КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.16.1927
УДК 007.2+ 004.942 + 004.05 +004.056.5

Козубцов Ігор Миколайович
доктор педагогічних наук, кандидат технічних наук, старший науковий співробітник,
провідний науковий співробітник науково-дослідного відділу кібернетичної безпеки в інформаційно-телекомунікаційних системах науково-дослідного управління (проблем захисту інформації)
Науковий центр зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0002-7309-4365
kozubtsov@gmail.com

Черноног Олександр Олександрович
Державний експерт експертної групи кібербезпеки
Директорат політики цифрової трансформації та інформаційної безпеки у сфері оборони, Міністерство оборони України, Київ, Україна
ORCID ID 0000-0002-3667-8994
skgzua@gmail.com.

Козубцова Леся Михайлівна
кандидат технічних наук, доцент кафедри математики та фізики
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID 0000-0002-7866-8575
l.kozubtsova@i.ua

Артемчук Михайло Васильович
старший викладач кафедри кібербезпеки факультету бойового застосування систем управління
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0003-4640-9429
mavrt@i.ua

Нещерет Іван Григорович
провідний науковий співробітник науково-дослідного відділу кібернетичної безпеки в інформаційно-телекомунікаційних системах науково-дослідного управління (проблем захисту інформації)
Науковий центр зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID 0000-0002-3500-5683
aslam@ukr.net

ВИБІР ОКРЕМИХ ПОКАЗНИКІВ ОЦІНЮВАННЯ ЗДАТНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ І КІБЕРБЕЗПЕКИ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ

Анотація. Предметом дослідження у науковій статті є система захисту і кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку. Метою статті є обґрунтування пропозицій щодо вибору окремих показників оцінювання здатності функціонування системи захисту і кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку в частковим показниками ефективності. Для досягнення мети та поставленого завдання використовувалась сукупність взаємопов'язаних теоретичних методів дослідження: аналізу й узагальнення наукової літератури; структурно-генетичного аналізу, при уточненні об'єкту та предмету дослідження; аналітично-порівняльного аналізу при оцінюванні новизни результатів дослідження; синтез та узагальнення – для обґрунтування показників; узагальнення – для формулювання висновків і рекомендацій. Результати дослідження та висновки. Результатом дослідження стало обґрунтоване рішення нової науково-практичної задачі з обґрунтування показників ефективності функціонування системи захисту інформації і кібербезпеки за результатами аналізу щорічних звітів

інцидентів кібербезпеки. Запропоноване рішення істотно робить вклад в забезпечення національної безпеки і оборони України. Наукова новизна одержаного результату. Вперше запропоновано окремі показники оцінювання здатності (ефективності) функціонування системи захисту і кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку. Перспективи подальших досліджень у даному напрямку. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого обґрунтування методики оцінювання здатності (ефективності) функціонування системи захисту інформації і кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку.

Ключові слова: кіберінцидент; показник; здатність; ефективність; функціонування; система захисту інформації і кібербезпеки; вимоги; узагальнений; інформаційно-комунікаційна система

ВСТУП

Ефективність системи – це властивість системи, що характеризує її здатність виконувати свою цільову функцію. Під «ефективністю системи захисту інформації і кібербезпеки» будемо розуміти ступінь відповідності досягнутих результатів поставленим цілям щодо захисту інформації.

Постановка проблеми. В умовах повномасштабної військової агресії Російської Федерації проти України час в Збройних силах України виникла нагальна потреба у методиці обчислення здатності (ефективності) функціонування системи захисту інформації і кібербезпеки інформації в інформаційно-комунікаційних системах (ІКС) спеціального зв'язку за результатами її здатності протидіяти кіберінцидентам ($E^{Ф}$). Прототип її наданий час відсутній. Розробка зазначеної методики унеможливлено без обґрунтованого вибору окремих показників здатності функціонування системи захисту інформації і кібербезпеки в ІКС в ролі часткових показників ефективності.

Показник ефективності – це величина, що характеризує ступінь досягнення системою будь-якої з поставлених перед нею завдань. Часткові показники ефективності ($E^{Ф}_{П}$), відображають якусь із значущих сторін функціонування системи (ймовірність виявлення порушника або його нейтралізації). Комплексний (узагальнений) показник ефективності ($E^{Ф}$) являють собою комбінацію часткових показників ($E^{Ф}_{П}$).

Таким чином, підставою для вирішення цієї пріоритетної науково-технічної задачі є оперативна ціль «1.5. Удосконалення системи кібербезпеки та захисту інформації» Концепції розвитку сектору безпеки і оборони України визначено [1, с. 33].

