів критичної інфраструктури вивчали: М. Гуцалюк [4], І. Мальцева, Ю. Черниш та В. Овсянніков [5], Я. Мануілов [6], Р. Мурасов, Я. Мельник [7], А. Тарасюк [8]. Національні інформаційні ресурси, що забезпечують функціонування органів державної влади та стан забезпечення їхньої безпеки, перебували у фокусі уваги: О. Довганя [9], О. Онищенка [10], А. Марущака [11], С. Петрова [12], В. Гловацького [13]. Проте жоден із вказаних фахівців предметно не розглядав особливості забезпечення кіберстійкості національних інформаційних ресурсів, комунікаційних та технологічних систем, що забезпечують функціонування органів державної влади в умовах правового режиму воєнного стану, що, беззаперечно, посилює актуальність цієї наукової статті.

Метою статті є визначення, на підставі аналізу деяких сучасних нормативно-правових актів, особливостей забезпечення кіберстійкості державних інформаційних ресурсів, комунікаційних та технологічних систем, що забезпечують функціонування органів влади в Україні в умовах воєнного стану, для вироблення шляхів управління та оцінювання вразливостей у ландшафті кіберзагроз.

Виклад основного матеріалу. Загалом кіберстійкість визначається як здатність системи захищатися від інцидентів кібератак та підтримувати належний рівень продуктивності за рахунок підтримання критичної функціональності та своєчасного відновлення до попереднього стану, який був до скоєння інциденту. Зловмисники та хакери намагаються використовувати слабкі місця в комп'ютерних системах, соціальних мережах чи інформаційній інфраструктурі. Вони можуть переслідувати широкий спектр цілей, включаючи: несанкціонований доступ до конфіденційної інформації, провокування масштабного збою у штатній роботі, створення передумов з метою отримання доступу до систем та комп`ютерів заради фінансової вигоди або саботажу. За таких умов, Україна має максимально активізувати процес розбудови та стабільного функціонування національної системи кібербезпеки для попередження та нейтралізації наслідків ворожих кібератак та кіберінцидентів. З початком повномасштабного російського вторгнення, одним із першочергових завдань держави стало врегулювання сфери безперебійного та повноформатного забезпечення функціонування державних інформаційних ресурсів.

Враховуючи наявні загрози та виклики, Кабінет Міністрів України своєю постановою затвердив порядок передачі, збереження, функціонування та доступу до державних інформаційних ресурсів (публічних електронних реєстрів) та їх резервних копій, розміщених на хмарних ресурсах або центрах обробки даних, що розташовані за межами України [14].

Зокрема, нормативно встановлено, що розміщення державних інформаційних ресурсів та їх резервних копій на хмарних ресурсах або центрах обробки даних, що

розташовані за межами України, здійснюється на підставі договору, що укладається замовниками за умови наявності обов'язкового погодження з органами Служби безпеки України. Під час переміщення інформаційно-комунікаційних систем, що не мають комплексної системи захисту інформації з підтвердженою відповідністю, замовники вживають заходів для її побудови або впровадження системи управління інформаційною безпекою щодо такої інформаційно-комунікаційної системи відповідно до законодавства України у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

При цьому, передача або переміщення державних інформаційних ресурсів до хмарних ресурсів або центрів обробки даних, що розташовані за межами України, здійснюється з використанням фізичних носіїв або електронних комунікаційних мереж. На нормативному рівні передбачено, що під час переміщення інформаційно-комунікаційної системи в цілому залучаються уповноважені представники замовника, адміністратора або технічного адміністратора державних інформаційних ресурсів, а передача (переміщення) державних інформаційних ресурсів, що містять конфіденційну інформацію, з використанням електронних комунікаційних мереж повинна здійснюватися виключно з використанням засобів криптографічного захисту інформації. У засобах криптографічного захисту інформації, які застосовуються для передачі (переміщення) державних інформаційних ресурсів, використовуються криптоалгоритми та криптопротоколи, які визначені національними стандартами, зокрема наведеними у переліку стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, визначеному Адміністрацією Держспецзв'язку, або ті, на які за результатами експертних досліджень видано позитивний експертний висновок.

