МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ

DOI: https://doi.org/10.26565/1684-8489-2022-1-02
УДК 006.013

Євген Олександрович Живило,
кандидат наук з державного управління,
докторант кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
м. Харків, Україна

e-mail: zhivilka@i.ua *https://orcid.org/0000-0003-4077-7853*

СИТУАЦІЙНИЙ ЦЕНТР МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ – МОДЕЛЬ ЗАВЧАСНОГО ВИЯВЛЕННЯ ТА АНАЛІЗУ КРИЗОВИХ СИТУАЦІЙ СЕКТОРУ БЕЗПЕКИ ДЕРЖАВИ

Анотація. Досліджено проблематику створення та забезпечення функціонування ситуаційного центру в системі Міністерства оборони України. Доведено необхідність створення спеціалізованої організаційної структури, одним із основних завдань якої визначено реагування на кіберзагрози воєнного характеру безпосередньо за загальною координацією Національного координаційного центру кібербезпеки у взаємодії з іншими суб'єктами забезпечення кібербезпеки держави.

Проаналізовано шляхи створення та функціонування ситуаційного центру, визначено перелік загроз за якими повинно здійснюватись реагування, як окремої структури (або його окремих елементів), так і спільного виконання визначених положенням завдань з Ситуаційним центром Збройних Сил України під час реагування Збройними Силами України на кризові (надзвичайні) ситуації в кіберпросторі України.

В умовах постійної мілітаризації кіберпростору національного сегменту Радою національної безпеки і оборони України прийнято рішення, щодо розширення та подальший розвиток єдиної мережі ситуаційних центрів та оснащення їх уніфікованим програмним та апаратним забезпеченням, що дозволить підвищити ефективність ухвалення рішень на всіх рівнях управління державою. Причиною такого зростання є саме кризові явища, які стають довготривалими, а процеси управління перетворюються з "попередження кризи" на, переважно, "ліквідацію кризи".

За цих умов постає доволі суттєва проблема, щодо питань взаємодії мережі ситуаційних центрів не тільки сфери національної безпеки і оборони, а також й ситуаційних центрів органів державної влади (резервних, на рухомій базі) на одній платформі в режимі реального часу.

Як цитувати: *Живило Є. О.* Ситуаційний центр Міністерства оборони України – модель завчасного виявлення та аналізу кризових ситуацій сектору безпеки держави. *Актуальні проблеми державного управління*. 2022. № 1 (60). С. 27–41. DOI: https://doi.org/10.26565/1684-8489-2022-1-02.

In cites: *Zhyvylo Y. O.* (2022). Situation Center of the Ministry of Defense of Ukraine – a model of early detection and analysis of crisis situations in the state security sector. *Pressing Problems of Public Administration, 1(60), 27–41.* DOI: https://doi.org/10.26565/1684-8489-2022-1-02 [in Ukrainian].

У цій ситуації, задля досягнення оперативної сумісності є вкрай важливим систематизувати однотипність в використанні спеціального програмного забезпечення та програмно-апаратних комплексів для забезпечення інтероперабельності, стійкого і безперервного функціонування, тестування, конфігурації та відстеження продуктивності у прийнятті рішень і контролю їх виконання.

Вочевидь, що у процесі розширення та нарощування потужностей мережі ситуаційних центрів. Державна служба спеціального зв'язку та захисту інформації України відіграватиме одну з ключових ролей. Стає зрозумілим, що такі центри, повинні бути об'єднані в єдину захищену мережу, з наданням можливості оперативно збирати інформацію, аналізувати її та приймати критично важливі для держави рішення.

Ключові слова: кіберзагрози, кібербезпека, ситуаційний центр, кіберпростір, спеціальне програмне забезпечення, ІТ-системи, критична інфраструктура, електронні комунікації.

Постановка проблеми. Проблема обґрунтування та вибору правильних управлінських рішень в органах державної влади особливої актуальності набуває у період загроз що існують для України, із захисту її суверенітету, територіальної цілісності й недоторканності [1].

Саме тому для керівників як вищих державних органів, так і місцевих органів управління критично важливою є наявність технологічного й інституційного середовища, яке б сприяло якісному аналізу інформації та оперативному прийняттю ефективних державних рішень, особливо у кризових ситуаціях [2].

В Україні триває формування дієвої єдиної мережі ситуаційних центрів (СЦ), так Міністерство оборони України (МО України) не є виключенням. Передбачається розгортання СЦ органів державної влади (резервних, на рухомій базі) на одній ІТ – платформі в режимі реального часу.

Діючі та сплановані до розгортання СЦ в своїй діяльності використовують спеціальне програмне забезпечення (СПЗ) з інформаційно-аналітичного супроводження, моніторингу, прогнозування, прийняття рішень, проведення аудиту, безпеки. Зазначені процеси повинні відбуватись в одному цифровому середовищі, надійно захищеному від зовнішнього несанкціонованого втручання та кібератак.

Тому усвідомлення необхідності створення відповідної організаційної структури у складі СЦ МО України є одним з основних завдань. Функціоналом цієї структури передбачено реагування на кіберзагрози та реалізація сталої технічної підтримки функціонування програмно-апаратного комплексу (платформи).

Як результат, інтеграція зусиль щодо організації вищезазначених завдань потребує глибоких подальших досліджень.

Аналіз останніх досліджень і публікацій. Проблематика пов'язана зі створення системи СЦ доволі змістовно досліджена в працях О. Гудими, О. Капштика,В. Карпенка, В. Легомінова, В. Пристайка, А. Семенченка тощо.

Дослідженню механізмів прийняття управлінських рішень, у т. ч. в умовах криз у державному управлінні, приділяли увагу В. Бакуменко, А. Васильєв, Ю. Гладун, М. Дніпренко, О. Карпенко, Р. Марутян, О. Орлов, Н. Подвірна, О. Труш та ін.

Серед дослідників організації всебічно обґрунтованих оцінок кіберзагрозу сучасному безпековому середовищі, в інтересах підготовки держави до оборони слід відзначити Є. Бабич, Ю. Даник, Д. Дубов, С. Кірсанов, О. Пермяков, А. Сбітнєв, О. Суходоля, В. Телелим, та ін. Однак актуальність та проблематика теми статті потребують подальшого дослідження у даній сфері.