Аналіз останніх досліджень і публікацій. Пошук інформації у відкритих джерелах на наявність показників ефективності функціонування системи захисту інформації і кібербезпеки сформував наступну картину.

У статті [2] наведено обґрунтування показника надійної для оцінки ефективності комплексної системи захисту інформації в інформаційно-телекомунікаційній системі оперативного інформування МВС України.

З погляду нашого об'єкту дослідження цікавим є вивчення підходу до вибору показників оцінювання [3].

В роботі [4] подано порядок обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки за результатами аудиту за умови відсутності кіберінциндентів.

Обраний в роботі [5] перелік показників оцінювання ефективності вирішує наукове завдання щодо оцінювання ефективності системи кібербезпеки за результатами виконання заходів забезпечення кібербезпеки ОКІІ організацій.

При вирішенні наукового завдання аналізувався сучасний передовий досвід та рекомендації країн партнерів щодо стандартизації підходів до оцінювання здатності функціонування системи захисту інформації і кібербезпеки інформації інформаційних систем [6 – 8]. Їх застосування в повному обсязі обмежується внаслідок додаткових національних специфічних функціональних здатностей системи захисту інформації і кібербезпеки інформації в ІКС спеціального зв'язку.

З огляду застосованих у публікаціях [2 – 8] підходів до вибору окремих показників оцінювання ефективності функціонування системи захисту інформації і кібербезпеки дають підстави їх застосування у вирішенні даного часткового завдання, яке націлене на забезпечення стійкого функціонування системи захисту інформації і кібербезпеки інформації в ІКС спеціального зв'язку.

Мета статті. Метою статті є обґрунтування пропозицій щодо вибору окремих показників оцінювання здатності функціонування системи захисту інформації і кібербезпеки інформації в ІКС спеціального зв'язку в якості часткових показників ефективності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Рішення цієї науково-технічної задачі пропонується із висування загальних вимог до будь-яких показників ефективності:

мати певний фізичний зміст;

бути придатним для кількісного аналізу;

мати просту і зручну форму;

відображати одну із значущих сторін функціонування системи;

забезпечувати необхідну чутливість.

Вихідними даними для вибору окремих показників оцінювання ефективності функціонування системи захисту інформації і кібербезпеки інформації в ІКС системах спеціального зв'язку є класифікатор інцидентів кібербезпеки та порушень, що застосовується у ЗС України [9]. Категорії інцидентів кібербезпеки в ІКС подано в табл. 1.

Таблиця 1.

Категорії інцидентів кібербезпеки в ІКС

Пріоритет	Назва категорії інциденту кібербезпеки в ІКС
1	Вторгнення зловмисника до системи (Intrusion)
2	Загроза конфіденційності та/або цілісності інформації (Information Content Security)
3	Загроза доступності інформації (Availability)
4	Шкідливий програмний засіб (Malicious Code)
5	Спроба зловмисника щодо вторгнення до системи (Intrusion Attempts)
6	Махінації (Fraud)
7	Наявність відомих вразливостей (Vulnerability)
8	Збір інформації зловмисником (Information Gathering)
9	Зловмисна інформація (Abusive content)
10	Інше (Other)

Згідно документу [7] інцидент, кіберзагроза вважається такою, що відбита системою захисту інформації і кібербезпеки в ІКС, за умови додержання визначених

термінів реагування, знешкодження та відновлення сталого функціонування. Терміни реагування визначені в наказі [7] та не будуть освітлятися оскільки не є предметом нашого дослідження. Тому в ролі окремих показників здатності (ефективності) системи захисту інформації і кібербезпеки в ІКС спеціального зв'язку пропонується застосувати класифікаційні ознаки інцидентів кібербезпеки.

Відповідно до означень показника та вимог що висуваються визначимо фактичну систему зв'язку часткових показників ефективності $E^{Ф}_{П}$ у складі узагальненого показника $E^{Ф}$ (табл. 2).

Таблиця 2.