Доступ з метою адміністрування державних інформаційних ресурсів, що розміщуються на хмарних ресурсах та центрах обробки даних, які розташовані за межами України, забезпечується з використанням засобів криптографічного захисту інформації. Забезпечення функціонування (зокрема адміністрування) державних інформаційних ресурсів здійснюється за участю представників замовника або адміністратора, або технічного адміністратора державних інформаційних ресурсів, відповідно до законодавства України у сфері захисту інформації. Резервування державних інформаційних ресурсів здійснюється з дотриманням встановлених для таких державних інформаційних ресурсів вимог щодо цілісності, конфіденційності та доступності. До переліку видів державних інформаційних ресурсів та систем, щодо яких може здійснюватися резервне копіювання, нормативно відносяться: бази даних, національні електронні інформаційні ресурси, публічні електронні реєстри, інформаційні (автоматизовані) системи, інформаційно-комунікаційні системи.

Таким чином, в умовах правового режиму воєнного стану на державному рівні було започатковано процедуру релокації державних інформаційних ресурсів – їхнє перенесення за межі України задля збереження та уникнення ризиків та загроз, пов'язаних із несанкціонованим їх поширенням або вірогідним знищенням ворогом таких ресурсів. Загальновідомо, що інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення). Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь із вказаних властивостей, відповідно є загрозами конфіденційності, цілісності або доступності

інформації. Захист інформації повинен забезпечуватись протягом всього періоду її існування. Адже загрози можуть впливати на інформацію не безпосередньо, а також й опосередковано. Наприклад, втрата керованості може призвести до нездатності системи забезпечувати захист інформації і, як результат, до втрати певних властивостей оброблюваної інформації. Політика безпеки інформації в автоматизованих системах є важливою частиною загальної політики безпеки будь-якого державного органу або організації. Для кожної автоматизованої системи політика безпеки інформації може бути індивідуальною і залежати від технології обробки інформації, особливостей операційної системи, фізичного середовища, а також від багатьох інших факторів та чинників.

В окресленому контексті Україна спрямує власні зусилля як на розвиток паритетної взаємної довіри з міжнародними партнерами задля спільної відповіді на кібератаки і подолання кризових ситуацій у кіберпросторі, так і на суто практичну співпрацю з метою обміну досвідом та інформацією про кібератаки і кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів тощо. Одночасно Україна бере активну участь у діалозі в рамках діяльності міжнародних організацій щодо спільного вироблення норм поведінки у кіберпросторі та вдосконалення відповідної нормативно-правової бази. Так, 21 червня 2024 року набрала чинності Постанова Кабінету Міністрів України "Деякі питання захисту державних інформаційних ресурсів та інформації з обмеженим доступом, які використовуються Міністерством оборони та Збройними Силами" [15].

Цим нормативним актом передбачаються особливості захисту державних інформаційних ресурсів та інформації з обмеженим доступом, які використовуються Міноборони та Збройними Силами України. На виконання цієї постанови нормативно дозволяється використання Міноборони та Збройними Силами в своїх інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах програмних засобах, засобах технічного захисту інформації, засобах криптографічного захисту інформації із підтвердженою відповідністю вимогам держав-партнерів, зокрема таких як: США, Канади, Німеччини, Франції, Польщі, Великобританії, Естонії, Латвії, Литви, Фінляндії, Данії, Норвегії, Нідерландів, Іспанії, Італії, Греції, Словенії, Австралії, Португалії, Швеції, Люксембургу, Бельгії, Румунії. Таким чином, Кабінет Міністрів України дозволив Збройним Силам України використовувати іноземні засоби у сфері здійснення захисту інформації у вітчизняних інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах програмних засобах, засобах технічного захисту інформації, засобах криптографічного захисту інформації тощо. Тобто в контексті посилення спроможностей держави щодо забезпечення динамічного розвитку захисту державних інформаційних ресурсів, систем технічного і криптографічного захисту інформації Україна покладається на допомогу партнерів та союзників. Захист інформації, що обробляється в автоматизованих системах, полягає у створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також значно знизити реальні та потенційні збитки.

З метою посилення кіберстійкості та адекватного реагування на кіберінциденти/кібератаки в умовах кібервійни було схвалено низку нормативно-правових актів, зокрема: Постанову Кабінету Міністрів України "Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі" від 04.04.23 р. № 299 [16], Постанову Кабінету Міністрів України "Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних

комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж" від 16.05.23 р. № 497 [17].