Досвід країн світу показує, що використання СЦ в системах кризового реагування набирає масового характеру. Одним із факторів, які впливають на результати роботи СЦ є стан інформаційного забезпечення.

В умовах динамічності при прийнятті державних рішень та реагуванні на кризові ситуації в межах мережі СЦ держави і в Головному СЦ виникає нагальна потреба залучення всіх існуючих інформаційних ресурсів держави [3].

У МО України та ЗС України налічується близько 20 інформаційно-аналітичних систем, які використовуються або проходять дослідну експлуатацію [4; 5], при цьому кількість зазначених систем має сталий показник на збільшення.

Враховуючи первинні джерела наукової інформації та інші матеріали і прогнози, доволі впевнено можливо стверджувати, що інформаційні ресурси держави знаходяться під впливом реальних та потенційних кіберзагроз.

Тому забезпечення стійкого і безперервного функціонування інформаційно-аналітичних систем СЦ МО України, їх тестування на вразливості, зміна конфігурації, залежно від вимог які виникають, відстеження продуктивності, згідно з визначеним регламентом, набуває важливого значення.

Поряд з цим, представники ІТ-структур єдиної мережі СЦ України намагаються знайти та впровадити системний підхід до застосування хмарних технологій при вирішенні задач організації доступу до розподілених інформаційних ресурсів, розробки уніфікованого програмного забезпечення щодо забезпечення побудови та супроводження динамічних реєстрів електронних інформаційних ресурсів в національному сегменті кіберпростору.

Мета статті. Отже, наукове обґрунтування створення організаційної структури у складі СЦ МО України із завданнями реагування кіберзагрози, які виникають в інформаційно-аналітичних системах, впровадження нових систем та інформаційних технологій, об'єднання та використання на одній платформі існуючих розрізнених інформаційних систем та технічної підтримки функціонування програмно-апаратного комплексу (платформи) набирає критичного характеру і є доволі виваженим.

Виклад основного матеріалу. Подолання напруженої воєнно-політичної ситуації, в умовах якої наша держава відстоює власну цілісність та суверенітет, вимагає подальшого вдосконалення системи організації СЦ як ефективного механізму стратегічних комунікацій з урахуванням досвіду провідних держав [8].

Сьогодні в умовах стрімкого збільшення ролі інформації і знань в житті суспільства, зростання інформатизації та ваги інформаційних технологій у суспільних та господарських відносинах, розвиток глобального інформаційного простору та, як наслідок – обмеженість у часі щодо оперативного прийняття рішення управлінцями є доволі обґрунтованими чинниками реформування різних сфер суспільного життя та самої системи державного управління в цілому.

Зважаючи на військово-політичні реалії в Україні, МО України зацікавлено у трансформації ЗС України, інших складових сектору безпеки та оборони держави щодо набуття спроможностей для ефективних дій в умовах виникнення кризових ситуацій.

Так, на виконання Директиви Головнокомандувача Збройних Сил України у 2021 р. було створено та розгорнуто Ситуаційний центр Збройних Сил України, структура якого приведена на рисунку 1, розроблена система ситуаційного управління ЗС України, структура якого змінюється, залежно від виникаючих завдань (загроз), один із розроблених варіантів подано на рисунку 2. Триває робота щодо створення системи СЦ ЗС України [1].