Система зв'язку показників $E^{Ф}$

частковий показник $E^{Ф}_{П}$	індикатори часткового показника $I^{Ф}_{П}$
Здатність системи протидіяти вторгненню зловмисника до системи ($E^{Ф}_{П1}$)	Компрометація облікового запису системи (сервісу), в тому числі в результаті крадіжки паролю зловмисником
	Компрометація системи, в тому числі в результаті експлуатації вразливості або роботи шкідливого програмного засобу (ШПЗ), що дозволяє віддалене керування
	Несанкціоноване підключення пристрою до ІКС, в тому числі цифрової радіостанції до системи цифрового радіозв'язку
Здатність системи протидіяти загрозам конфіденційності та/або цілісності інформації ($E^{Ф}_{П2}$)	Порушення порядку доступу до інформації в системі, в тому числі в результаті експлуатації вразливості або роботи ШПЗ
Здатність системи протидіяти загрозам доступності інформації ($E^{Ф}_{П3}$)	Відмова в обслуговуванні або порушення сталого функціонування сервісу (об'єкта ІКС) в результаті DoS-, DDo-Sатаки, помилкових дій користувачів, відключення електричної енергії тощо
Здатність системи протидіяти шкідливим програмним засобам ($E^{Ф}_{П4}$)	Виявлення шкідливого програмного засобу, що не дозволяє віддалене керування та не несе загрози цілісності і конфіденційності та/або доступності інформації
Здатність системи протидіяти спробам зловмисника щодо вторгнення до системи ($E^{Ф}_{П5}$)	Виявлення спроб використання зловмисником вразливостей програмного забезпечення, невдалих спроб автентифікації в системі, в тому числі в системі цифрового радіозв'язку
Здатність системи протидіяти махінаціям ($E^{Ф}_{П6}$)	Розсилання зловмисником повідомлень з метою крадіжки пароля користувача
	Несанкціонований доступ до ресурсів системи шляхом використання прав іншого об'єкта
	Передача захищеного паролем архіву під час обміну відкритою інформацією
	Несанкціоноване використання програмного забезпечення, що втручається в роботу комплексу засобів захисту
	Порушення порядку використання ресурсів (використання не за призначенням, у несанкціонованих цілях), в тому числі обробка інформації в автоматизованій системі без створення комплексної системи захисту інформації з підтвердженою відповідністю
Здатність системи протидіяти наявності відомих вразливостей ($E^{Ф}_{П7}$)	Відсутність критичного оновлення безпеки програмного забезпечення (прошивки телекомунікаційного обладнання)
	Функціонування автоматизованого робочого місця або сервера з

ISSN 2663 - 4023

	порушенням вимог з організації антивірусного захисту в ІКС
	Порушення порядку підключення автоматизованої системи до мережі Інтернет
	Порушення встановлених правил розмежування доступу, в тому числі використання пароля понад встановлений термін або такого, що не відповідає визначеним вимогам безпеки
	Використання свідомо уразливого протоколу, режиму роботи, налаштувань обладнання або програмного забезпечення при передачі паролів, іншої чутливої інформації
	Несанкціоноване використання програмного забезпечення, що збільшує ризик порушення безпеки інформації, в тому числі отриманого з недостовірних джерел
	Помилкові дії або бездіяльність користувача, що призводять до збільшення ризику порушення безпеки інформації цифрових систем радіозв'язку
Здатність системи протидіяти збору інформації зловмисником ($E^{Ф}_{П8}$)	Збирання інформації зловмисником про користувача, склад інформаційно-телекомунікаційної системи, існуючі вразливості, в тому числі нетехнічними засобами
Здатність системи протидіяти зловмисній інформації ($E^{Ф}_{П9}$)	Масове розсилання небажаної кореспонденції (SPAM)
	Виявлення у відкритому доступі інформації, що здатна зашкодити інтересам
Здатність системи протидіяти іншим видам загроз ($E^{Ф}_{П10}$)	Виявлення шкідливого програмного засобу, що відбулося одночасно з його блокуванням/видаленням наявним антивірусним програмним забезпеченням за умови знаходження джерела розповсюдження шкідливого програмного засобу за межами ІКС

Для оцінки $I^{Ф}_{П}$ рекомендуються наступні критерії табл. 3.

Таблиця 3.

Критерії оцінювання індикаторів часткових показників $I^{Ф}_{П}$

Критерій $I^{Ф}_{П}$	Рівень
$I^{Ф}_{П}= 0$	не реалізовано загрозу
$I^{Ф}_{П} = 1$	реалізовано загрозу

Для оцінки показників $E^{Ф}_{П}$ рекомендуються наступні критерії (табл. 4).

Таблиця 4.

Критерії оцінювання показників $E^{Ф}_{П}$

Критерій $E^{Ф}_{П}$	Рівень
$0 \le E^{Ф}_{П} \le 0{,}25$	незадовільний (НЗ)
$0{,}25 < E^{Ф}_{П} \le 0{,}5$	низький (Н)
$0{,}5 < E^{Ф}_{П} \le 0{,}75$	середній (С)
$0{,}75 < E^{Ф}_{П} \le 0{,}9$	високий (В)
$0{,}9 < E^{Ф}_{П} \le 1$	найвищий (НВ)

Критерії оцінки ефективності функціонування системи захисту інформації і кібербезпеки за узагальненим (фактичним) показником $E^{Ф}$ (табл. 5).