Так, Кабінет Міністрів України своїми постановами схвалив процедуру реагування на кіберінциденти та кібератаки з метою вчасного реагування, визначив правовий порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Нормативно встановлено, що процедура реагування на кібератаки та кіберінциденти складається з декількох етапів: підготовки, виявлення й аналізу, стримування, усунення, відновлення, аналізу ефективності заходів з реагування тощо. Також визначено порядок та умови проведення оцінки критичності кібератак та кіберінцидентів. Зокрема, положеннями чинного законодавства передбачено, що організація пошуку потенційної вразливості системи здійснюється її власником, а у разі потреби власник системи може прийняти рішення про залучення координатора для організації пошуку потенційної вразливості системи. Залучення координатора відбувається шляхом укладення між власником системи та координатором договору про надання послуг з організації пошуку потенційної вразливості системи. Пошук потенційної вразливості системи здійснюється на підставі публічної пропозиції, яка оприлюднюється власником системи на власному офіційному веб-сайті. У разі залучення власником системи координатора публічна пропозиція оприлюднюється координатором на його власному офіційному веб-сайті. У такому разі власник системи оприлюднює на своєму офіційному веб-сайті посилання на відповідну сторінку веб-сайту координатора. Публічна пропозиція розробляється власником системи або координатором відповідно до примірної публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж і методичних рекомендацій з розроблення публічної пропозиції про здійснення пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, що затверджуються Адміністрацією Держспецзв'язку. Після завершення пошуку потенційної вразливості системи дослідник повідомляє про результати власнику системи або координатору згідно із умовами публічної пропозиції та подає йому звіт про таке. Одночасно дія зазначеного порядку не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю, розвідувальну таємницю, банківську таємницю тощо.

У згаданому контексті протягом 2023 року Адміністрацією Держспецзв'язку з метою посилення стану кіберстійкості державних інформаційних ресурсів, автоматизованих систем управління технологічними процесами, державного реєстру об'єктів критичної інформаційної інфраструктури було розроблено такі накази: "Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами" від 29.05.23 р. № 463 [18], "Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі" від 03.07.23 р. № 570 [19], "Про затвердження Положення про систему захищеного доступу державних органів до мережі Інтернет" від 30.08.23 р. № 771 [20], "Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу" від 30.08.23 р. № 773 [21], "Про затвердження форм подання

відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури" від 02.09.23 р. № 793 [22], "Про затвердження форми Плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня "кібератака/кіберінцидент" від 04.10.23 р. № 877 [23], "Про затвердження Рекомендацій з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня "кібератака/кіберінцидент" від 01.12.23 р. № 1077 [24].

Таким чином, були оприлюднені розроблені під егідою Держспецзв'язку України методичні рекомендації, присвячені проблематиці реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, підвищення рівня кіберзахисту систем електронного документообігу, посиленого захисту об'єктів критичної інфраструктури тощо. Зазначені рекомендації не є нормативно-правовими актами, а мають лише інформаційно-роз'яснювальний та рекомендаційний характер. Іншими словами, вони не встановлюють правових норм і є виключно добровільними для використання та застосування. Так, зокрема Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами визначають: вимоги до кіберзахисту, порядок їх впровадження та підтвердження виконання; загальну систему дій щодо проектування, впровадження, підтримки та постійного вдосконалення кіберзахисту автоматизованих систем управління технологічними процесами; мінімальні рівні впровадження стандартного цільового профілю кіберзахисту для об'єктів критичної інфраструктури I рівня (катастрофічні наслідки) та II рівня (критичні наслідки) негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури тощо. Цей документ розроблений з урахуванням Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної структури, стандартів NIST (Національного інституту стандартів і технології США) та інших нормативних актів.

У свою чергу, методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі були розроблені на виконання вимог пункту 3 Постанови Кабінету Міністрів України "Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі" від 04.04.23 р. № 299 та призначені для суб'єктів забезпечення кібербезпеки під час вжиття заходів із кіберзахисту відповідно до етапів реагування на різні види подій у кіберпросторі, визначення категорій (рівнів) їх критичності. Ці методичні рекомендації визначають: необхідний перелік заходів із кіберзахисту, яких можуть вживати суб'єкти забезпечення кібербезпеки послідовно за етапами реагування на кіберінциденти/кібератаки; мету та цілі виконання заходів; механізм застосування критеріїв, за якими визначається категорія (рівень) критичності кіберінциденту/кібератаки; принципи пріоритезації кіберінцидентів/кібератак; типовий перелік заходів із реагування на кіберінциденти/ кібератаки для одночасного відстеження заходів до їх завершення тощо.