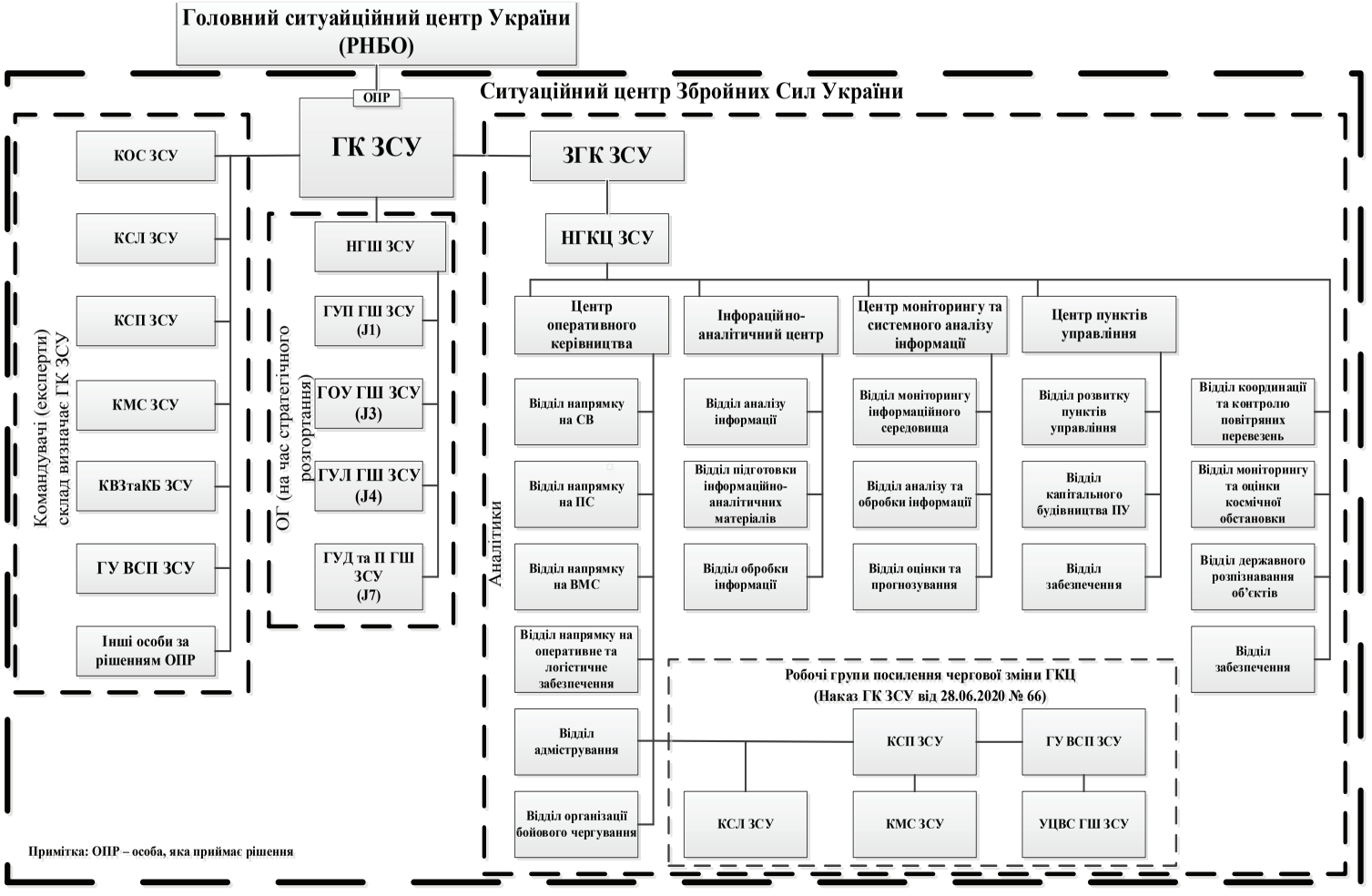

Рис. 1. Структура ситуаційного центру Збройних Сил України
Fig. 1. Structure of the Situation Center of the Armed Forces of Ukraine

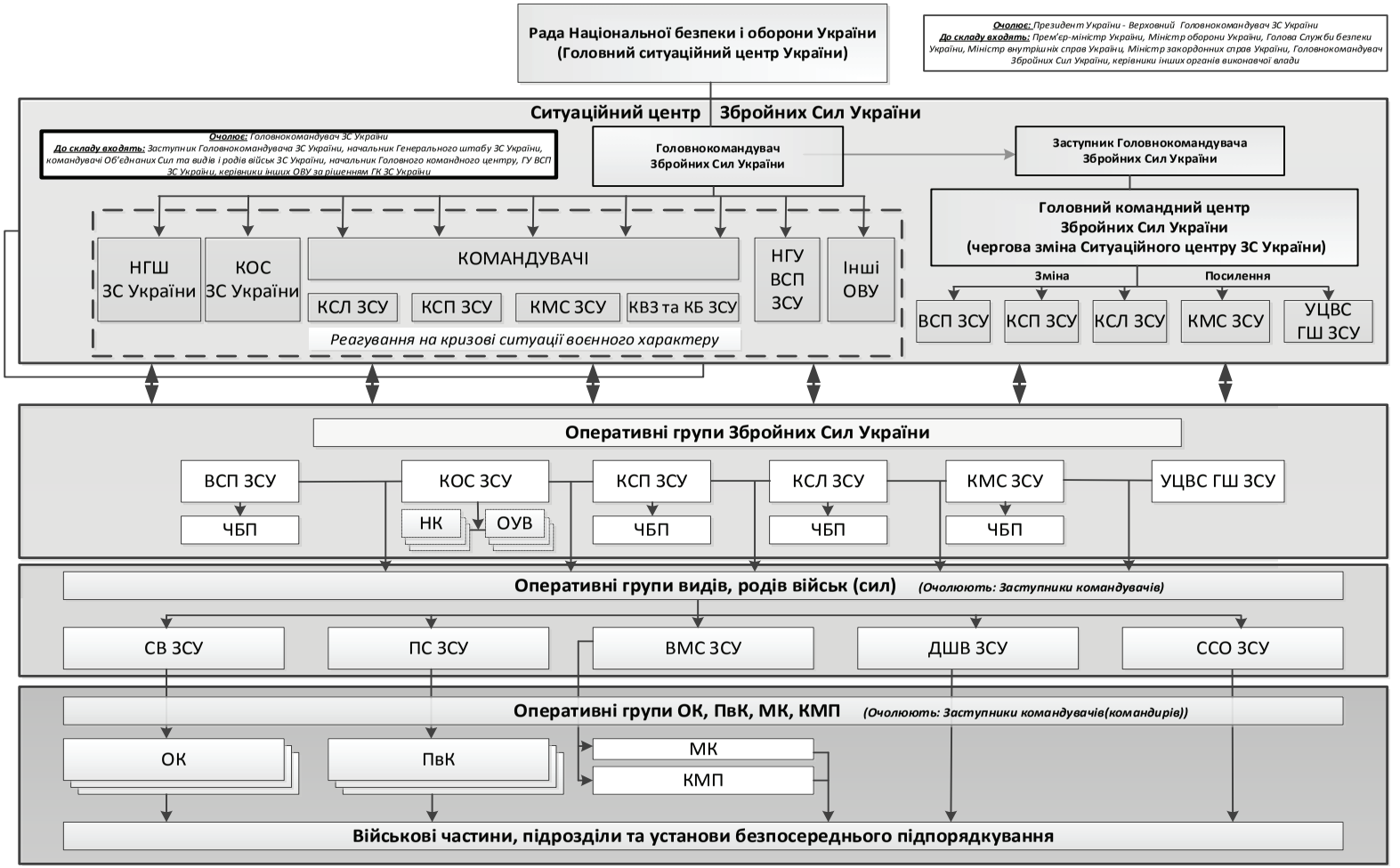

Рис. 2. Варіант структури ситуаційного центру Збройних Сил України
Fig. 2. Variant of the structure of the situational center of the Armed Forces of Ukraine

МО України також активізувало діяльність щодо створення та забезпечення функціонування СЦ в системі МО України. Цю роботу наростили, відповідно до рішення Ради національної безпеки і оборони України від 4 червня 2021 р. "Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони", введеного в дію Указом Президента України від 18 червня 2021 р. № 260/2021 [7], Положення про Міністерство оборони України, затвердженого постановою Кабінету Міністрів України від 26 листопада 2014 р. № 671 (у редакції постанови Кабінету Міністрів України від 19 жовтня 2016 р. № 730). Так, відповідно до цього нормативно-правового поля, Наказом Міністерства оборони України № 396 від 23 грудня 2021 р. було утворено робочу групу з питань створення та забезпечення функціонування СЦ в системі МО України [10].

