УДК 004.77

к.н.держ.упр. **Живило Є.О.** (ВІТІ)
Злобін К.В. (ВІТІ)
Кузь В.С. (ВІТІ)

DOI: http://doi.org/10.17721/2519-481X/2023/80-12

ВИМОГИ З КІБЕРЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА СЕРВІСІВ ЗВ'ЯЗКУ ПІД ЧАС ЇХ РОЗГОРТАННЯ ТА ЕКСПЛУАТАЦІЇ НА ПУНКТАХ УПРАВЛІННЯ СКЛАДОВИХ СИЛ ОБОРОНИ ТА БЕЗПЕКИ

Актуальність данної роботи обумовлена тим, що за останні роки війська зв'язку постійно розвивались та оснащувались новітніми цифровими засобами зв'язку, що дозволяє їм успішно виконувати завдання за призначенням. Сьогодні інформаційно-комунікаційні системи які розгорнуті на пунктах управління різних ланок управління забезпечують виконання пріоритетних завдань з управління військами. Функціонально, система зв'язку та інформаційні системи розгорнуті на пунктах управління, як єдине інформаційно-комунікаційне середовище на основі впровадження новітніх інформаційно-комунікаційних технологій, протоколів обміну інформацією, комплексів, систем та засобів зв'язку, що забезпечує обмін усіма видами інформації між органами військового управління (органами управління) та пунктами управління на всіх ланках управління. Діюча система зв'язку забезпечує обмін інформацією із гарантованою захищеністю в єдиному інформаційному просторі як сукупність матеріальних функцій (в тому числі персоналу та інших ресурсів), що об'єднуються для виконання певного завдання.

В свою чергу інформаційні системи, як сукупність обладнання, методів та процедур, і, в разі необхідності, персоналу, організованого для виконання функцій обробки інформації діють у відповідності до визначеної структури, а саме:

- сервіси, в контексті зв'язку та інформаційні системи;
- архітектура, в контексті зв'язку та інформаційні системи;
- функції, в контексті сервіс-орієнтованої архітектури;
- взаємосумісність;
- захист інформації та кіберзахист.

Зрозуміло, що чим важливіший об'єкт управління, тим більш ємкісний потік інформації може бути спрямований на нього. Зазначене дозволяє противнику/зловмиснуку визначити найбільш важливі цілі і спрямувати на них інші види інформації або придушити їх різними способами. Так, в інтересах забезпечення кіберзахисту електронних інформаційних ресурсів, комунікаційних і технологічних систем пунктів управління Збройних Сил України розгорнута і функціонує технологічна інфраструктура кіберзахисту Збройних Сил України, яка є складовою єдиної системи захисту інформації та кіберзахисту в інформаційно-комунікаційних системах Міністерства оборони і Збройних Сил України. В цих умовах, для вирішення завдань з унеможливлення небажаних втручань, порушення сталого функціонування інформаційно-комунікаційного середовища на пунктах управління, противаги в здобутті конфіденційної інформації, викрадення даних та інше розгортаються мінімально необхідні компоненти інфраструктури кіберзахисту. Основними компонентами відповідної технологічної інфраструктури кіберзахисту є система управління подіями інформаційної безпеки (Security Information Event Management, SIEM), платформа обміну інформацією про загрози (Malware Information Sharing Platform & Threat Sharing, MISP), система централізованого управління міжмережевими екранами та система виявлення і протидії кіберзагрозам, у тому числі комп'ютерним вірусам, на кінцевому обладнанні.

Тому, вирішення завдань з забезпечення кіберзахисту в ході розгортання та експлуатації електронних комунікаційних мереж та сервісів зв'язку на пунктах управління різних ланок управління виявляється доволі серйозним та актуальним завданням.

Ключові слова: пункт управління, інформаційно-комунікаційне середовище, кіберпростір, кіберзагроза, кібербезпека, кібероборона.

Вступ. Питання кібербезпеки (КБ) в Збройних Силах України (ЗС України), а особливо в зоні проведення військових дій, сьогодні майже не висвітлюється. При цьому відомо, що деструктивному впливу піддається не тільки електронно-комунікаційна система, а і особовий

склад який залучений до виконання бойових завдань [1]. Новітні засоби розвідки дають змогу дізнатися не лише про місце, з якого ведуться переговори, а й безпосередньо про зміст переговорів та листування. І головною проблемою в цьому питанні, на жаль, є не розробка та доопрацювання десятків інструкцій та керівництв, а недостатня обізнаність особового складу, щодо налаштування політик безпеки особистих мобільних пристроїв та озброєння-військової техніки зв'язку.

Сьогодні більшість тих, хто залучений до складу Сил оборони та безпеки (СО), включаючи рядовий і офіцерський склад, не усвідомлюють про наявність кіберзагроз та потенційно можливі негативні наслідки, які можуть створити небезпеку життєво важливим інтересам громадянам, особам, суспільству і державі. В цих умовах, важливо забезпечити цілісність і конфіденційність інформації під час виконання бойових завдань, перебуваючи **в районах зосередження, бойового злагодження, пунктах управління** (ПУ), **пунктах постійної дислокації. Визнавати відповідальність за проведення переговорів службового характеру з використанням персональних мобільних пристроїв та електронних** комунікаційних мереж. Нажаль військовослужбовці не в змозі самостійно забезпечити безпечне налагодження та експлуатацію тих чи інших додатків/застосунків, програмного забезпечення (ПЗ), набору інструментів, технологій і даних від несанкціонованого доступу.

Інформація – це найважливіший актив, а стабільне функціонування системи зв'язку і комунікаційних систем (СЗКС) та послуг має важливе значення для належного управління системою консультацій, командування і управління (С3). Складові СО і союзники покладаються на використання СЗКС для ефективного обміну інформацією та ефективного функціонування. Така побудова СЗКС (CIS) потребує ряду принципів, які дозволять отримувати переваги технологій, а також розібратися з пов'язаними ризиками і складнощами виконання операцій з інформаційним перевантаженням [2].