ISSN 2663 - 4023

Таблиця 5.

Критерії оцінювання показників $E^{Ф}$

Критерій $E^{Ф}$	Рівень впровадження заходів з захисту інформації і кібербезпеки на ІКС	
$0 \le E^{Ф} \le 0{,}25$	Частковий	незадовільний (НЗ)
$0{,}25 < E^{Ф} \le 0{,}5$	Ризикорієнтований	низький (Н)
$0{,}5 < E^{Ф} \le 0{,}75$	Повторюваний	середній (С)
$0{,}75 < E^{Ф} \le 1$	Адаптивний	високий (В)

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі подано рішення науково-практичної задачі з обґрунтування окремих показників оцінювання здатності (ефективності) функціонування системи захисту інформації і кібербезпеки ІКС за результатами аналізу щорічних звітів інцидентів кібербезпеки. Обрані показники оцінювання здатності функціонування системи захисту інформації і кібербезпеки ІКС відповідають обраним специфічним вимогами. На відміну від показників, що рекомендовані у стандартах країн партнерів обрані в роботі забезпечують врахування національної особливості в оцінювання здатності функціонування системи захисту інформації і кібербезпеки інформації ІКС. Таким чином, запропоноване рішення науково-практичної задачі є істотним вкладом в забезпечення національної безпеки і оборони України, особливого значення набувши в умовах повномасштабної військової агресії Російської Федерації проти України [10].

Наукова новизна одержаного результату. Вперше запропоновано окремі показники оцінювання здатності (ефективності) функціонування системи захисту інформації і кібербезпеки інформації в ІКС спеціального зв’язку.

Перспективи подальших досліджень у даному напрямку. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні результати, що одержані в процесі наукового пошуку, становлять підґрунтя для подальшого обґрунтування методики оцінювання здатності (ефективності) функціонування системи захисту інформації і кібербезпеки інформації в ІКС спеціального зв’язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Петренко, А. (2016). *План дій щодо впровадження оборонної реформи у 2016-2020 роках (дорожня карта оборонної реформи)*. ДВПСП та МС МО України.

2 Кудінов, В.А. (2011). Оцінка ефективності комплексної системи захисту інформації в системі оперативного інформування МВС України. *Науково-практичний журнал. Сучасна спеціальна техніка, 1*(24), 91-96.

3 Журавель, М.Ю., Полозова, Т.В., Стороженко, О.В. (2011). Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки транспорту і промисловості*, (33), 171-177.

4 Козубцова, Л.М., Рудоміно-Дусятська, І.А. Сновида В.Є. (2021). Обчислення показників ефективності функціонування системи захисту інформації і кібербезпеки. *Науковий журнал «Комп'ютерно-інтегровані технології: освіта, наука, виробництво», 45*, 19-25.

5 Козубцова, Л.М., Хлапонин, Ю.І., Козубцов, І.М. (2021). Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури організацій. *Сучасні інформаційні технології у сфері безпеки та оборони*, *2*(41), 17-22.

6 *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (2018). National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.04162018.

7 *National Online Informative References Program | CSRC*. (2021). NIST Computer Security Resource

Center | CSRC. https://csrc.nist.gov/projects/olir.

8 *Security and Privacy Controls for Federal Information Systems and Organizations*. (2013). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-53r4.

9 Наказ командира військової частини А0106 від 10.02.2021 №83/нагп «Про затвердження Класифікації інцидентів кібербезпеки та порушень захисту інформації в інформаційно-телекомунікаційних системах, системах спеціального зв'язку ЗС України».

10 Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації, Рішення Ради національної безпеки і оборони України (2017) (Україна). https://zakon.rada.gov.ua/laws/show/n0015525-16#Text.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023

Igor M. Kozubtsov
doctor of Pedagogical Sciences, candidate of technical sciences, senior researcher,
Leading Research Fellow of the Research Department of Cyber Security in Information and Telecommunication Systems Research Research (Information Protection Problems)
Scientific Center for communications and informatization of the Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0002-7309-4365
kozubtsov@gmail.com

Oleksandr O. Chernonoh
State expert of the cybersecurity expert group
Directorate of digital transformation and information security policy in the field of Defense, Ministry of defense of Ukraine, Kiev, Ukraine
ORCID ID 0000-0002-3667-8994
skgzua@gmail.com.

