УДК 342
DOI https://doi.org/10.32850/sulj.2022.4.3.38

КІБЕРБЕЗПЕКА КРИТИЧНИХ ІНФРАСТРУКТУР: ЗАКОРДОННИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

Пядишев В. Г.

Сьогодні критичні інфраструктури України зазнають дестабілізуючих атак з боку російської федерації. Здійснюються як фізичні, і кібератаки. У цих умовах захист критичних інфраструктур, їх відновлення після атак, а також забезпечення їхньої стійкості до атак є одним із пріоритетних завдань держави. І хоча фахівці України відшукують можливості відновлювати пошкоджені критичні інфраструктури в найкоротший час після атак, усі передові практики захисту критичних інфраструктур від атак, зокрема, кібератак становлять для фахівців України величезний інтерес. Обсяг статті не дозволяє здійснити огляд усіх країн світу. Тому ми обрали найпередовіші країни: в Азії це Сінгапур, на американському континенті це США, у Європі це Євросоюз.

У Сінгапурі привертає увагу Закон про кібербезпеку, який є основою для захисту критично важливої інформаційної інфраструктури від загроз кібербезпеці, вжиття заходів щодо запобігання, управління та реагування на загрози та інциденти кібербезпеки критичних інфраструктур. Інтерес представляє також Агентство кібербезпеки Сінгапуру та його робота.

В Австралії основою для управління ризиками, пов'язаними з критичною інфраструктурою є Закон про безпеку критично важливої інфраструктури №29, 2018. Закон суворо визначає права та обов'язки Міністра, Секретаря, а також всіх осіб, які з тих чи інших причин зобов'язані підтримувати кібербезпеку критичних інфраструктур.

У Сполучених Штатах Америки питаннями кібербезпеки загалом та питаннями захисту критичної інфраструктури займається єдине агентство – «Агентство кібербезпеки та безпеки інфраструктури». Сприяння широкому обміну інформацією щодо критично важливих інфраструктур між власниками та операторами критично важливих інфраструктур та державними органами, що відповідають за захист інфраструктури, чим знижується вразливість країни перед тероризмом, здійснюється відповідно до Закону про інформацію критичної інфраструктури від 25 листопада 2002 р.

У Євросоюзі з питань захисту від кіберіатак важливе значення має Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 р. «Про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем на території Союзу». Вона встановлює заходи, спрямовані на досягнення найвищого загального рівня безпеки мережевих та інформаційних систем у Євросоюзі.

Незважаючи на масовість, глибину та витонченість кібератак, які здійснює російська федерація, служби України вишукують можливості досить швидкого відновлення критичних інфраструктур. При цьому вони набувають найціннішого досвіду із захисту та відновлення критичних інфраструктур. Але все ж таки для них сьогодні важлива кожна крихта кращих практик, напрацьованих закордонними колегами.

Ключові слова: *критична інфраструктура, кібербезпека, кібератака, стійкість, відновлення.*

Piadyshev V. H. Cyber security of critical infrastructures: foreign experience and Ukrainian realities

Today, Ukraine's critical infrastructures are under destabilizing attacks from the Russian Federation. Both physical and cyber attacks are being carried out. Under these conditions, the protection of critical infrastructures, their recovery after attacks, as well as ensuring their resilience to attacks are one of the priority tasks of the state. And although Ukrainian specialists are looking for ways to restore damaged critical infrastructures as soon as possible after attacks, all the best practices for protecting critical infrastructures from attacks, in particular cyber attacks, are of great interest to Ukrainian specialists. The volume of the article does not allow for a review of all countries of the world. Therefore, we have chosen the most advanced countries: in Asia it is Singapore, in the Americas it is the United States, in Europe it is the European Union.

In Singapore, attention has been drawn to the Cyber Security Act, which forms the basis for protecting critical information infrastructure from cyber security threats, taking measures to prevent, manage and respond to cyber security threats and incidents of critical infrastructures. Also the Singapore Cyber Security Agency and its work are of great interest.