Врахування принципів зв'язку та інформаційних систем (en: Communication and Information Systems Principles) дозволить СО спільно використовувати інформацію в рамках єдиного інформаційного простору. Зазначене надає право командирам та штабам всіх рівнів отримати значні переваги під час планування та ведення операцій (бойових дій), покращити ситуаційну обізнаність, управління військами (силами) та зброєю. Такий підхід дозволить СО отримувати переваги з використання та впровадження інформаційних технологій (ІТ).

За цих умов постає доволі суттєва проблема, щодо забезпечення доступності, цілісності, конфіденційності та КБ до інформації яка циркулює в інформаційно-комунікаційних систем (ІКС) ПУ органів військового управління (ОВУ). Особливо це стосується систем і мереж, які використовуються суб'єктами СО для управління особливо важливою інформацією. Виконання вимог з: надійності і безпеки відповідних сервісів зв'язку, виявлення та протидії зловмисній діяльності, доступності, цілісності та безпеки інформації які включають елементи фізичної безпеки (наприклад, безпеку персоналу та документів) і ЗІ є ключовими елементами безпеки в СЗКС [3]. Також, доволі суттєвим питанням є виконання заходів з забезпечення безпеки зв'язку і комп'ютерної безпеки, управління службами СЗКС у відповідь на зловмисні дії, вчинені в кіберпросторі. У той же час, інформація повинна бути захищена до належного рівня, гарантуючи доступність до достовірної інформації авторизованим користувачам і унеможливить доступ до достовірної інформації неавторизованих осіб.

Отже, розробка базових вимог з кіберзахисту ІКС та сервісів зв'язку під час їх розгортання та експлуатації на ПУ складових СО є вкрай важливим. Їх запровадження та виконання оперативним складом ПУ різних ланок управління забезпечить сталу експлуатацію захищених інформаційно-телекомунікаційних послуг (сервісів) на ПУ, ефективну технічну підтримку базових і функціональних служб, а також ІТ для обробки даних та їх відображення в системі управління військами, функціональну взаємодію та сумісництво СЗКС на ПУ складових СО.

Аналіз останніх досліджень. Аналіз існуючої нормативно-правовової бази щодо створення та функціонування системи КБ та кібероборони в ІКС спеціальних користувачів

свідчить про те, що Національна система КБ, одним із трьох завдань якої є кіберзахист державного інформаційного ресурсу**,** створюється і розвивається відповідно до Конституції України, законів України та інших нормативно-правових актів, що регулюють суспільні відносини у сфері національної безпеки, оборони, інформаційної та КБ і захисту інформації. Виходячи з цього, системи кіберзахисту в ІКС спеціальних користувачів також створюються та функціонують відповідно до вимог законів та нормативно-правових актів України, а саме:

Законів України: "Про національну безпеку України" [4]; "Про основні засади забезпечення кібербезпеки України" [5]; "Про захист інформації в інформаційно-телекомунікаційних системах" [6]; "Про розвідку" [7]; "Про Національну програму інформатизації" [8]; "Про ратифікацію Конвенції про кіберзлочинність" [9]; "Про Державну службу спеціального зв'язку та захисту інформації України" [10]; "Про державну таємницю" [11]; "Про доступ до публічної інформації" [12]; "Про захист персональних даних" [13]; "Про оборону України" [14]; "Про інформацію" [15]; "Про Збройні Сили України" [16].

Документів довгострокового та оборонного планування України: Стратегія національної безпеки України [17]; Стратегія кібербезпеки України [18]; Стратегія воєнної безпеки України [19]; Стратегічний оборонний бюлетень України [20]; Питання Апарату Ради національної безпеки і оборони України, Про Національний координаційний центр кібербезпеки [21]; Стратегія інформаційної безпеки України [22].

Нормативних документів міжнародних організацій, згода на використання яких надана Верховною Радою України. Зокрема, рекомендації Міжнародного союзу електрозв'язку (ITU), міжнародні стандарти з інформаційної безпеки ISO/IEC 27000, стандарти (рекомендації) Національного інституту стандартів і технологій США – NIST та стандартів та специфікацій національного інституту стандартів (ANSI).

Нормативно-правових актів Міністерства оборони України (Далі – МО України) та ЗС України, більшість з яких має обмеження доступу, видаються відповідно до вимог законів України, підзаконних актів державних органів, уповноважених у сферах електронних комунікацій, інформатизації, захисту інформації тощо, частина з яких також не є відкритою інформацією відповідно до вимог законів України [5, 6, 10].

Мета статті. Вирішення завдань забезпечення кіберзахисту електронних комунікаційних мереж та сталого функціонування сервісів зв'язку на пунктах управління різних ланок управління є вкрай актуальним, а формулювання та реалізація відповідних технічних вимог є ключовим елементом для складових сил оборони та безпеки в умовах сьогодення.

Виклад основного матеріалу. Формування та розвиток нової моделі системи зв'язку та інформаційних систем СО України здійснюється у відповідності з кращими практиками ключових іноземних партнерів, передусім Європейського Союзу, Сполучених Штатів Америки та інших держав-членів НАТО, на основі національних інтересів України.

Стратегічні принципи зв'язку та інформаційних систем (en: CIS strategic principles) СО (визначені відповідно до документу Ради штабу НАТО з консультацій, командування та управління AC/322-D (2018) 0020. Alliance C3 Strategy – Part 1, 27 April 2018.) включають [23]:

– спільне використання інформації в рамках єдиного інформаційного простору із запровадженням та супроводженням реєстру інформаційних ресурсів, електронних баз даних інформації та інформаційного менеджменту;

– забезпечення безперешкодного обміну інформацією між стаціонарними СЗКС та польовими мережами зв'язку;

– функціонування інформації в мережевому захищеному середовищі балансуючи між принципами "обов'язок щодо розповсюдження" (en: "duty to share") та "потреби в інформації" (en: "need to know");

– масштабованість СЗКС та їх сервісів (здатність динамічно адаптуватись до змін вимог), гнучкість (здатність адаптуватись до змін умов обстановки яка склалась), захищеність (здатність забезпечити політики безпеки в існуючому середовищі ризиків) та стійкість (здатність до відновлення системи після вразливості "нульового дня");

– забезпеченість СЗКС відповідними сервісами згідно методології DOTMLPFI;

Примітка. 6 DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, and Interoperability) – напрями розвитку оборонних потенціалів (Доктринальна база (D), Організація (O), Підготовка (T), Ресурсне забезпечення (M), Персонал (P), Якість управління та освіта (L), Військова інфраструктура (F), Взаємосумісність (I)), які є складовою процесу оборонного планування НАТО (en: NATO Defense Planning Process) [2].