Документом передбачається підготовка пропозицій та інформаційних матеріалів щодо:

– шляхів створення СЦ в системі МО України;

– всебічно обґрунтованих оцінок загроз (визначення їх переліку), за якими повинно відбуватися реагування з розгортанням СЦ в системі МО України;

– прогнозів виникнення та розвитку кризових ситуацій, підготовку проєктів управлінських рішень, рекомендацій щодо заходів протидії негативним впливам в інтересах оборони;

– можливостей спільного реагування з СЦ ЗС України на визначений перелік загроз;

– оцінки перспективи спільного функціонування в мережі СЦ в умовах цифрової трансформації сфери національної безпеки і оборони;

– розроблення проекту Положення про СЦ в системі МО України;

– можливостей розгортання резервного СЦ та СЦ на рухомій базі;

– оснащення СЦ уніфікованим (з Головним СЦ, Урядовим СЦ, СЦ державних органів та пунктами управління ЗС України) програмним та апаратним забезпеченням із інформаційно-аналітичного супроводження прийняття управлінських рішень.

Слід зауважити, що зазначеним документом та розробленим проектом положення про Управління забезпечення реагування на кризові ситуації (безпосередньо відповідального за стале функціонування СЦ в системі МО України), відповідно до визначених повноважень та завдань не передбачається визначення особи та/або підрозділу, відповідальних за стан захисту інформації (забезпечення інформаційної безпеки) та кіберзахисту СЦ.

При цьому, відповідно до розробленої спеціалізованої організаційної структури, та на виконання [6; 11; 12], передбачено реалізувати наступні заходи, а саме:

– визначення переліку інформаційних, програмних та апаратних ресурсів програмно-апаратного комплексу, рівень їх критичності для структури та/або її функціонування, можливий рівень наслідків у випадку порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) інформаційних систем (мережі), порушення функціонування його компонентів;

– визначення політики управління ризиками кібернетичної та інформаційної безпеки і методики їх оцінювання та оброблення;

– проведення обстеження платформи з метою оновлення даних щодо функціонування програмно-апаратного комплексу, технологічних процесів

обробки інформації яка ним опрацьовується, визначення переліку критичних інформаційних ресурсів та компонентів комплексу, які підлягають кіберзахисту, тощо;

– здійснення перегляду переліку загроз на інформаційно-розрахункові ресурси, ризиків інформаційної безпеки та рівня прийнятного ризику у разі, якщо за результатами обстеження виявлено, зміни в технології обробки інформації, впроваджено нові програмні або апаратні компоненти, змінено перелік критичних інформаційних ресурсів та компонентів платформи, які підлягають захисту, тощо;

– розроблення/оновлення технічного завдання на створення комплексної системи захисту інформаційних ресурсів та інформації на об'єктах інформаційної діяльності, іншої документації та впровадження оновлених вимог у разі виявлення нових загроз та/або ризиків;

– відпрацювання та оновлення технічної, проектної та іншої документації на комплексну систему захисту інформації ІТС (в захищеній від модифікації електронній та/або паперовій формі) з обов'язковим описом реалізованих в ІТС організаційних та технічних заходів безпеки інформації;

– визначення порядку розмежування, надання, зміни та скасування прав доступу користувачів та адміністраторів до служб (функцій), інформації та компонентів платформи, здійснення контролю (аудиту) використання прав доступу ними;

– формування, надання, скасування та контроль (аудит) за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних, для доступу до служб (функцій), інформації та компонентів ІТС;

– забезпечення безперебійної роботи ІТ – платформи в режимі реального часу, зокрема здійснення резервування даних та її компонентів, зберігання резервних копій даних, відновлення даних з резервних копій та заміни складових платформи у випадку виходу їх з ладу, тощо.

Отже, враховуючи зазначене вище, вважається за необхідне розглянути інциденти кібербезпеки, існуючі загрози та їх модифікації порушення захисту інформації які носять вірогідний та імовірний характер впливу на стале функціонування СЦ в системі МО України. Їх можливо класифікувати за категоріями та ступенем небезпеки. При цьому кіберінциденти, що потребують реагування у разі їх виявлення, поділяються на категорії. Категорія кіберінциденту визначає причину, через яку приймається рішення про необхідність реагування на інцидент кібербезпеки.

Для кожної категорії кіберінцидентів визначений цифровий код, назва українською та англійською мовами, а також пріоритет.

Категорії інцидентів кібербезпеки в ІТС СЦ в системі МО України та ЗС України подано в таблиці 1.

Інцидент, який може бути віднесений до декількох категорій, реєструється (обліковується) як інцидент категорії, що має вищий пріоритет. Опис інцидентів кібербезпеки в ІТС СЦ в системі МО України та ЗС України наведено в таблиці 2.

Кіберінциденти логічно поділити за ступенем небезпеки, який визначається категорією кіберінцидента і об'єктом, на якому кіберінцидент було зафіксовано (об'єктом, на який здійснюється кібервплив).

Таблиця 1
Категорії інцидентів кібербезпеки в ІТС СЦ в системі МО України та ЗС України
Table 1
Categories of cyber security incidents in ITS SC in the system of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine

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

Таблиця 2
Опис інцидентів кібербезпеки в ІТС СЦ в системі МО України та ЗС України
Table 2
Description of cyber security incidents in the ITS of the SC in the system of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine

№ з/п	Опис інциденту кібербезпеки	Назва категорії кіберінциденту (код)
1	2	3
1	Компрометація облікового запису системи (сервісу), в т. ч. у результаті крадіжки паролю зловмисником	Вторгнення зловмисника до системи (5)
2	Компрометація системи, в т. ч. у результаті експлуатації вразливості або роботи ШПЗ, що дозволяє віддалене керування	Вторгнення зловмисника до системи (5)
3	Несанкціоноване підключення пристрою до інформаційно-телекомунікаційної системи, в т. ч. цифрової радіостанції до системи цифрового радіозв'язку	Вторгнення зловмисника до системи (5)
4	Порушення порядку доступу до інформації в системі (в т. ч. у результаті експлуатації вразливості або роботи ШПЗ)	Загроза конфіденційності та/або цілісності інформації (7)
5	Відмова в обслуговуванні або порушення сталого функціонування сервісу (об'єкта ІТС) у результаті DoS-, DDoS-атаки, помилкових, дій користувачів, відключення електричної енергії, тощо	Загроза доступності інформації (6)
6	Виявлення шкідливого програмного засобу, що не дозволяє віддалене керування та не несе загрози цілісності і конфіденційності та/або доступності інформації	Шкідливий програмний засіб (2)
7	Виявлення спроб використання зловмисником вразливостей програмного забезпечення, невдалих спроб автентифікації в системі, в т. ч. у системі цифрового радіозв'язку	Спроби зловмисника щодо вторгнення до системи (4)
8	Розсилання зловмисником повідомлень з метою крадіжки пароля користувача	Махінації (8)
9	Несанкціонований доступ до ресурсів системи шляхом використання прав об'єкта (несанкціоноване використання NAT, підміна MAC-адреси)	Махінації (8)

1	2	3
10	Передача захищеного паролем архіву під час обміну відкритою інформацією в АСУ ЗС України “Дніпро”	Махінації (8)
11	Несанкціоноване використання програмного забезпечення, що втручається в роботу комплексу засобів захисту	Махінації (8)
12	Порушення порядку використання ресурсів (використання не за призначенням, у несанкціонованих цілях), в т. ч. обробка інформації в АС без створення КСЗІ з підтвердженою відповідністю, обробка інформації з обмеженим доступом в АС, що призначена для обробки відкритої інформації, передача інформації з обмеженим доступом у мережі Інтернет, в автоматизованій системі управління Збройних Сил України “Дніпро”, по відкритих телефонних мережах	Махінації (8)
13	Відсутність критичного оновлення безпеки програмного забезпечення (прошивки телекомунікаційного обладнання)	Наявність, відомих вразливостей (9)
14	Функціонування АРМ або сервера з порушенням вимог інструкції з організації антивірусного захисту в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України	Наявність відомих вразливостей (9)
15	Порушення порядку підключення автоматизованої системи до мережі Інтернет	Наявність відомих вразливостей (9)
16	Порушення встановлених правил розмежування доступу, в т. ч. використання пароля (SNMP community, ключа шифрування системи цифрового радіозв’язку) понад встановлений термін або такого, що не відповідає визначеним вимогам безпеки	Наявність відомих вразливостей (9)
17	Використання свідомо уразливого протоколу, режиму роботи, налаштувань обладнання або програмного забезпечення при передачі паролів, іншої чутливої інформації	Наявність відомих вразливостей (9)
18	Несанкціоноване використання програмного забезпечення, що збільшує ризик порушення безпеки інформації, в т. ч. отриманого з недостовірних джерел	Наявність відомих вразливостей (9)
19	Помилкові дії або бездіяльність користувача, що призводять до збільшення ризику порушення безпеки інформації цифрових систем радіозв’язку, а саме: робота передавача на випромінювання в період радіомовчання, робота радіозасобів без радіоданих під час переміщення пунктів управління (вузлів зв’язку), спотворення форми сигналу на виході передавача	Наявність відомих вразливостей (9)
20	Збирання інформації зловмисником про користувача, склад інформаційно-телекомунікаційної системи, існуючі вразливості, в т. ч. нетехнічними засобами	Збір інформації зловмисником (3)
21	Масове розсилання небажаної кореспонденції (SPAM)	Зловмисна інформація (1)
22	Виявлення у відкритому доступі інформації, яка здатна зашкодити інтересам МО України та Збройних Сил України	Зловмисна інформація (1)
23	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 ІТС ЗС України	Інше (10)

Об’єкти ІТС ЗС України за їх вкладом в функціонування ІТС ЗС України належать до однієї з трьох категорій критичності:

І категорія критичності (ключові елементи ІТС ЗС України) – це елементи транспортної мережі та сервери, що забезпечують роботу сервісів;

ІІ категорія критичності – кінцеві пристрої (АРМ, IP телефон і т. ін.), що забезпечують роботу чергових змін структурних елементів СЦ в системі МО України та ЗС України, посадових осіб оперативно-чергової та чергової служб;

ІІІ категорія критичності – інші елементи ІТС ЗС України.

Ступінь небезпеки кіберінциденту визначає термін виконання заходів щодо реагування на інцидент кібербезпеки з моменту його виявлення. Ступені небезпеки кіберінцидентів в ІТС СЦ МО України та ЗС України наведено в таблиці 3.

Таблиця 3

Ступені небезпеки кіберінцидентів в ІТС СЦ МО України та ЗС України

Table 3

Degrees of danger of cyber incidents in the ITS Center of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine

Ступінь небезпеки інциденту кібербезпеки	Визначення	Граничні терміни заходів реагування		
		Підтвердження (Acceptance)	Стримування (Containment)	Відновлення (Recovery)
Надзвичайний (код - чорний)	Інцидент, що становить безпосередню загрозу життю чи здоров'ю людей або призводить до фізичного пошкодження (виведення з ладу) об'єкта І категорії критичності	30 хвилин	1 година	8 годин
Критичний (код - червоний)	Інцидент, що становить безпосередню загрозу функціонуванню і безповоротності роботи об'єкта І категорії критичності та/або можливості надання ним основних послуг	1 година	3 години	8 годин (у робочі дні)
Високий (код - помаранчевий)	Інцидент, що свідчить про наявність передумов порушення функціонування і безперервності роботи об'єкта І категорії критичності. Інцидент, що становить безпосередню загрозу функціонуванню і безповоротності роботи об'єкта ІІ категорії критичності та/або можливості надання ним основних послуг	1 година (у робочі дні)	5 годин (у робочі дні)	1 доба (у робочі дні)
Середній (код - жовтий)	Інцидент, що має ознаки підготовки кібернетичного впливу вищого ступеня небезпеки на об'єкті І категорії критичності. Інцидент, що свідчить про наявність передумов порушення функціонування і безперервності роботи об'єкта ІІ категорії критичності. Інцидент, що становить безпосередню загрозу функціонуванню і безповоротності роботи об'єкта ІІІ категорії критичності та/або можливості надання ним основних послуг	2 години (у робочі дні)	8 годин (у робочі дні)	3 доби (у робочі дні)
Низький (код - зелений)	Інцидент, що має ознаки підготовки кібернетичного впливу вищого ступеня небезпеки на об'єкті ІІ категорії критичності. Інцидент, що свідчить про наявність передумов порушення функціонування і безперервності роботи об'єкта ІІІ категорії критичності	8 годин (у робочі дні)	2 доби (у робочі дні)	5 діб (у робочі дні)
Інформаційний (код - білий)	Подія, явища і чинники, що потребують додаткового дослідження, та, за сумісністю ознак, можуть у подальшому бути віднесені до інцидентів кібербезпеки в ІТС	-	-	-

Класифікацію кіберінцидентів в ІТС СЦ МО України та ЗС України за категоріями та ступенем небезпеки наведено в таблиці 4.