In Australia, the Critical Infrastructure Security Act 29, 2018 is the basis for managing the risks associated with

critical infrastructure. The Act strictly defines the rights and obligations of the Minister, the Secretary, and all persons who, for one reason or another, are required to maintain the cybersecurity of critical infrastructures.

In the United States of America, cybersecurity in general and the protection of critical infrastructure are handled by a single agency, the Cybersecurity and Infrastructure Security Agency. Promoting the wide exchange of information on critical infrastructures between owners and operators of critical infrastructures and government agencies responsible for protecting the infrastructure, thereby reducing the country's vulnerability to terrorism, is carried out in accordance with the Critical Infrastructure Information Law of November 25, 2002.

In the European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 "On measures to ensure a high overall level of security of network and information systems in the territory of the Union" is of great importance on issues of protection against cyberattacks. It establishes measures aimed at achieving a high overall level of security for network and information systems in the European Union.

Despite the mass nature, depth and sophistication of cyber attacks carried out by the Russian Federation, Ukrainian services are finding ways to quickly restore critical infrastructures. At the same time, they gain valuable experience in protecting and restoring critical infrastructures. But still, every grain of the best practices developed by foreign colleagues is important for them today.

Key words: *critical infrastructure, cyber security, cyber attack, resilience, recovery.*

Загальна постановка проблеми. Нині, під час крайньої активізації агресивних дій збройних сил Російської Федерації проти України, питання захисту критичних інфраструктур України стоїть особливо гостро. Крім фізичних атак на наші критичні інфраструктури, постійно проводяться кібератаки. Кібератаки, які здійснювалися досі на критичні інфраструктури будь-якої іншої країни у світі, за регулярністю, масовістю, глибиною та витонченістю не йдуть у жодне порівняння з кібератаками, які сьогодні відбуваються на критичні інфраструктури України [1]. Кібератаки здійснюються також на державні сайти України [2].

Проте критичні інфраструктури України виживають та відновлюються після вказаних кібератак. Це зумовлено низкою причин.

Ступінь наукової розробки теми. Ще до великомасштабних атак в Україні наукові дослідження у сфері захисту критичних інфраструктур від кібератак проводились такими вченими як П. Д. Рогов [3], І. П. Сініцин, П. П. Ігнатенко, О. О. Слабоспицька, О. В. Артеменко [4], Н. О. Ткачук [5], І. Субач [6]. Ці та інші дослідження сприяли розробці відповідної нормативно-правової бази, яку склали такі документи:

– Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [7];

– Вимоги до функціонування системи кіберзахисту у банківській системі України [8];

– Положення про організацію кіберзахисту у банківській системі України [9];

– Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимогу щодо захисту якої встановлено законом [10];

– Методичні рекомендації щодо категоризації об'єктів критичної інфраструктури [11];

– Законопроект «Про внесення змін до деяких законів України щодо невідкладних заходів щодо посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури» [12];

– Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, практичних прийомів боротьби з кібератаками на критичні інфраструктури, а також відновлення останніх після кібератак[13].

Також можна стверджувати, що сьогодні у процесі відображення кібератак та осмислення їх результатів в Україні напрацьовується безцінний новий передовий досвід.

Разом з тим, немає підстав вважати, що українські фахівці вже сприйняли увесь накопичений досі передовий досвід зарубіжних країн у сенсі протидії кібератакам на критичні інфраструктури. Підставою для такого висновку є відсутність в українських наукових фахових виданнях обговорення результатів зарубіжних наукових досліджень, а також нормативно-правової бази з питань протидії кібертакам на критичні інфраструктури. Водночас євроатлантичні прагнення України однозначно передбачають надалі зближення нормативно-правової бази, програмних та інших технічних засобів та методів протидії кібератакам на критичні інфраструктури, а також забезпечення стійкості останніх.

Метою пропонованої роботи є аналіз нормативно-правової бази передових країн з питань захисту від кібератак на критичні інфраструктури, а також забезпечення стійкості останніх.

Виклад основного матеріалу.

Обсяг статті не дозволяє здійснити огляд усіх країн світу. Тому ми обрали найпередовіші країни: в Азії це Сінгапур, на американському континенті це США, у Європі це Євросоюз, ще й Австралія.