– опис та забезпеченість спроможностей СЗКС, як сервісів, сервіс-орієнтовану архітектуру та запровадження підходів до їх життєвого циклу;

– підтримку обміну інформацією з обмеженням доступу будь-якого рівня та всіх функціональних сервісів, притаманних окремим структурним підрозділам ОВУ;

– відкритість, модульність та гнучкість для повторного використання, динамічність до розвитку і взаємосумісності та здатність до інтеграції в існуючі та майбутні спроможності архітектур СЗКС;

– відповідність пріоритету розвитку спроможностей парадигмі "ABC" (Adopt, Buy, Create) (тобто, модернізація наявного, далі – закупівля готових ресурсів, і, як крайня міра – створення нового або їх комбінація);

– заснування дисципліни з корпоративної архітектури;

– адекватну захищеність проти всіх категорій загроз, у т.ч. тих, що випливають із кіберпростору, зв'язку та інформаційних систем, їх сервісів та електронних систем;

– підтримку колективних заходів з кіберзахисту (кібероборони) всіх складових СО; запровадження практик ITIL (Бібліотека інфраструктури IT (en: Information Technology Infrastructure Library, ITIL).

Об'єднана ІКС СО повинна використовувати гнучкі та адаптовані набори нематеріальних (політика безпеки, визначені процеси і процедури, стандартизація інформаційного циклу) та матеріальних (стаціонарна та польова мережі, сервіси та підтримуючі інфраструктури зі зв'язку) засобів, якими забезпечуються складові СО. Розгортання об'єднаної ІКС СО зі створенням єдиного інформаційного простору повинно відповідати таким принципам:

– цінова ефективність від використання;

– можливості максимального повторного використання;

– відповідність принципам єдиного інформаційного простору;

– урахування С3-таксономії;

– поетапний підхід;

– використання уніфікованих мережевих стандартів та рішень;

– підтримка угруповань СО, склад яких динамічно змінюється;

– інформаційна орієнтованість мережі.

Об'єднання систем зв'язку та інформаційних систем в ІКС складових СО повинно здійснюватись за допомогою визначених рівнів взаємосумісності, а саме ізольована, поєднана, функціональна, доменів та корпоративна. При цьому взаємосумісності систем звязку та інформаційних систем не є абсолютною умовою. Оговорюючи об'єднану ІКС СО, вважається за необхідне розглянути інциденти КБ, існуючі загрози та їх модифікації порушення захисту інформації які носять вірогідний та імовірний характер впливу на стале функціонування ПУ різних ланок управління СО та безпеки. 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 КБ [24].

Для кожної категорії кіберінцидентів визначений цифровий код, назва українською та англійською мовами, а також пріоритет. Категорії інцидентів КБ на ПУ різних ланок управління СО та безпеки подано в таблиці 1.

Таблиця 1

Категорії інцидентів КБ на ПУ різних ланок управління СО та безпеки

од	**Пріоритет**	**Назва категорії інциденту КБ в ІКС**
	9	Зловмисна інформація (Abusive content)
	4	Шкідливий програмний засіб (Malicious Code)
	8	Збір інформації зловмисником (Information Gathering)
	5	Спроба зловмисника щодо вторгнення до системи (Intrusion Attempts)
	1	Вторгнення зловмисника до системи (Intrusion)
	3	Загроза доступності інформації (Availability)
	2	Загроза конфіденційності та/або цілісностіінформації (lnformation Content Security)
	6	Махінації (Fraud)
	7	Наявність відомих вразливостей (Vulnerability)
0	10	Інше (Other)

Інцидент, який може бути віднесений до декількох категорій, реєструється (обліковується) як інцидент категорії, яка має вищий пріоритет. Опис інцидентів КБ в ІКМ ПУ різних ланок управління СО та безпеки наведено в таблиці 2.

Таблиця 2

Опис інцидентів КБ в ІКМ ПУ різних ланок управління СО та безпеки

	Опис інциденту КБ	**Назва категорії кіберінциденту (код)**
	2	3
	Компрометація облікового запису системи (сервісу), в тому числі в результаті крадіжки паролю зловмисником	Вторгнення зловмисника до системи (5)
	Компрометація системи, в тому числі в результаті експлуатації вразливості або роботи шкідливого програмного забезпечення, що дозволяє віддалене керування	Вторгнення зловмисника до системи (5)
	Несанкціоноване підключення пристрою до ІКС, в тому числі цифрової радіостанції до системи цифрового радіозв’язку	Вторгнення зловмисника до системи (5)
	Порушення порядку доступу до інформації в системі (в тому числі в результаті експлуатації вразливості або роботи шкідливого програмного забезпечення)	Загроза конфіденційності та/або цілісності інформації(7)

