Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістр
(ступінь вищої освіти)

на тему: **«Дослідження шляхів створення та розгортання системи кібербезпеки в інформаційно-телекомунікаційних системах вузлів зв'язку»**

Виконав: студент 6 курсу, групи д6ТТ спеціальності 172 «Електронні комунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)

Голубцов С.С.
(прізвище та ініціали)

Керівник Фомін О.С.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Полтава - 2025 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти: Магістр
Спеціальність 172 «Електронні комунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри автоматики, електроніки та телекомунікацій

_____ О.В. Шефер
"02" 09 2024 р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Голубцову Сергію Сергійовичу

1. Тема проекту (роботи) **«Дослідження шляхів створення та розгортання системи кібербезпеки в інформаційно-телекомунікаційних системах вузлів звязку.»**

керівник проекту (роботи) ФОМІН Олександр Сергійович, к.т.н., доцент
затверджена наказом вищого навчального закладу
від "09" 08 2024 року №218 09.а

2. Строк подання студентом проекту (роботи) 19.12.2024 р.

3. Вихідні дані до проекту (роботи) Оцінка поточної ситуації з кіберзахисту в ІТС польових вузлів зв'язку. Аналіз існуючих систем кібербезпеки та ефективність їх застосування. Рекомендації щодо інтеграції сучасних технологій та обладнання різних виробників в польових умовах.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Розроблено проект оперативно-тактичних вимог до систем кібернетичної безпеки в інформаційно-телекомунікаційних системах польових вузлів зв'язку пунктів управління тактичної, оперативної та стратегічної ланок управління Збройних Сил України. Розроблено проект тактико-технічних вимог до програмного забезпечення розподілених підсистем системи кібернетичної безпеки в інтересах забезпечення заходів з кіберрозвідки, кіберзахисту, ведення кібердій (кібероперацій) та кібероборони в інформаційно-телекомунікаційних системах польових вузлів зв'язку пунктів управління тактичної, оперативної та стратегічної ланок управління Збройних Сил України.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):

1) Аналіз існуючого стану системи кібербезпеки в ІТС ПВЗ різних ланок управління ЗС України.
2) Аналіз порушень політик безпеки в інформаційно-телекомунікаційних системах ЗС України.
3) Типові схеми розгортання системи кібербезпеки в ІТС ПВЗ.
4) Застосування технології віртуальних приватних мереж на ПВЗ ПУ.
5) Розгортання інфраструктури відкритих ключів (PKI).
6) Розробка проекту оперативно-тактичних вимог до систем кібернетичної безпеки в ІТС ПВЗ ПУ.
7) Основні бойові завдання систем кібернетичної безпеки в ІТС ПВЗ ПУ.
8) Висновки по роботі.

6. Дата видачі завдання 02.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін та обсяг виконання етапів роботи			Примітка (плакати)
1	Аналіз існуючого стану системи кібербезпеки в ІТС ПВЗ різних ланок управління ЗС України.	07.10.24	I	15%	Пл. 1-3
2	Аналіз порушень політик безпеки в інформаційно-телекомунікаційних системах ЗС України.			25%	Пл. 4-6 Пл. 7-9
3	Типові схеми розгортання системи кібербезпеки в ІТС ПВЗ тактичної, оперативної та стратегічної ланок управління ЗС України.	12.11.24	II	30%	Пл. 10-13
4	Застосування технології віртуальних приватних мереж на ПВЗ ПУ різних ланок управління ЗС України.			40%	Пл. 14-16
5	Розгортання інфраструктури відкритих ключів (PKI).			50%	Пл. 17-18
6	Розробка проекту оперативно-тактичних вимог до систем кібернетичної безпеки в ІТС ПВЗ ПУ.	19.12.24	III	60%	Пл. 19-20
7	Основні бойові завдання систем кібернетичної безпеки в ІТС ПВЗ ПУ.			80%	Пл. 21
9	Загальні висновки до магістерської роботи.			100%	Пл. 22-25

Магістрант (підпис) Голубцов С.С. (прізвище та ініціали)

Керівник роботи (підпис) Фомін ,О.С (прізвище та ініціали)

ЗМІСТ

ВСТУП

Актуальність. Підготовка та ефективне застосування Збройних Сил України, а також інших військових формувань і правоохоронних органів спеціального призначення, є критично важливими для забезпечення національної безпеки. Це залежить від визначених функцій і завдань, які покладені на ці організації згідно з законодавством України, а також від умов воєнно-політичної і воєнно-стратегічної обстановки, тенденцій її розвитку та потенційних загроз.

У 2024 році тривала реформа системи управління Збройних Сил України, що передбачає посилення можливостей органів військового управління та підвищення якості оперативного і бойового управління. У рамках цієї реформи було проведено оптимізацію системи управління угрупованнями сил, зокрема перехід від трьох до двох оперативно-тактичних угруповань, що сприяє ефективнішій організації та управлінню.

Структура пунктів управління різних рівнів регламентується директивами Генерального штабу, що визначає їх склад, призначення та функції в контексті загальної системи управління військами. Одним із важливих аспектів є оптимізація органів військового управління відповідно до стандартів НАТО, переоснащення системи зв’язку на цифрову платформу та впровадження сучасних інформаційних технологій. Зважаючи на недостатню надійність існуючих інформаційно-телекомунікаційних систем, питання захисту інформації та кібербезпеки набуває особливої актуальності. Це стосується не лише конфіденційності та цілісності даних, але й їх доступності в умовах збройного конфлікту. Управління у готовності до виконання завдань вимагає чіткої організації та належного забезпечення інформаційної безпеки.