Сінгапур

Серед країн Азії найбільшу готовність протистояти кіберзагрозам для критичних інфраструктур демонструє Сінгапур. З 31 серпня 2018 р. набула чинності більшість розділів Закону про кібербезпеку 2018 р. [14]. Закон встановлює основу для захисту критично важливої інформаційної інфраструктури від загроз кібербезпеці, вжиття заходів щодо запобігання, управління та реагування на загрози та інциденти кібербезпеки у Сінгапурі, а також регулювання постачальників ліцензованих послуг кібербезпеки

У країні діє Агентство кібербезпеки Сінгапуру (Cyber Security Agency of Singapore – CSA) [15]. Тут розроблено та неухильно дотримується Звід практичних правил кібербезпеки для критичної інформаційної інфраструктури.

Під час дебатів Комітету постачання 4 березня 2022 року Міністерство зв'язку та інформації оголосило про плани створення безпечного в цифровому відношенні економічно динамічного та соціально стабільного Сінгапуру. Нові ініціативи підвищать кіберстійкість секторів критичної інформаційної інфраструктури (CII) та посилять безпеку кіберпростору Сінгапуру. Особливо слід зазначити, що Агентство кібербезпеки Сінгапуру (CSA) оновить та розширить Закон про кібербезпеку, щоб охопити віртуальні активи (наприклад, хмарні системи), базову цифрову інфраструктуру та ключові цифрові послуги [16].

Австралія

Привертає увагу Закон Австралії про безпеку критично важливої інфраструктури № 29, 2018 [17]. Цей закон створює підґрунтя для управління ризиками, пов'язаними з критичною інфраструктурою. Структура закону така:

(a) ведення реєстру інформації про об'єкти критичної інфраструктури (реєстр не буде оприлюднений);

(b) вимога до особи, відповідальної за один або кілька об'єктів критичної інфраструктури, мати та дотримуватися програми управління ризиками критичної інфраструктури (якщо не застосовується виняток);

(c) вимога сповіщення про інциденти кібербезпеки;

(d) запровадження підвищених зобов'язань щодо кібербезпеки, що належать до систем національного значення;

(e) вимога до певних організацій, які стосуються критично важливого об'єкта інфраструктури, надавати інформацію про цей об'єкт і повідомляти, якщо щодо об'єкта відбуваються певні події;

(f) дозволяти міністру вимагати від певних організацій, пов'язаних з критично важливим об'єктом інфраструктури, здійснювати або утримуватися від скоєння дії чи речі, якщо міністр переконаний у тому, що існує ризик дії чи бездіяльності, що завдало б шкоди безпеці;

(g) дозвіл Секретарю вимагати від певних осіб, які стосуються критично важливого об'єкта інфраструктури, надання певної інформації чи документів;

(h) встановлення режиму реагування Співдружності на серйозні інциденти у сфері кібербезпеки;

(i) дозвіл Секретарю провести оцінку об'єкта критичної інфраструктури, щоб визначити, чи існує ризик національної безпеки, пов'язаний з цим об'єктом.

Певна інформація, отримана або згенерована відповідно до цього Закону або яка стосується його дії, є захищеною інформацією. Існують обмеження щодо того, коли особа може записувати, використовувати або розкривати захищену інформацію.

Положення цього Закону про цивільні санкції можуть бути виконані за допомогою постанов про цивільні санкції, судові заборони або повідомлення про порушення, і можуть бути прийняті належні до виконання зобов'язання щодо дотримання положень про цивільні санкції. З цією метою застосовується Закон про регулюючі повноваження. Деякі положення цього Закону підлягають моніторингу та розслідуванню відповідно до Закону про регулюючі повноваження. Деякі положення цього Закону можуть бути виконані шляхом накладення кримінального покарання.

Міністр може приватно оголосити актив важливим інфраструктурним активом.

Міністр може приватно оголосити об'єкт критичної інфраструктури системою національного значення.

Секретар має надавати міністру звіти для подання до парламенту щодо дії цього закону.