	Опис інциденту КБ	Назва категорії кіберінциденту (код)
	Відмова в обслуговуванні або порушення сталого функціонування сервісу (об'єкта ІКС) в результаті DoS-, DDoS-атаки, помилкових, дій користувачів, відключення електричної енергії, тощо	Загроза доступності інформації(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)
	Виявлення спроб використання зловмисником вразливостей ПЗ, невдалих спроб автентифікації в системі, в тому числі в системі цифрового радіозв'язку	Спроби зловмисника щодо вторгнення до системи (4)
	Розсилання зловмисником повідомлень з метою крадіжки пароля користувача	Махінації (8)
	Несанкціонований доступ до ресурсів системи шляхом використання прав об'єкта (несанкціоноване використання NAT, підміна MAC-адреси)	Махінації (8)
0	Передача захищеного паролем архіву під час обміну відкритою інформацією в автоматизованій системі управління ЗС України "Дніпро"	Махінації (8)
1	Несанкціоноване використання ПЗ, що втручається в роботу комплексу засобів захисту	Махінації (8)
2	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, обробка інформації з обмеженим доступом в автоматизованій системі, що призначена для обробки відкритої інформації, передача інформації з обмеженим доступом в мережі Інтернет, в автоматизованій системі управління ЗС України "Дніпро", по відкритих телефонних мережах	Махінації (8)
3	Відсутність критичного оновлення безпеки ПЗ (прошивки телекомунікаційного обладнання)	Наявність, відомих вразливостей (9)
4	Функціонування автоматизованого робочого місця або сервера з порушенням вимог інструкції' з організації антивірусного захисту в СЗКС МО України та ЗС України	Наявність відомих вразливостей (9)
5	Порушення порядку підключення автоматизованої системи до мережі Інтернет	Наявність відомих вразливостей (9)
6	Порушення встановлених правил розмежування доступу, в тому числі 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)
7	Використання свідомо уразливого протоколу, режиму роботи, налаштувань обладнання або ПЗ при	Наявність відомих вразливостей (9)

	Опис інциденту КБ	Назва категорії кіберінциденту (код)
	передачі паролів, іншої чутливої інформації	
8	Несанкціоноване використання ПЗ, що збільшує ризик порушення безпеки інформації, в тому числі отриманого з недостовірних джерел	Наявність відомих вразливостей (9)
9	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 ПУ (вузлів зв'язку), спотворення форми сигналу на виході передавача	Наявність відомих вразливостей (9)
0	Збирання інформації зловмисником про користувача, склад ІКС, існуючі вразливості, в тому числі нетехнічними засобами	Збір інформації зловмисником (3)
1	Масове розсилання небажаної кореспонденції (SPAM)	Зловмисна інформація (1)
2	Виявлення у відкритому доступі інформації, що здатна зашкодити інтересам МО України та ЗС України	Зловмисна інформація (1)
3	Виявлення шкідливого програмного засобу, що відбулося одночасно з його блокуванням/видаленням наявним антивірусним ПЗ за умови знаходження джерела розповсюдження шкідливого програмного засобу за межами ІКС ЗС України	Інше (10)

Розглядаючи нормативно-правову базу на загальнодержавному рівні, необхідно зазначити, що правову основу забезпечення КБ України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" (Документ 2163-VIII) від 17.08.2022, Указу Президента України "Питання Головнокомандувача Збройних Сил України" від 27 березня 2020 року № 123/2020, вимог рішення Ради національної безпеки і оборони України від 14 травня 2021 р. "Про невідкладні заходи з кібероборони держави", введеного в дію Указом Президента України від 26 серпня 2021 р. № 446 та у відповідності до вимог схваленого на засіданні Кабінету Міністрів України Плану організації виконання рішення Ради національної безпеки і оборони України від 14 травня 2021 р. "Про невідкладні заходи з кібероборони держави", введеного в дію Указом Президента України від 26 серпня 2021 р. № 446 передбачено підтримання та нарощування спроможностей до застосування ЗС України, а також сил і засобів інших складових СО.

Як однією з похідних, розвитку та впровадження, зазначеної вище нормативно-правової бази, відбулась розробка та затвердження Міністром оборони України "Функціональних груп спроможностей Міністерства оборони України, Збройних Сил України та інших складових Сил оборони" від 26 листопада 2021 року. Паралельно з цим, робочою групою був розроблений "Єдиний перелік (каталог) спроможностей Міністерства оборони України, Збройних Сил України та інших складових Сил оборони", який було затверджено Міністром оборони України 31 грудня 2021 року. Так, Розділом 7. ЗВ'ЯЗОК ТА ІНФОРМАЦІЙНІ СИСТЕМИ (COMMUNICATION&INFORMATION SYSTEMS – CIS), на Командування військ зв'язку та кібернетичної безпеки ЗС України (2CIS-5.1) покладається

“Створення і забезпечення захищених інформаційно-телекомунікаційних послуг (сервісів) для ОВУ та розгортання ПУ на рухомій базі” – код спроможності 2CIS-5. Зазначений розділ переліку охоплює спроможності СО з організації (забезпечення) зв’язку та обміну інформацією в інформаційних системах.

Переліком визначено ряд базових вимог до носіїв спроможності, одним з яких є здатність створення і забезпечення захищених інформаційно-телекомунікаційних послуг (сервісів) для ОВУ та розгортання ПУ на рухомій базі у відповідності до матриці надання мінімально необхідних сервісів оперативному складу (службовим особам) ПУ оперативної (оперативно-тактичної, тактичної) ланок управління [25]. Встановлено, що організація розгортання, здійснення управління, забезпечення функціонування єдиної системи захисту інформації та кіберзахисту в ІКС МО України і ЗС України покладається на Генеральний штаб ЗС України. При цьому розгортання та забезпечення функціонування технологічної інфраструктури кіберзахисту ЗС України здійснюється силами військових частин та підрозділів захисту інформації та КБ Командування Військ зв’язку та КБ ЗС України [26]. Порядок організації доступу телекомунікаційних вузлів ПУ до мережі Інтернет та електронної комунікаційної мережі ЗС України визначається старшим ОВУ у відповідному бойовому розпорядженні (розпорядженні зі зв’язку). Транзит трафіку ЕКМ ЗС України між ІТВ ЗС України здійснюється виключно в зашифрованому вигляді згідно з вимогами законодавства у сфері технічного та криптографічного захисту інформації.