Таблиця 4

Класифікацію кіберінцидентів в ІТС СЦ МО України та ЗС України за категоріями та ступенем небезпеки

Table 4

Classification of cyber incidents in the ITS Center of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine by categories and degree of danger

Пріоритет	Код	Назва категорії інциденту кібербезпеки в ІТС ЗС України	Життя та здоров'я людей, апаратна частина об'єктів ІТС ЗС України	Об'єкти ІТС ЗС України, І категорії критичності	Об'єкти ІТС ЗС України, ІІ категорії критичності	Об'єкти ІТС ЗС України, ІІІ категорії критичності
1	5	Вторгнення зловмисника до системи (Intrusion)	код - чорний	код - червоний	код - помаранчевий	код - жовтий
2	7	Загроза конфіденційності та/або цілісності інформації (Information Content Security)	код - чорний	код - червоний	код - помаранчевий	код - жовтий
3	6	Загроза доступності інформації (Availability)	код - чорний	код - червоний	код - помаранчевий	код - жовтий
4	2	Шкідливий програмний засіб (MaliciousCode)	код - чорний	код - помаранчевий	код - жовтий	код - зелений
5	4	Спроби зловмисника щодо вторгнення до системи (Intrusion Attempts)	код - чорний	код - помаранчевий	код - жовтий	код - зелений
6	8	Махінації (Fraud)	код - чорний	код - помаранчевий	код - жовтий	код - зелений
7	9	Наявність відомих вразливостей (Vulnerability)	код - чорний	код - помаранчевий	код - жовтий	код - зелений
8	3	Збір інформації зловмисником (Information Content)	-	код - жовтий	код - зелений	код - зелений
9	1	Зловмисна інформація (Abusive Content)	-	код - жовтий	код - зелений	код - зелений
10	10	Інше (Other)	-	-	-	-

Отже, наукове обґрунтування створення організаційної структури у складі СЦ МО України із завданнями реагування на кіберзагрози, що виникають в інформаційно-аналітичних системах, впровадження нових систем та інформаційних технологій, об'єднання та використання на одній платформі існуючих розрізнених інформаційних систем та технічної підтримки функціонування програмно-апаратного комплексу (платформи) набирає критичного характеру і є доволі виваженим.

Враховуючи зазначене, необхідно зробити наголос на необхідності створення та введенні у штатний розпис організаційної структури у складі СЦ МО України з завданнями реагування на виникаючі кіберзагрози.

Формування та розвиток у складі СЦ МО України необхідних військових організаційних структур для дій у кіберпросторі, їх комплектування, підготовка та всебічне забезпечення дозволить:

– визначити завдання для ЗС України у частині здійснення оборони кіберпростору (участі у заходах з кібероборони держави);

– визначити основні функції та повноваження МО України та ЗС України у керівництві заходами з кібероборони України та кібервійськами;

– забезпечити оперативними інформаційно-аналітичними матеріалами в ході застосування упершій хвилі відсічі і стримування збройної агресії проти України кібервійськ з проведенням дій (операцій) у кіберпросторі та стримуванні подальшої ескалації воєнного конфлікту [14];

– забезпечити підтримання спроможностей сил системи МО України та ЗС України щодо завдання противнику у кіберпросторі політичних, економічних, воєнних та інших втрат, з огляду на це, він буде змушений відмовитися від ескалації збройної агресії проти України;

– надати стратегічну мобільність у веденні асиметричних, мережецентричних, багатосферних і непрямих дій у кіберпросторі, які нівелюватимуть чисельну та технологічну перевагу противника в інформаційному просторі та кіберпросторі [13];

– створити комплексну систему захисту інформації та кібербезпеки в ІТС СЦ МО України та ЗС України в інтересах зміцнення безпекового середовища держави;

– проводити розробку та тестування технічних рішень за експертної підтримки держав-членів НАТО та партнерів в ІТС СЦ МО України та ЗС України;

– практично залучити фахівців (спеціалістів) з кібербезпеки до участі у навчаннях НАТО з кібербезпеки, багатонаціональних навчаннях Cyber Flag, Locked Shields, Cyber Coalition, Crossed Swords;

– здійснити державно-приватне партнерство у сфері кібероборони, в т. ч. залучення висококваліфікованих цивільних фахівців приватних структур, ресурсів ІТ-компаній до виконання завдань з кібероборони держави в умовах постійного деструктивного кібервпливу.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Зважаючи на змістовне викладення матеріалу, враховуючи визначені пріоритети державної політики у сферах національної безпеки і оборони зі створення та функціонування системи СЦ ЗС України та СЦ МО України, доведено необхідність створення спеціалізованої організаційної структури в системі МО України з завданнями реагування на виникаючі кіберзагрози воєнного характеру безпосередньо за загальною координацією Національного координаційного центру кібербезпеки у взаємодії з іншими суб'єктами забезпечення кібербезпеки держави [9].

Функціонування зазначеної військової організаційної структури дозволить виконувати заходи, щодо стримування, локалізації і відбиття воєнної агресії у кіберпросторі (кібероборони), ураження через кіберпростір об'єктів інформаційної інфраструктури противника, ведення кіберрозвідки, кіберпідтримки своїх військ (сил), участі у забезпеченні кібербезпеки України, виконання заходів з кіберзахисту інформаційної інфраструктури Міністерства оборони та Збройних Сил України, а також критичної інформаційної інфраструктури держави в умовах надзвичайного і воєнного стану.