США

При розгляді особливостей боротьби з кіберзагрозами об'єктам критичної інфраструктури США привертає увагу та обставина, що питаннями кібербезпеки загалом і питаннями захисту критичної інфраструктури займається єдине агентство – «Агентство кібербезпеки та безпеки інфраструктури» (Cybersecurity and Infrastructure Security Agency – CISA) [18] .

Щодо підтримки критичної інфраструктури, спеціальне керівництво та супровідний список призначені для підтримки державних, місцевих та галузевих партнерів у визначенні найважливіших

секторів інфраструктури та основних працівників, необхідних для підтримки послуг та функцій, від яких щодня залежать американці, а також здатності працювати стійко, зокрема, під час пандемії COVID-19.

Цей документ також містить рекомендації для державних, місцевих, племінних та територіальних юрисдикцій та приватного сектору щодо визначення основних працівників критичної інфраструктури. Сприяння здатності цих працівників продовжувати роботу в періоди обмежень спільноти, управління доступом, соціального дистанціювання або наказів/розпоряджень про закриття має вирішальне значення для стійкості спільноти та безперервності основних функцій.

Щодо забезпечення кібербезпеки, управління ризиками зі складу CISA, зокрема, для нового коронавірусу (COVID-19) надає керівникам інструмент, який допоможе їм обміркувати проблеми фізичної безпеки, ланцюжка поставок та кібербезпеки, які можуть виникнути внаслідок поширення COVID-19.

CISA випускає попередження, що нагадують про необхідність виявляти пильність щодо шахрайства, зокрема, пов'язаного з COVID-19. Кіберзлочинці можуть надсилати електронні листи зі шкідливими вкладеннями або посиланнями на шахрайські веб-сайти, щоб обманним шляхом змусити жертв розкрити конфіденційну інформацію або зробити пожертву шахрайським благодійним організаціям або організаціям. CISA закликає до обережності при поводженні з будь-якими електронними листами з темою, вкладенням або гіперпосиланням, пов'язаними з COVID-19, і з благаннями, текстами або дзвінками у соціальних мережах, пов'язаних з COVID-19.

13 березня 2020 року CISA випустила попередження, яке закликає організації прийняти підвищений рівень кібербезпеки, закликаючи організації прийняти підвищений рівень кібербезпеки під час розгляду альтернативних варіантів робочого місця для своїх співробітників. Варіанти віддаленої роботи або телероботи вимагають корпоративної віртуальної приватної мережі (VPN) для підключення співробітників до мережі інформаційних технологій (IT) організації.

CISA закликає повідомляти їм про інциденти, фішинг, шкідливі програми та інші проблеми кібербезпеки.

Сприяння широкому обміну інформацією щодо критично важливих інфраструктур між власниками та операторами критично важливих інфраструктур та державними органами, що відповідають за захист інфраструктури, чим знижується вразливість країни перед тероризмом, здійснюється відповідно до Закону про інформацію критичної інфраструктури від 25 листопада 2002 р. [19].

Євросоюз

У законодавстві Євросоюзу з питань захисту від кіберіатак на себе звертає увагу Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 р. «Про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем на території Союзу» [20], яка приймалася з урахуванням 75-ти визначальних факторів та в якій предмет та сфера дії документа визначені у параграфі 1 в такий спосіб.

Директива встановлює заходи, спрямовані на досягнення високого рівня безпеки мережевих та інформаційних систем у Євросоюзі, щоб покращити функціонування внутрішнього ринку.

З цією метою у розділі I Директива:

(a) встановлює зобов'язання для всіх держав-членів прийняти національну стратегію безпеки мереж та інформаційних систем;

(b) створює групу співробітництва для підтримки та сприяння стратегічній співпраці та обміну інформацією між державами-членами, а також для розвитку довіри між ними;

(c) створює мережу груп реагування на інциденти комп'ютерної безпеки («мережа CSIRT»), щоб сприяти розвитку довіри між державами-членами та сприяти швидкому та ефективному оперативному співробітництву;

(d) встановлює вимоги безпеки та сповіщення для операторів основних послуг та постачальників цифрових послуг;

(e) встановлює зобов'язання для держав-членів щодо призначення національних компетентних органів, єдиних контактних осіб та CSIRT із завданнями, пов'язаними з безпекою мереж та інформаційних систем.