Для надання оперативному складу ПУ базових, функціональних сервісів, доступу до мережі Інтернет спеціалісти зв’язку телекомунікаційних вузлів розгортають локальні мережі різного призначення, вживають відповідних технічних та організаційних заходів для забезпечення їх цілісності, безперервності надання електронних комунікаційних послуг, недопущення несанкціонованого доступу до розгорнутих мереж. Різні за призначенням (умовами доступу до інформації, що обробляється) мережі відокремлюються одна від одної на фізичному (шляхом використання окремого обладнання для різних мереж) або на логічному (шляхом використання технології VLAN тощо) рівні. Налаштування локальних мереж для підключення кінцевого (термінального) обладнання, яке використовується без створення комплексної системи захисту інформації (особисті засоби електронних комунікацій оперативного складу ПУ тощо), повинно забезпечувати ізоляцію обладнання таких мереж одне від одного та від локальних мереж іншого призначення. Ізоляція може бути реалізована шляхом відокремлення портів комутаційного обладнання мережі (технологія Private VLAN), налаштуванням спеціального режиму роботи точок безпроводового доступу (Guest Network) тощо.

Під час розгортання локальних мереж має використовуватися обладнання, ПЗ (прошивка) яке ліцензійно підтримується виробником. Вкрай важливо передбачити своєчасне оновлення ПЗ (прошивки) обладнання в разі виявлення його критичної вразливості яке покладається на адміністратора мережі. Розгортання, модернізація, припинення експлуатації, згортання відповідних інформаційно-комунікаційних систем (мереж) ПУ вноситься адміністратором в SIEM. Обладнання ЕКМ розгортається таким чином, щоб фізичний доступ до нього був обмежений лише персоналом польових ТВ, в обов’язки якого входить експлуатація (обслуговування) зазначеного обладнання. Доступ адміністраторам до адміністрування обладнання ЕКМ повинен надаватися виключно з IP-адрес робочих станцій, які визначені для адміністрування ЕКМ. Рекомендовано розміщення робочих станцій адміністраторів в окремій локальній мережі (Management VLAN). Доступ до управління технічними засобами електронних комунікацій має надаватися користувачам та адміністраторам в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації. Використання для адміністрування технічних засобів електронних комунікацій незахищених протоколів передачі даних (HTTP, Telnet тощо) забороняється. При цьому паролі облікових записів користувачів та адміністраторів технічних засобів електронних комунікацій мають відповідати вимогам парольної політики у ЗС України.

Налаштування обладнання ЕКМ має забезпечувати реєстрацію та передачу в SIEM даних щонайменше про такі події: вхід користувачів та адміністраторів; невдалі спроби

входу користувачів та адміністраторів; зміна конфігураційних налаштувань. Налаштування обладнання, що служить для з'єднання локальної мережі з іншими мережами (маршрутизатор або міжмережевий екран), повинно забезпечувати політику пропуску трафіку та передачу даних про нього в SIEM з метою аналізу на предмет виявлення ознак кібератак.

Політика пропуску трафіку (правила фільтрації) визначає обмеження на пропуск трафіку між взаємоз'єднаними мережами на основі критеріїв дозволених та заборонених служб, протоколів, портів, станів взаємодії (statefulness), мережевих адрес, вебсайтів тощо. До проведення налаштування передачі даних про трафік у SIEM повинно забезпечуватись локальне зберігання зазначених даних не менше 30 діб та передача їх в електронному вигляді за запитом командира (заступника) військової (их) частин та підрозділів захисту інформації та КБ Командування Військ зв'язку та кібербезпеки ЗС України для аналізу.

Налаштування шлюзу між локальними мережами і мережею Інтернет має, крім того, забезпечувати автоматичне застосування встановлених правил обробки мережевого трафіку, у тому числі блокування кібератак у разі виявлення ознак відомих кіберзагроз.

Зазначені вимоги реалізуються міжмережевими екранами (ММЕ). У разі відсутності ММЕ, необхідно здійснити відповідні налаштування маршрутизаторів мережі. Оновлення даних про кіберзагрози в системі централізованого управління міжмережевими екранами забезпечується силами військових частин та підрозділів захисту інформації та КБ Командування Військ зв'язку та кібербезпеки ЗС України шляхом управління ліцензіями (підписками на джерела даних про кіберзагрози виробника ММЕ) та інтеграції з MISP. У разі якщо умови роботи ЕКМ не дозволяють проходження трафіку через міжмережеві екрани, то для виявлення кіберзагроз налаштовується передача на міжмережеві екрани копії трафіку (технологія Traffic Mirroring).

Для забезпечення належного функціонування ЕКМ необхідно створювати систему резервування копій конфігурацій обладнання ЕКМ та інформаційних ресурсів/даних об'єктів критичної інфрастуктури СЗКС СО. Передбачити оперативний доступ до ресурсів/даних зазначених систем, як на мобільних так і на стаціонарних резервних платформах, пунктах, центрах. Резервні копії повинні зберігатися у зашифрованому вигляді на окремих змінних (зовнішніх) носіях, віртуальних серверах або в зашифрованому вигляді на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України [27].

В рамках підготовки оперативного складу щодо коректного налаштування та підтримки політик ІБ та КБ, необхідно передбачити залучення їх до відповідних навчальних курсів з базових заходів КБ, що підтверджуються відповідними сертифікатами.

Оперативний склад ПУ експлуатує базові і функціональні сервіси, при цьому доступ до мережі Інтернет має виключно через кінцеве (термінальне) обладнання, підключене до локальних мереж ІТВ (польових ВЗ). Використання інших мереж електронних комунікацій, у тому числі операторів мобільного зв'язку, на ПУ забороняється.

У комунікаційних мережах ПУ необхідно забезпечити контроль доступу до сервісів обміну електронними поштовими повідомленнями. При цьому доступ до захищених сервісів домену mil.gov.ua надається оперативному складу ПУ без обмежень, а доступ до сервісів обміну електронними поштовими повідомленнями в інших доменах надається для окремих пристроїв у разі необхідності, про що вказується в заявці на підключення кінцевого обладнання структурного підрозділу з відповідним обгрунтуванням.