У подальшому, інтегрування оперативних (бойових та спеціальних) спроможностей набутих СЦ МО України до мережі СЦ Сил оборони, Головного СЦ і розгалуженої мережі СЦ держави дозволить об'єднати інформаційно-аналітичні системи СЦ, впровадити нові системи та інформаційні технології з подальшим застосуванням їх на одній платформі в рамках функціонування єдиного програмно-апаратного комплексу (платформи).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Живило Є. О. Формування та запровадження ситуаційного управління сектором безпеки та оборони держави – основа ефективної системи державного управління. *Публічне управління XXI століття: погляд у майбутнє* : збірник тез XXI Міжнародного наукового конгресу. Харків : Вид-во ХарРІ НАДУ "Магістр", 2021. URL: %D0%A1%D0%B8%D1%82%D1%83%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9%20%D1%86%D0%B5%D1%82%D1%80_%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F/zbirnik_kongress_2021.pdf (дата звернення: 22.09.2022). DOI: https://doi.org/10.34213/mnkongr.2021.

2. Пристайко В. В. Ситуаційні центри як ключовий інституційний механізм державного антикризового управління: зарубіжний досвід. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Державне управління.* 2019. Том 30 (69). № 3. URL: %D0%A1%D0%B8%D1%82%D1%83%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9%20%D1%86%D0%B5%D1%82%D1%80_%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F/26.pdf (дата звернення: 26.09.2022). DOI: https://doi.org/10.32838/2663-6468/2019.3/24.

3. Семенченко А. І., Журавльов А. В., Карпенко О. В. та ін. Ситуативні центри органів державної влади. URL: //http://academy.gov.ua/NMKD/library_nadu/Nayk_rozrob/27e3c680-aac9-440b-b17b-00979f76d8a9.pdf (дата звернення: 22.08.2022).

4. Соколов К. О., Гудима О. П., Шиятий О. Б., Ткаченко В. А. Основні напрями створення ІТ-інфраструктури Міністерства оборони України. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ.* Київ, 2015. № 3 (55). С. 26–30.

5. Соколов К. О., Гудима О. П., Шиятий О. Б., Миронюк А. Б. Застосування інформаційних технологій у інформаційно-аналітичному забезпеченні органів військового управління. *Наука і техніка Повітряних Сил ЗС України. Військові та технічні науки.* Харків, 2015. № 3 (20). С. 30–32.

6. Відомості про виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. *Офіційний вісник України.* 2019. № 50. ст. 1697.

7. Зеленський увів у дію рішення РНБО щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери нацбезпеки. URL: //https://ua.interfax.com.ua/news/general/751001.html (дата звернення: 22.08.2022).

8. Про створення Ситуаційного центру Збройних Сил України : Директива Головнокомандувача Збройних Сил України від 19.10.2020 р. № Д-8.

9. Про рішення Ради національної безпеки і оборони України від 27.01.2016 р. "Про Стратегію кібербезпеки України" : Указ Президента України від 15.03.2016 р. № 96/2016 URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 22.08.2022).

10. В Міноборони України буде створено ситуаційний центр. URL: https://opk.com.ua/%D0%B2-%D0%BC%D1%96%D0%BD%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D0%B1%D1%83%D0%B4%D0%B5-%D1%81%D1%82%D0%B2%D0%BE%D1%80%D0%B5%D0%BD%D0%BE-%D1%81%D0%B8/ (дата звернення: 22.08.2022).

11. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету міністрів України від 19.06.2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 22.09.2022).

12. Технічні вимоги на створення спеціалізованого програмного забезпечення "Державний реєстр об'єктів критичної інформаційної інфраструктури". *Департамент кіберзахисту Адміністрації Держспецзв'язку*. Київ, 2021, 31 с.

13. Всеохоплююча оборона України: стан, проблеми та заходи щодо зміцнення кібероборони держави і створення кібервійськ. URL: https://opk.com.ua/%D0%B2%D1%81%D0%B5%D0%BE%D1%85%D0%BE%D0%BF%D0%BB%D1%8E%D1%8E%D1%87%D0%B0-%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B0-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D1%81%D1%82%D0%B0%D0%BD-%D0%BF%D1%80/ (дата звернення: 22.08.2022).

14. Про рішення Ради національної безпеки і оборони України від 20.08.2021 р. "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 17.09.2021 р. № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 22.08.2022).

Стаття надійшла до редакції 23.08.2022 р.
Стаття рекомендована до друку 23.09.2022 р.

Y. O. Zhyvylo,
PhD in Public Administration,
Postdoctoral fellow of the Public policy Department,
Education and Research Institute of Public Administration
of V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
e-mail: zhivilka@i.ua *https://orcid.org/0000-0003-4077-7853*

SITUATION CENTER OF THE MINISTRY OF DEFENSE OF UKRAINE – A MODEL OF EARLY DETECTION AND ANALYSIS OF CRISIS SITUATIONS IN THE STATE SECURITY SECTOR

Annotation. The article examines the issue of creating and ensuring the functioning of the situation center in the system of the Ministry of Defense of Ukraine. The necessity of creating a specialized organizational structure, one of the main tasks of which is to respond to military cyber threats directly under the general coordination of the National Coordination Center for Cyber Security in cooperation with other actors in the field of cyber security.

The ways of creation and functioning of the situation center are analyzed, the list of threats to which the separate structure (or its separate elements) and joint performance of the tasks defined by the provisions with the Situational Center of the Armed Forces of Ukraine during the Armed Forces respond to the crisis situations in the cyberspace of Ukraine.

In the context of constant militarization of cyberspace of the national segment, the National Security and Defense Council of Ukraine decided to expand and further develop a single network of situation centers and equip them with unified software and hardware that will increase decision-making efficiency at all levels of government. The reason for this growth is precisely the crisis phenomena, which become long-lasting, and management processes are transformed from "crisis prevention" to, mainly, "crisis management".