Інші параграфи (2 – 6) першого розділу визначають необхідні поняття, а також вимоги, виконання яких необхідне при відпрацюванні ряду процесів та явищ:

– опрацювання персональних даних;

– мінімальна гармонізація;

– визначення;

– ідентифікація операторів основних послуг;

– значний руйнівний ефект.

Розділ II «Національні рамки безпеки мережевих та інформаційних систем» у параграфах 7–10 висвітлює наступні моменти:

– національна стратегія безпеки мережевих та інформаційних систем;

– національні компетентні органи та єдиний контактний центр;

– групи реагування на інциденти комп'ютерної безпеки (CSIRT);

– співпраця на національному рівні.

Розділ III присвячено питанням кооперації між країнами-членами Євросоюзу.

Розділ IV охоплює питання безпеки мережі та інформаційних систем операторів базових послуг

Розділ V стосується питань безпеки мережі та інформаційних систем провайдерів цифрових послуг

Висновки.

1. Сьогодні найбільша кількість кібератак здійснюється на критичні інфраструктури двох країн, а саме: України та росії. Перше – один із елементів російської агресії, а друге – результат відплати України, а також допомоги зарубіжних країн.

2. Незважаючи на масовість, глибину та витонченість кібератак, а також фізичних атак, служби України вишукують можливості досить швидкого відновлення критичних інфраструктур.

3. При цьому фахівці різних спеціальностей України набувають цінного досвіду щодо захисту та відновлення критичних інфраструктур, якого, на своє щастя, досі не могла набути жодна країна у світі.

4. Все ж таки при цьому для українських фахівців сьогодні важлива кожна крихта кращих практик, напрацьованих закордонними колегами.

5. На наш погляд сьогодні найбільш повний, всеосяжний підхід до організації кіберзахисту критичних інфраструктур демонструє країна Сінгапур.

6. Але нам, українцям, в силу нашого географічного положення, наших євроатлантичних прагнень та відповідних перспектив слід, насамперед, вивчити досвід колег з Євросоюзу щодо боротьби з кібератаками на критичні інфраструктури, забезпечення їх стійкості до атак та відновлення після них.

Література

1. Статистика кібератак на українську критичну інфраструктуру. Site/ URL: https://www.cip.gov.ua/ua/news/statistika-kiberatak-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-15-22-bereznya (дата звернення: 06.01.2023).

2. Кібератаки на українські державні сайти. Site. URL: https://uk.wikipedia.org/wiki/ Кібератаки_на_українські_державні_сайти_(2022) (дата звернення: 06.01.2023).

3. Рогов П. Д. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері / П. Д. Рогов, Б. О. Воровіч, В. А. Ткаченко // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. № 1. С. 64-72. URL: http://nbuv.gov.ua/UJRN/Znpcvsd_2017_1_13 (дата звернення: 06.01.2023).

4. Сініцин І. П., Ігнатенко П. П., Слабоспицька О. О., Артеменко О. В.. Комплексний підхід до побудови системи кіберзахисту критичної інформаційної інфраструктури держави. *Проблеми програмування. 2017. № 3.* С. 128-148. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/144499/08-Sinitsyn.pdf?sequence=1. (дата звернення: 06.01.2023).

5. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. *Інформація і право. № 1(24)/2018.* С. 133-138. URL: http://ippi.org.ua/sites/default/files/16_4.pdf. (дата звернення: 06.01.2023).

6. Субач, І. Архітектура та функціональна модель перспективної проактивної інтелектуальної SIEM-системи для кіберзахисту об'єктів критичної інфраструктури / Ігор Субач, Артем Микитюк, Володимир Кубрак // Information Technology and Security. 2019. Vol. 7, Iss. 2 (13). Pp. 208–215. (дата звернення: 06.01.2023).

7. Кабінет Міністрів України. Постанова від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» {Із змінами, внесеними згідно з Постановою КМ № 991 від 02.09.2022}. Site. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 06.01.2023).