Доступ оперативному складу ПУ до локальних мереж має надаватись з використанням індивідуальних даних автентифікації (логін, пароль, сертифікат тощо) за протоколом контролю доступу і автентифікації IEEE 802.1x. У разі неможливості використання протоколу IEEE 802.1x пристроям оперативного складу ПУ при їх підключенні до локальних мереж мають видаватися незмінні (постійні) IP-адреси. У такому разі IP-адреса пристрою закріплюється за його MAC-адресою та видається за протоколом DHCP. Безпроводовий доступ до локальних мереж пристроям, MAC-адрес яких немає в переліку дозволених, має бути заблокований налаштуванням точок безпроводового доступу, комутаційного

обладнання тощо. Ведення обліку IP-адрес, виданих пристроям оперативного складу ПУ, покладається на ІТВ [28].

Пристрої електронних комунікацій (комп'ютери, мобільні комунікаційні пристрої тощо, у тому числі особисті), що підключаються до ЕКМ, мають відповідати таким вимогам:

– встановлена операційна система та ПЗ, які дозволено використовувати у ЗС України, повинно технічно підтримуватись виробником та мати відповідні ліцензії;

– оновлення ПЗ у разі виявлення його критичної вразливості (при цьому пристрої необхідно підключити до системи виявлення і протидії кіберзагрозам, у тому числі комп'ютерним вірусам);

– налаштування політик безпеки, виконання зазначеного заходу унеможливлює доступ до змінних (зовнішніх) пристроїв та носіїв інформації, ідентифікаторів яких немає в списку дозволених;

– користувачі та адміністратори повинні отримати доступ до пристроїв в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації.

Вимоги до автоматизованих робочих місць або інщих пристроїв, що підключаються до ІКС, визначаються комплексною системою захисту інформації (методикою розгортання) таких ІКС.

Оперативним складом ПУ мають створюватися (оновлюватися) резервні копії власних інформаційних ресурсів з періодичністю, достатньою для їх відновлення у разі пошкодження або знищення внаслідок кіберінцидентів та кібератак. Резервні копії повинні зберігатися на окремих змінних (зовнішніх) носіях, які не використовуються для перенесення інформації між автоматизованими робочими місцями та виконання інших завдань.

Отже, проведене дослідження дозволило сформулювати вимоги з кіберзахисту інформаційно-комунікаційних систем та сервісів зв'язку під час їх розгортання та експлуатації на ПУ складовими СО.

В науковій праці побудовано алгоритм базових дій з налаштування політики безпеки як на програмному так і на технічному рівні основного обладнання зв'язку яке розгортається на ПУ для оперативної роботи особового складу.

Наведені пропозиції забезпечать заходи безпеки на ПУ різних ланок управлінян з захисту інформаційно-телекомунікаційних та інших електронно-комунікаційних систем та інформації, яка зберігається, обробляється чи передається в цих системах із додержанням доступності, цілісності, автентифікації, конфіденційності та ідентифікації відправника/отримувача.

Висновки. Виходячи з викладеного, можливо зробити наступні висновки:

1. СО спільно використовують інформацію в рамках єдиного інформаційного простору із запровадженням та супроводженням реєстру інформаційних ресурсів, електронних баз даних інформації та інформаційного менеджменту.

2. Архітектура та масштабованість ІКС і їх сервісів на ПУ різних ланок управління розгортається та експлуатується відповідно до документу Ради штабу НАТО з консультацій, командування та управління AC/322-D (2018) 0020. Alliance C3 Strategy – Part 1, 27 April 2018.

3. Існує ряд кіберзагроз та їх модифікації спрямовані на порушення захисту інформації, що носять вірогідний та імовірний характер впливу на стале функціонування ПУ різних ланок управління СО.

4. В рамках наведених пропозицій є вкрай важливим реалізувати на ПУ СО вимоги, щодо кіберзахисту ІКС та сервісів зв'язку під час їх розгортання та експлуатації.

ЛІТЕРАТУРА*:*

1. Черниш Р.Ф., Ігнатюк М.В. Протидія деструктивному інформаційному впливу в Україні: правові та організаційні аспекти [Електронний ресурс] – Режим доступу: http://lsej.org.ua/1_2022/54.pdf.

2. Доктрина зв'язок та інформаційні системи, введена в дію Головнокомандувачем Збройних Сил України від 20 червня 2020 року, ВКП 6-00(01).01.

3. Живило Є.О., Черноног О.О. Стратегія кібероборони України // Збірник наукових праць ВІТІ № 4 – 2017 [Електронний ресурс] – Режим доступу: //http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Закон України "Про національну безпеку України" від 21.06.2018 р. № 2469-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

7. Закон України "Про розвідку" від17.09.2020 № 912-IX [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/912-20#Text.

8. Закон України "Про Національну програму інформатизації" від 04.02.1998 р. № 74/98-ВР // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text.

9. Закон України "Про ратифікацію Конвенції про кіберзлочинність" від 10.03.2006 р. № 2163-VIII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

10. Про Державну службу спеціального зв'язку та захисту інформації : Закон України від 23.02.2006 р. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

11. Закон України "Про державну таємницю"від 21 січня 1994 № 3855-XII(зі змінами) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

12. Закон України "Про доступ до публічної інформації" від 13 січня 2011 р. № 2939-VI. [Електронний ресурс] – Режим доступу : https://zakon.rada.gov.ua/laws/show/2939-17#Text.

13. Закон України "Про захист персональних даних" від 01.06.2010 р. № 2297-VI [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

14. Закон України "Про оборону України" від 06.12.1991 р. № 1932-XII // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

15. Закон України України "Про інформацію" № 2938-VI. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

16. Закон України "Про Збройні Сили України" від 6 грудня 1991 року № 1934-XII (зі змінами) // Законодавство України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/1934-12#Text.

17. Стратегія національної безпеки України, введена в дію Указом Президента України від 14 вересня 2020 року № 392/2020 Про рішення Ради національної безпеки і оборони України], від 14 вересня 2020 року Про Стратегію національної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/3922020-35037.

18. Стратегія кібербезпеки України, введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021, – Режим доступу https://www.president.gov.ua/documents/4472021-40013.