Lesya M. Kozubtsova
candidate of technical sciences, associate professor of the Department of mathematics and physics
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID 0000-0002-7866-8575
l.kozubtsova@i.ua

Mykhailo V. Artemchuk
Senior Lecturer, Department of Cyber Security, Faculty of Combat Application of Control and Communication Systems,
Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0003-4640-9429
mavrt@i.ua

Ivan H. Neshcheret
Leading Research Fellow of the Research Department of Cyber Security in Information and Telecommunication Systems Research Research (Information Protection Problems)
Scientific Center for communications and informatization of the Military Institute of telecommunications and informatization named after Heroes of Krut, Kiev, Ukraine
ORCID ID 0000-0002-3500-5683
aslam@ukr.net

SELECTION OF INDIVIDUAL INDICATORS FOR ASSESSING THE ABILITY OF THE INFORMATION SECURITY AND CYBERSECURITY SYSTEM TO FUNCTION IN SPECIAL COMMUNICATION INFORMATION AND COMMUNICATION SYSTEMS

Abstract. The subject of research in the scientific article is the system of Information Protection and cybersecurity in information and communication systems of special communication. The purpose of the article is to substantiate proposals for the selection of individual indicators for assessing the ability of the information security and cybersecurity system to function in Special Communication Information and communication systems in partial performance indicators. To achieve the goal and task, a set of interrelated theoretical research methods was used: analysis and generalization of scientific literature; structural and genetic analysis, when clarifying the object and subject of research; analytical and comparative analysis when evaluating the novelty of research results; synthesis and generalization-to justify indicators; generalization – to formulate conclusions and recommendations. Research results and conclusions. The result of the study was a reasonable solution of a new scientific and practical task to substantiate the performance indicators of the information security and cybersecurity system based on the results of the analysis of annual reports of cybersecurity incidents. The proposed solution significantly contributes to ensuring the national security and defense of Ukraine. Scientific novelty of the result obtained. For the first time, separate indicators for assessing the ability (effectiveness) of the functioning of the information security and cybersecurity system in Special Communication Information and communication systems are

proposed. Prospects for further research in this area. The presented study does not exhaust all aspects of this problem. The theoretical results obtained in the course of scientific research form the basis for further substantiation of the methodology for assessing the ability (effectiveness) of the functioning of the information security system and cybersecurity of information in information and communication systems of special communication.

Keywords: cyber incident; indicator; ability; efficiency; functioning; information security and cybersecurity system; requirements; generalized; information and communication system

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Petrenko, A. (2016). Plan dii shchodo vprovadzhennia oboronnoi reformy u 2016-2020 rokakh (dorozhnia karta oboronnoi reformy). DVPSP ta MS MO Ukrainy.

2 Kudinov, V.A. (2011). Otsinka efektyvnosti kompleksnoi systemy zakhystu informatsii v systemi operatyvnoho informuvannia MVS Ukrainy. Naukovo-praktychnyi zhurnal. Suchasna spetsialna tekhnika, 1(24), 91-96.

3 Zhuravel, M.Iu., Polozova, T.V., Storozhenko, O.V. (2011). Formuvannia systemy pokaznykiv otsinky rivnia informatsiinoi bezpeky pidpryiemstva. Visnyk ekonomiky transportu i promyslovosti, (33), 171-177.

4 Kozubtsova, L.M., Rudomino-Dusiatska, I.A. Snovyda V.Ie. (2021). Obchyslennia pokaznykiv efektyvnosti funktsionuvannia systemy zakhystu informatsii i kiberbezpeky. Naukovyi zhurnal «Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo», 45, 19-25.

5 Kozubtsova, L.M., Khlaponyn, Yu.I., Kozubtsov, I.M. (2021). Metodyka otsiniuvannia efektyvnosti vykonannia zakhodiv zabezpechennia kiberbezpeky obiektiv krytychnoi informatsiinoi infrastruktury orhanizatsii. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 2(41), 17-22.

6 Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018). National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.04162018.

7 National Online Informative References Program | CSRC. (2021). NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/projects/olir.

8 Security and Privacy Controls for Federal Information Systems and Organizations. (2013). National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-53r4.

9 Nakaz komandyra viiskovoi chastyny A0106 vid 10.02.2021 №83/nahp «Pro zatverdzhennia Klasyfikatsii intsydentiv kiberbezpeky ta porushen zakhystu informatsii v informatsiino-telekomunikatsiinykh systemakh, systemakh spetsialnoho zviazku ZS Ukrainy».

10 Pro zahrozy kiberbezpetsi derzhavy ta nevidkladni zakhody z yikh neitralizatsii, Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy (2017) (Ukraina). https://zakon.rada.gov.ua/laws/show/n0015525-16#Text.