Використовуючи розробки та напрацювання Держспецзв'язку, Державна служба статистики України своїм наказом від 24.07.24 р. № 195 [25] нормативно затвердила процес управління вразливостями в інформаційній системі органів державної статистики. Зокрема, встановлено, що процес управління вразливостями визначає механізм здійснення пошуку та виявлення потенційної вразливості в інформаційній системі органів державної статистики, а також управління життєвим циклом вразливостей кібербезпеки з метою проведення їх оцінки, усунення та пом'якшення. Діяльність з управління вразливостями проводиться відповідно до встановленого плану управління вразливостями, а життєвий цикл управління вразливостями включає діяльність із виявлення та оцінки, пріоритизації, усунення та моніторингу вразливостей.

Управління вразливостями, зазвичай, визначається як процес виявлення, класифікації, визначення пріоритетів і усунення вразливостей в операційних системах, корпоративних додатках (як в хмарі, так і локально), браузерах і додатках кінцевих користувачів.

Процес управління вразливостями спрямований на постійне виявлення вразливостей, які можна виправити шляхом здійснення виправлень і налаштування параметрів безпеки. При цьому, вразливістю вважаються будь-які засоби, за допомогою яких зовнішній зловмисник може отримати неавторизований доступ або привілейований контроль над додатком, службою, кінцевою точкою або сервером. Відчутні приклади включають порти зв'язку, відкриті для мережі Інтернет, небезпечні конфігурації програмного забезпечення або операційної системи, методи, за допомогою яких можна отримати привілейований доступ через схвалену взаємодію з даним додатком, а також вразливість, яка дозволяє шкідливим програмам інфікувати систему. Кожна нова вразливість становить потенційний ризик, у зв'язку з чим повинен використовуватися певний процес для того, щоб отримати надійний спосіб швидко і постійно виявляти і усувати вразливості.

Високий рівень управління вразливостями передбачає 6 видів процесів, при цьому кожен з процесів включає в себе підпроцеси і задачі. Перше – виявлення, що включає інвентаризацію всіх активів в середовищі, визначення деталей, включаючи операційну систему, служби, програми та конфігурації, для виявлення вразливостей. Зазвичай це включає як сканування мережі, так і сканування системи за допомогою агента з перевіркою достовірності. Виявлення має виконуватися регулярно по автоматизованому графіку. Друге, розстановка пріоритетів: виявлені вразливості необхідно розділити на групи і призначити їм пріоритети на основі ризиків, в залежності від ступеня важливості для організації. Третє, це оцінка, що надає змогу встановити базовий рівень ризику для конкретної вразливості. По-четверте, це визначення засобів усунення на основі пріоритетності ризиків, що передбачає виправлення (за допомогою реконфігурації) та встановлення засобів контролю, щоб виправлення було успішно завершено і прогрес можна було задокументувати. П'яте, це перевірка виправлення, яка виконується за допомогою додаткових сканувань. По-шосте, це звітування з метою інформування керівництва щодо поточного стану ризиків, пов'язаного із IT-вразливостями.

Крім того, чимало рішень кібербезпеки виходять за рамки простого управління вразливостями, додаючи цінність за рахунок інтеграції інших функцій безпеки, які в сукупності допомагають краще захистити середовище шляхом: виявлення вразливостей; класифікації даних; виявлення вторгнень; управління привілейованим доступом; виявлення загроз і реагування; аудиту відповідності та звітності. Саме тому ефективне управління вразливостями означає перехід від методу "виправляти все і завжди", до розумної розстановки пріоритетів щодо усунення загроз [26, с. 27]. Тобто управління вразливостями – важливий елемент кіберстійкості та захисту інформаційної інфраструктури державного сектору. Безпека даних та захист від кібератак вимагають постійного моніторингу, проактивного виявлення та усунення ризиків, а також постійного аналізу і розуміння тієї чи іншої кібератаки. Розуміння та тлумачення небезпек та реалізація відповідних контрзаходів захисту забезпечуватимуть захист даних від потенційних кіберзагроз.