19. Стратегія воєнної безпеки України, введена в дію Указом Президента України від 25 березня 2021 року № 121/2021 Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року Про Стратегію воєнної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/1212021-37661.

20. Указ Президента України №473/2021 від 17 вересня 2021 року №473/2021 Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України" [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/4732021-40121.

21. Указ Президента України №27/2020 28 січня 2020 року Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/27/2020#Text.

22. Стратегія інформаційної безпеки України, введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року Про Стратегію інформаційної безпеки України [Електронний ресурс] – Режим доступу: https://www.president.gov.ua/documents/6852021-41069.

23. Живило Є.О. Сервіси зв'язку об'єднаної мережі за стандартами країн НАТО // Електронна бібліотека Нац. ун-т ім. Ю. Кондратюка, 82 с. – 2023. [Електронний ресурс] – Режим доступу: //http://lib.nupp.edu.ua/elcat/alog?tab=b961c4f53c15ad9d36d3fa0351b68eb0.

24. Живило Є.О. Ситуаційний центр Міністерства оборони України – модель завчасного виявлення та аналізу кризових ситуацій сектору безпеки держави // Збірник наукових праць ХНУ ім. В. Н. Каразіна №1 (60) – 2022 [Електронний ресурс] – Режим доступу: https://periodicals.karazin.ua/apdu/article/view/21125/19764.

25. Єдиний перелік (каталог) спроможностей Міністерства оборони України, Збройних Сил України та інших складових Сил оборони, затверджено Міністром оборони України 31 грудня 2021 року.

26. Лісаконов В. Багатошарові кібератаки Росії не знають меж, 2019 [Електронний ресурс] – Режим доступу: https://concordium.com/articles-and-blogs/.

27. Центр обробки даних контейнерного типу [Електронний ресурс] – Режим доступу: https://it-integrator.ua/sites/default/files/imce/prezentaciya_rishennya_v_umovah_voyennogo_chasu.pdf.

28. Живило Є.О., Докіль В. М. Модель методики оцінювання спроможностей військ зв'язку та кібербезпеки Збройних Сил України щодо виконання завдань з відбиття воєнної агресії в кіберпросторі // Сучасні інформаційні технології у сфері безпеки та оборони № 1 (46)/2023: – НУОУ, Київ, 2023. – С. 32-40.

REFERENCES:

1. Cherny`sh R.F., Ignatyuk M.V. Proty`diya destrukty`vnomu informacijnomu vply`vu v Ukrayini: pravovi ta organizacijni aspekty` [Elektronny`j resurs] – Rezhy`m dostupu: http://lsej.org.ua/1_2022/54.pdf.

2. Doktry`na zv'yazok ta informacijni sy`stemy`, vvedena v diyu Golovnokomanduvachem Zbrojny`x Sy`l Ukrayiny` vid 20 chervnya 2020 roku, VKP 6-00(01).01.

3. Zhy`vy`lo Ye.O., Chernonog O.O. Strategiya kiberoborony` Ukrayiny` // Zbirny`k naukovy`x pracz` VITI # 4 – 2017 [Elektronny`j resurs] – Rezhy`m dostupu: //http://www.viti.edu.ua/files/zbk/2017/4/4_4_2017.pdf.

4. Zakon Ukrayiny` "Pro nacional`nu bezpeku Ukrayiny`" vid 21.06.2018 r. # 2469-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Zakon Ukrayiny` "Pro osnovni zasady` zabezpechennya kiberbezpeky` Ukrayiny`" vid 05.10.2017 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Zakon Ukrayiny` "Pro zaxy`st informaciyi v informacijno-telekomunikacijny`x sy`stemax" [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

7. Zakon Ukrayiny` "Pro rozvidku" vid17.09.2020 # 912-IX [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/912-20#Text.

8. Zakon Ukrayiny` "Pro Nacional`nu programu informaty`zaciyi" vid 04.02.1998 r. # 74/98-VR // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text.

9. Zakon Ukrayiny` "Pro raty`fikaciyu Konvenciyi pro kiberzlochy`nnist`" vid 10.03.2006 r. # 2163-VIII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

10. Pro Derzhavnu sluzhbu special`nogo zv'yazku ta zaxy`stu informaciyi : Zakon Ukrayiny` vid 23.02.2006 r. [Elektronny`j resurs]. – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

11. Zakon Ukrayiny` "Pro derzhavnu tayemny`cyu"vid 21 sichnya 1994 # 3855-XII (zi zminamy`) [Elektronny`j resurs]. – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

12. Zakon Ukrayiny` "Pro dostup do publichnoyi informaciyi" vid 13 sichnya 2011 r. # 2939-VI. [Elektronny`j resurs] – Rezhy`m dostupu : https://zakon.rada.gov.ua/laws/show/2939-17#Text.

13. Zakon Ukrayiny` “Pro zaxy`st personal`ny`x dany`x” vid 01.06.2010 r. # 2297-VI [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

14. Zakon Ukrayiny` “Pro oboronu Ukrayiny`” vid 06.12.1991 r. # 1932-XII // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

15. Zakon Ukrayiny` Ukrayiny` “Pro informaciyu” # 2938-VI. [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

16. Zakon Ukrayiny` “Pro Zbrojni Sy`ly` Ukrayiny`” vid 6 grudnya 1991 roku # 1934-XII (zi zminamy`) // Zakonodavstvo Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/1934-12#Text.

17. Strategiya nacional`noyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 14 veresnya 2020 roku # 392/2020 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny`], vid 14 veresnya 2020 roku Pro Strategiyu nacional`noyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/3922020-35037.

18. Strategiya kiberbezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 26 serpnya 2021 roku # 447/2021, – Rezhy`m dostupu https://www.president.gov.ua/documents/4472021-40013.

19. Strategiya voyennoyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 25 bereznya 2021 roku # 121/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 25 bereznya 2021 roku Pro Strategiyu voyennoyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/1212021-37661.