Under these conditions, there is a significant problem with the interaction of the network of situational centers not only in the field of national security and defense, but also situational centers of public authorities (reserve, mobile) on one platform in real time.

In this situation, in order to achieve interoperability, it is extremely important to systematize uniformity in the use of special software and software and hardware to ensure interoperability, stable and continuous operation, testing, configuration and performance monitoring in decision making and monitoring.

It is obvious that the State Service for Special Communications and Information Protection of Ukraine will play one of the key roles in the process of expanding and increasing the capacity of the network of situational centers. It is becoming clear that such centers should be integrated into a single secure network, with the ability to quickly collect information, analyze it and make critical decisions for the state.

Keywords: cyber threats, cybersecurity, situation center, cyberspace, special software, IT-systems, critical infrastructure, electronic communications.

REFERENCES

1. Zhyvylo, Ye.O. (2021). Formuvannia ta zaprovadzhennia sytuatsiinoho upravlinnia sektorom bezpeky ta oborony derzhavy – osnova efektyvnoi systemy derzhavnoho upravlinnia. *Publichne upravlinnia KhKhI stolittia: pohliad u maibutnie zbirnyk tez XKhI mizhnarodnoho naukovoho konhresu*. Kharkiv: Vydavnytstvo KharRI KharRI NADU "Mahistr". URL: %D0%A1%D0%B8%D1%82%D1%83%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9%20%D1%86%D0%B5%D1%82%D1%80_%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F/zbirnik_kongress_2021.pdf (data zvernennia: 22.08.2022). DOI: https://doi.org/10.34213/mnkongr.2021 [in Ukrainian].

2. Prystaiko, V.V. (2019). Sytuatsiini tsentry yak kliuchovyi instytutsiinyi mekhanizm derzhavnoho antykryzovoho upravlinnia: zarubizhnyi dosvid. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Derzhavne upravlinnia, tom 30 (69), no. 3.* URL: %D0%A1%D0%B8%D1%82%D1%83%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%B9%20%D1%86%D0%B5%D1%82%D1%80_%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%8F/26.pdf (data zvernennia: 22.08.2022). DOI: https://doi.org/10.32838/2663-6468/2019.3/24 [in Ukrainian].

3. Semenchenko, A.I., Zhuravlov, A.V., Karpenko, O.V. and others. Sytuatyvni tsentry orhaniv derzhavnoi vlady. URL: //http://academy.gov.ua/NMKD/library_nadu/Nayk_rozrob/27e3c680-aac9-440b-b17b-00979f76d8a9.pdf (data zvernennia: 22.08.2022) [in Ukrainian].

4. Sokolov, K.O., Hudyma, O.P., Shyiatyi, O.B., Tkachenko, V.A. (2015). Osnovni napriamy stvorennia IT-infrastruktury Ministerstva oborony Ukrainy. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU, no. 3 (55), 26–30*. Kyiv [in Ukrainian].

5. Sokolov, K.O., Hudyma, O.P., Shyiatyi, O.B., Myroniuk, A.B. (2015). Zastosuvannia informatsiinykh tekhnolohii u informatsiino-analitychnomu zabezpechenni orhanivviiskovoho upravlinnia*. Nauka i tekhnika Povitrianykh Syl ZS Ukrainy. Viiskovita tekhnichni nauky, no. 3 (20), 30–32*. Kharkiv [in Ukrainian].

6. Vidomosti pro vykonannia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury: Postanova Kabinetu Ministriv Ukrainy vid 19.06.2019 r. № 518. (2019). *Ofitsiinyi visnyk Ukrainy, no. 50, st. 1697*.

7. Zelenskyi uviv u diiu rishennia RNBO shchodo udoskonalennia merezhi sytuatsiinykh tsentriv ta tsyfrovoi transformatsii sfery natsbezpeky. URL: //https://ua.interfax.com.ua/news/general/751001.html (data zvernennia: 22.08.2022).

8. Pro stvorennia Sytuatsiinoho tsentru Zbroinykh Syl Ukrainy: Dyrektyva Holovnokomanduvacha Zbroinykh Syl Ukrainy vid 19.10.2020 r. No. D-8.

9. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27.01.2016 r. "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 15.03.2016 r. No. 96/2016. (2016). URL: https://www.president.gov.ua/documents/962016-19836 (data zvernennia: 22.08.2022).

10. V Minoborony Ukrainy bude stvoreno sytuatsiinyi tsentr. URL: https://opk.com.ua/%D0%B2-%D0%BC%D1%96%D0%BD%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B8-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D0%B1%D1%83%D0%B4%D0%B5-%D1%81%D1%82%D0%B2%D0%BE%D1%80%D0%B5%D0%BD%D0%BE-%D1%81%D0%B8/ (data zvernennia: 22.08.2022).

11. Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury: Postanova Kabinetu ministriv Ukrainy vid 19.06.2019 r. No. 518. (2019). URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (data zvernennia: 22.08.2022).

12. Tekhnichni vymohy na stvorennia spetsializovanoho prohramnoho zabezpechennia "Derzhavnyi reiestr obiektiv krytychnoi informatsiinoi infrastruktury". (2021). *Departament kiberzakhystu Administratsii Derzhspetszviazku*. Kyiv.

13. Vseokhopliuiucha oborona Ukrainy: stan, problemy ta zakhody shchodo zmitsnennia kiberoborony derzhavy i stvorennia kiberviisk. URL: https://opk.com.ua/%D0%B2%D1%81%D0%B5%D0%BE%D1%85%D0%BE%D0%BF%D0%BB%D1%8E%D1%8E%D1%87%D0%B0-%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D0%B0-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8-%D1%81%D1%82%D0%B0%D0%BD-%D0%BF%D1%80/ (data zvernennia: 22.08.2022).

14. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20.08.2021 r. "Pro Stratehichnyi oboronnyi biuleten Ukrainy": Ukaz Prezydenta Ukrainy vid 17.09.2021 r. No. 473/2021. (2021). URL: https://www.president.gov.ua/documents/4732021-40121 (data zvernennia: 22.08.2022).

The article was received by the editors 23.08.2022.
The article is recommended for printing 23.09.2022.