Висновки.

Держава робить важливі та поступальні кроки з метою посилення стану кіберстійкості національних інформаційних ресурсів, комунікаційних та технологічних систем, що забезпечують функціонування органів державної влади в умовах правового режиму воєнного стану. Сучасні платформи виявлення кіберзагроз агрегують та

аналізують дані про такі загрози із різних джерел, надаючи корисну інформацію з метою організації допомоги державним органам у випередженні нових загроз. Основна ідея посилення стану кіберстійкості передбачає виявлення та управління вразливостями. Виявлення вразливостей здійснюється за допомогою відповідного програмного забезпечення, яке перевіряє комп'ютери, мережі та програми на наявність відомих вразливостей. У процесі пошуку вразливостей значна увага приділяється передовим технологіям штучного інтелекту, які здатні допомогти підвищити швидкість та ефективність у виявленні загроз, здійснювати прогнозування вразливостей та автоматизацію відповідей.

При цьому управління вразливістю – це процес виявлення, оцінки, розставлення пріоритетів, виправлення (повне усунення та запобігання потенційним атакам або мінімізація наслідків та масштабу атак) та складання звітів про вразливості безпеки у веб-додатках, мобільних пристроях та програмному забезпеченні. Управління вразливостями – це систематичний процес, що включає виявлення, оцінку, пріоритизацію та усунення вразливостей в ІТ-системах, додатках і мережах, а його мета – зменшити ризик використання цих вразливостей, постійно відстежуючи слабкі місця та застосовуючи необхідні заходи безпеки. Управління вразливістю та загрозами – це безперервний процес, що включає всі етапи роботи з вразливістю та загрозами: виявлення, розстановка пріоритетів, формування політик, актуалізація та усунення.

Управління вразливостями в сучасному складному ландшафті кібербезпеки посідає важливе місце. В результаті управління вразливостями надається можливість отримувати актуальні дані щодо стану ІТ-середовища, їхньої наявності та пов'язаних з ними ризиків. Вразливості не повинні бути проігнорованими та мають на меті значно зменшити або обмежити ризики проведення кібератак та посилити стан кіберзахисту. Етапи усунення вразливостей передбачають декілька можливих варіантів: виправлення – повне усунення вразливості без можливості її використання; пом'якшення наслідків – мінімізація ймовірності чи наслідків використання вразливості; прийняття – відсутність будь-яких дій через незначну небезпеку вразливості або значне перевищення вартості усунення над витратами у разі її експлуатації. Завдяки постійному скануванню та моніторингу цифрових активів ці рішення надають уявлення про потенційні ризики та пропонують вказівки щодо виправлення або пом'якшення виявлених слабких місць для покращення загальної безпеки. Управління вразливістю являє собою поєднання процесів і продуктів, спрямованих на підтримку інвентаризації цифрової інфраструктури того чи іншого державного органу, її перевірку на вразливості та усунення виявлених недоліків.

Таким чином, управління вразливостями є необхідним компонентом ефективної стратегії кібербезпеки для будь-якого державного органу. Це особливо стосується таких галузей, як фінанси та банківська справа, сільське господарство, важка промисловість, виробництво, енергетика та комунальні послуги, роздрібна торгівля, транспорт та державне управління.

Використана література

1. Костроміна М.О., Гарнатко Л.О. Кіберстійкість і кібербезпека: у чому різниця? *Сучасний захист інформації.* 2022. № 4 (52). С. 71-75.

2. Федієнко О.П. Міжнародні стандарти оцінки кіберстійкості. *Інформація і право.* № 3(50)/2024. С. 124-135.

3. Шиповський В. Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури. *Захист інформації.* 2023. Т. 25. № 1. С. 37-45.

4. Гуцалюк М.В. Стратегії протидії сучасним кіберзагрозам та забезпечення кіберстійкості критичної інфраструктури України. *Інформація і право.* № 2(49)/2024. С. 164-177.

5. Мальцева І.Р., Черниш Ю.О., Овсянніков В.В. Аналіз методик оцінки кіберстійкості критичної інфраструктури. *Кібербезпека: освіта, наука, техніка.* – (Електронне фахове наукове видання). 2021. С. 29-35.

6. Мануїлов Я.С. Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. *Інформація і право.* № 1(44)/2023. С. 154-167.