8. Розроблені вимоги до функціонування системи кіберзахисту в банківській системі України. *Національний банк України. 19 серп. 2022*. Site. URL: https://bank.gov.ua/ua/news/all/rozrobleni-vimogi-do-funktsionuvannya-sistemi-kiberzahistu-v-bankivskiy-sistemi-ukrayini. (дата звернення: 06.01.2023).

9. Постанова Правління Національного банку України від 12 серпня 2022 року № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України». *Національний банк України. 12 серп. 2022*. Site. URL: https://bank.gov.ua/ua/legislation/Resolution_12082022_178. (дата звернення: 06.01.2023)

10. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної

інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Постанова Кабінету Міністрів України від 11 листопада 2020 р. N 1176. Site. URL: https://ips.ligazakon.net/document/KP201176?an=1. (дата звернення: 06.01.2023)

11. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України. 15.01.2021 № 23. Site. URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text. (дата звернення: 06.01.2023).

12. Asters розробила положення законопроєкту, які допоможуть посилити кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури в Україні. Site. URL: https://eba.com.ua/asters-rozrobyla-polozhennya-zakonoproyektu-yaki-dopomozhut-posylyty-kiberzahyst-derzhavnyh-informatsijnyh-resursiv-ta-obyektiv-krytychnoyi-informatsijnoyi-infrastruktury-v-ukrayini/. (дата звернення: 06.01.2023)

13. Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Site. URL: https://dut.edu.ua/ua/news-1-569-9870-metodichni--rekomendacii--schodo--pidvischennya--rivnya-kiberzahistu-kritichnoi-informaciynoi-infrastrukturi_kafedra-cistem-tehnichnogo-zahistu-informacii. (дата звернення: 06.01.2023).

14. Cybersecurity Act 2018 operative from 31 August 2018 to protect critical information infrastructure against cybersecurity threats. Site. URL: https://www.allenandgledhill.com/media/2996/ag-cybersecurity-act-2018-operative-from-31-august-2018-to-protect-critical-information-infrastructure.pdf. (дата звернення: 06.01.2023).

15. MCI response to PQ on Steps to Protect Singapore's Critical Infrastructure from Malware Threat. Parliament Sitting on 4 July 2022. Site. URL: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/7/mci-response-to-pq-on-steps-to-protect-singapore-critical-infrastructure-from-malware-threat. (дата звернення: 06.01.2023)

16. Leck, A., Chia, K. Singapore: New initiatives to ensure digital security and enhanced cyber resilience. Global Compliance News. March 26, 2022. Site. URL: https://www.globalcompliancenews.com/2022/03/26/singapore-new-initiatives-to-ensure-digital-security-and-enhanced-cyber-resilience-17032022/ (дата звернення: 06.01.2023)

17. Security of Critical Infrastructure Act 2018, No. 29, 2018. Ausrtalia, Compilation No. 4. Compilation date: 2 April 2022. Includes amendments up to: Act No. 33, 2022. Registered: 2 May 2022. Site.URL: https://www.legislation.gov.au/Details/C2022C00160 (дата звернення: 06.01.2023)

18. Cybersecurity and Critical Infrastructure. *Homeland Security*. Site. URL: https://www.dhs.gov/archive/coronavirus/cybersecurity-and-critical-infrastructure (дата звернення: 06.01.2023).

19. The Critical Infrastructure Information Act of November 25, 2002. *Homeland Security*. Site. URL: https://www.dhs.gov/publication/critical-infrastructure-information-act#:~:text=The%20Critical%20Infrastructure%20Information%20Act,reducing%20the%20nation's%20vulnerability%20to (дата звернення: 06.01.2023).

20. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high overall level of security for network and information systems within the Union territory. Site. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення: 06.01.2023).

Пядишев В. Г.,
доктор юридичних наук, професор,
професор кафедри кібербезпеки
та інформаційного забезпечення
факультету підготовки фахівців
для підрозділів кримінальної поліції
Одеського державного університету
внутрішніх справ