20. Ukaz Prezy`denta Ukrayiny` #473/2021 vid 17 veresnya 2021 roku #473/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 20 serpnya 2021 roku “Pro Strategichny`j oboronny`j byuleten` Ukrayiny`” [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/4732021-40121.

21. Ukaz Prezy`denta Ukrayiny` #27/2020 28 sichnya 2020 roku Pro vnesennya zmin do Ukaziv Prezy`denta Ukrayiny` vid 27 sichnya 2015 roku # 37 ta vid 7 chervnya 2016 roku # 242 [Elektronny`j resurs] – Rezhy`m dostupu: https://zakon.rada.gov.ua/laws/show/27/2020#Text.

22. Strategiya informacijnoyi bezpeky` Ukrayiny`, vvedena v diyu Ukazom Prezy`denta Ukrayiny` vid 28 grudnya 2021 roku # 685/2021 Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` vid 15 zhovtnya 2021 roku Pro Strategiyu informacijnoyi bezpeky` Ukrayiny` [Elektronny`j resurs] – Rezhy`m dostupu: https://www.president.gov.ua/documents/6852021-41069.

23. Zhy`vy`lo Ye.O. Servisy` zv'yazku ob'yednanoyi merezhi za standartamy` krayin NATO // Elektronna biblioteka Nacz. un-t im. Yu. Kondratyuka, 82 s. – 2023. [Elektronny`j resurs] – Rezhy`m dostupu: //http://lib.nupp.edu.ua/elcat/alog?tab=b961c4f53c15ad9d36d3fa0351b68eb0.

24. Zhy`vy`lo Ye.O. Sy`tuacijny`j centr Ministerstva oborony` Ukrayiny` – model` zavchasnogo vy`yavlennya ta analizu kry`zovy`x sy`tuacij sektoru bezpeky` derzhavy` // Zbirny`k naukovy`x pracz` XNU im. V. N. Karazina #1 (60) – 2022 [Elektronny`j resurs] – Rezhy`m dostupu: https://periodicals.karazin.ua/apdu/article/view/21125/19764.

25. Yedy`ny`j perelik (katalog) spromozhnostej Ministerstva oborony` Ukrayiny`, Zbrojny`x Sy`l Ukrayiny` ta inshy`x skladovy`x Sy`l oborony`, zatverdzheno Ministrom oborony` Ukrayiny` 31 grudnya 2021 roku.

26. Lisakonov V. Bagatosharovi kiberataky` Rosiyi ne znayut` mezh, 2019 [Elektronny`j resurs] – Rezhy`m dostupu: https://concordium.com/articles-and-blogs/.

27. Centr obrobky` dany`x kontejnernogo ty`pu [Elektronny`j resurs] – Rezhy`m dostupu: https://it-integrator.ua/sites/default/files/imce/prezentaciya_rishennya_v_umovah_voyennogo_chasu.pdf.

28. Zhy`vy`lo Ye.O., Dokil` V. M. Model` metody`ky` ocinyuvannya spromozhnostej vijs`k zv'yazku ta kiberbezpeky` Zbrojny`x Sy`l Ukrayiny` shhodo vy`konannya zavdan` z vidby`ttya voyennoyi agresiyi v kiberprostori // Suchasni informacijni texnologiyi u sferi bezpeky` ta oborony` # 1 (46)/2023: – NUOU, Ky`yiv, 2023. – C. 32-40.

PhD. Zhivilo E.O., Zlobin K.V., Kuz V.S.

REQUIREMENTS FOR CYBER PROTECTION OF INFORMATION AND COMMUNICATION SYSTEMS AND COMMUNICATION SERVICES DURING THEIR DEPLOYMENT AND OPERATION AT THE CONTROL POINTS OF THE COMPONENTS OF THE DEFENSE AND SECURITY FORCES

The relevance of this work is due to the fact that in recent years the communication forces have been constantly developing and equipped with the latest digital means of communication, which allows them to successfully perform their assigned tasks. Today, information and communication systems that are deployed at the control points of various branches of management ensure the implementation of priority tasks for the management of troops. Functionally, the communication system and information systems are deployed at control points as a single information and communication environment based on the implementation of the latest information and communication technologies, information exchange protocols, complexes, systems and means of communication, which ensures the exchange of all types of information between bodies military management (management bodies) and control points at all levels of management. An active communication system ensures the exchange of information with guaranteed security in a single information space as a set of material functions (including personnel and other resources) that combine to perform a certain task.

In turn, information systems, as a set of equipment, methods and procedures, and, if necessary, personnel organized to perform information processing functions operate in accordance with a defined structure, namely:

- services, in the context of communication and information systems;

- architecture, in the context of communication and information systems;

- functions in the context of service-oriented architecture;

- interoperability;

- information protection and cyber protection.

It is clear that the more important the object of management, the more capacious flow of information can be directed to it. This allows the adversary/attacker to identify the most important targets and direct other types of information to them or suppress them in various ways. Thus, in the interests of ensuring cyber protection of electronic information resources, communication and technological systems of the control points of the Armed Forces of Ukraine, the technological infrastructure of cyber protection of the Armed Forces of Ukraine has been deployed and is functioning, which is a component of the unified system of information protection and cyber protection in the information and communication systems of the Ministry of Defense and the Armed Forces of Ukraine. In these conditions, to solve the tasks of preventing unwanted interventions, disruption of the stable functioning of the information and communication environment at control points, counterweights in obtaining confidential information, data theft, and other minimally necessary components of the cyber protection infrastructure are deployed. The main components of the relevant technological infrastructure of cyber protection are the security information event management system (SIEM), the threat information exchange platform (Malware Information Sharing Platform & Threat Sharing, MISP), the centralized management system of inter-network screens and the system for detecting and countering cyber threats. including computer viruses on end equipment.

Therefore, solving the tasks of ensuring cyber protection in the course of deployment and operation of electronic communication networks and communication services at the control points of various branches of management turns out to be quite a serious and urgent task.

Keywords: control point, information and communication environment, cyber space, cyber threat, cyber security, cyber defense.