7. Мурасов Р., Мельник Я. Оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 1(46). С. 41-44.

8. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи: монографія. Одеса: Фенікс, 2020. 400 с.

9. Довгань О.Д. Інформаційні ресурси: національні та державні, зміст, поняття. *Інформація і право.* № 3(15)/2015. С. 85-91.

10. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища / О.С. Онищенко, В.М. Горовий, В.І. Попик та ін. – (НАН України, Нац. б-ка України ім. В.І. Вернадського). Київ, 2014. 243 с.

11. Марущак А.І., Петров С.Г. Зміст поняття "державні електронні інформаційні ресурси". *Інформація і право.* № 4(27)/2018. С. 15-21.

12. Петров С.Г. Захист державних електронних інформаційних ресурсів України. *Інформація і право.* № 3(34)/2020. С. 62-68.

13. Гловацький В.В. Безпека державних інформаційних ресурсів. *Наукові записки Українського науково-дослідного інституту зв'язку.* 2016. № 3(43). С. 79-82.

14. Деякі питання забезпечення функціонування державних інформаційних ресурсів: Постанова Кабінету Міністрів України від 30.12.22 р. № 1500. URL: https://zakon.rada.gov.ua/laws/show/1500-2022-%D0%BF#Text

15. Деякі питання захисту державних інформаційних ресурсів та інформації з обмеженим доступом, які використовуються Міністерством оборони та Збройними Силами: Постанова Кабінету Міністрів України від 18.06.24 р. № 719. URL: https://zakon.rada.gov.ua/laws/show/719-2024-%D0%BF#Text

16. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.23 р. № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

17. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: Постанова Кабінету Міністрів України від 16.05.23 р. № 497. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text

18. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 29.05.23 р. № 463. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodic hnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnolog ichnimi-procesami

19. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03.07.23 р. № 570. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberp rostori

20. Про затвердження Положення про систему захищеного доступу державних органів до мережі Інтернет: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.08.23 р. № 771. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-

derzhspeczv-yaz ku-pro-zatverdzhennya-polozhennya-pro-sistemu-zakhishenogo-dostupu-derzhavnikh-organiv-do-merezhi-int ernet-vid-30-serpnya-2023-roku-771

21. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 30.08.23 р. № 773. URL:https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kib erzakhistu-sistem-elektronnogo-dokumentoobigu-vid-30-serpnya-2023-roku-773

22. Про затвердження форм подання відомостей до державного реєстру об'єктів критичної інформаційної інфраструктури: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02.09.23 р. № 793. URL:https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-form-podannya-vidomostei-do-derzhavnogo-reyestru-ob-yektiv-kritichnoyi-informaciinoyi-infrastrukturi-vid-02-veresnya-2023-roku-793

23. Про затвердження форми Плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня "кібератака/кіберінцидент": наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 04.10.23 р. № 877. URL:https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-pro-zatverdzhennya-formi-planu-zakhistu-ob-yekta-kritichnoyi-infrastrukturi-za-proyektnoyu-zagrozoyu-nacionalnogo-rivnya-kiberataka-kiberincident-vid-04–zh ovtnya-2023-roku-877

24. Про затвердження Рекомендацій з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня "кібератака/кіберінцидент": наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 01.12.23 р. № 1077. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-01-grudnya-2023-roku-1011-pro-zatverdzhennya-richnogo-planu-zdiisnennya-zakhodiv-derzhavnogo-naglyadu-kontrolyu-u-sferi-doderzhannya-vimog-zakonodavstva-z-nadannya-poslug-u-galuzi-tekhnich nogo-zakhistu-informaciyi-ta-kriptografichnogo-zakhistu-informaciyi-krim-elektronnikh-dovirchikh-poslug-administraciyeyu-derzhavnoyi-sluzhbi-specialnogo-zv-yazku-ta-zakhistu-informaciyi-ukrayini-na-2024-rik

25. Процес управління вразливостями в інформаційній системі органів державної статистики: наказ Державної служби статистики України від 24.07.24 р. № 195. URL: https://www.ukrstat.gov. ua/norm_doc/2024/195/prosec.pdf

26. Найман Г.Г., Гаркавенко Д.М. Методи та засоби управління вразливостями корпоративної інформаційної системи на основі машинного навчання. *Сучасний захист інформації.* 2021. № 3(47). С. 24-28.

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