В умовах сучасних викликів та загроз, важливо розглянути шляхи створення та розгортання системи кібербезпеки в інформаційно-

телекомунікаційній системі Збройних Сил України, використовуючи міжнародні досягнення у цій сфері. Це дозволить підвищити ефективність управління та забезпечення безпеки в умовах сучасних військових конфліктів.

Отже **мета роботи** полягає в обґрунтуванні та розробці перспективних схем розгортання системи кібербезпеки для інформаційно-телекомунікаційних систем польових вузлів зв'язку, що функціонують в пунктах управління різних ланок Збройних Сил України.

У першому розділі проведено аналіз уразливостей, методів захисту інформації, систем автентифікації та процедур реагування на кіберінциденти в контексті військових операцій. Також розглянуто функціонування системи кібербезпеки в інформаційно-телекомунікаційних системах польових вузлів зв'язку на тактичному, оперативному та стратегічному рівнях управління, а також її вплив на систему управління Збройних Сил України та автоматизоване управління військами.

Другий розділ кваліфікаційної роботи присвячений розробці проекту оперативно-тактичних вимог до системи кібербезпеки в інформаційно-телекомунікаційних системах польових вузлів зв'язку на тактичному, оперативному та стратегічному рівнях управління Збройних Сил України.

У третьому розділі роботи були розроблені можливі варіанти схем розгортання системи кібербезпеки в інформаційно-телекомунікаційних системах польових вузлів зв'язку різних ланок управління Збройних Сил України. Також запропоновано перелік необхідного програмного забезпечення для ефективного розгортання системи кібербезпеки в інформаційно-телекомунікаційних системах польових вузлів зв'язку на тактичному, оперативному та стратегічному рівнях управління.

Об'єктом дослідження є система кібербезпеки в інформаційно-телекомунікаційних системах польових вузлів зв'язку пунктів управління Збройних Сил України.

Предметом є розробка, оптимізація та оцінка ефективності механізмів і технологій кібербезпеки, що застосовуються в інформаційно-телекомунікаційних системах польових вузлів зв’язку пунктів управління Збройних Сил України.

Відповідно до визначеної мети в дипломній роботі поставлені, і вирішені наступні задачі:

- Розроблено проєкт оперативно-тактичних вимог до систем кібернетичної безпеки в інформаційно-телекомунікаційних системах польових вузлів зв’язку пунктів управління тактичної, оперативної та стратегічної ланок управління Збройних Сил України.

- Розроблено проект тактико-технічних вимог до програмного забезпечення розподілених підсистем системи кібернетичної безпеки в інтересах забезпечення заходів з кіберрозвідки, кіберзахисту, ведення кібердій (кібероперацій) та кібероборони в інформаційно-телекомунікаційних системах польових вузлів зв’язку пунктів управління тактичної, оперативної та стратегічної ланок управління Збройних Сил України.

Наукова новизна роботи полягає в розробленні комплексного сценарію DDoS із множинним обходом в навчальних цілях.

Методи дослідження. Для вирішення поставлених задач в дипломній роботі використовувались загальнонаукові підходи дослідження: системний, історичний, міждисциплінарний; методи: аналіз, синтез, індукція, дедукція, порівняльний, візуальний (графічний).

Основні результати, отримані в роботі що виносяться на захист:

1. Проект оперативно-тактичних вимог до систем кібербезпеки в інформаційно-телекомунікаційній системі польових вузлів зв’язку пунктів управління тактичної, оперативної та стратегічної ланок управління Збройних Сил України.

2. Схеми розгортання системи кібернетичної безпеки в інформаційно-телекомунікаційній системі польових вузлів зв’язку тактичної, оперативної та стратегічної ланок управління Збройних Сил України.

Отримані результати досліджень мають практичну цінність і можуть бути використані при створенні та розгортанні Центру оперативного реагування на інциденти кібербезпеки. Основним призначенням цього центру є підвищення захищеності кіберпростору в мережах як закритої, так і відкритої складової інформаційно-телекомунікаційних систем Збройних Сил України. Центр також буде відповідати за реагування на інциденти кібербезпеки та кібератаки в системі управління збройних сил, а також за збір і обробку журналів подій з пристроїв забезпечення кібернетичної безпеки, мережевих пристроїв та автоматизованих робочих місць, підключених до інформаційно-телекомунікаційних систем Збройних Сил України.

Результати дослідження будуть використані для формування пропозицій щодо розробки та вдосконалення існуючої нормативно-правової бази в сфері кіберзахисту об’єктів критичної інфраструктури в інформаційно-телекомунікаційних системах Збройних Сил України. Це стосуватиметься розробки проєктів Стратегії кібербезпеки Збройних Сил України та Концепції кібербезпеки Збройних Сил України, а також Настанови з кібероперацій.

Крім того, результати сприятимуть удосконаленню Наказу Міністерства оборони України “Про затвердження Тимчасової настанови із забезпечення кібербезпеки в інформаційно-телекомунікаційних системах Міністерства оборони України та Збройних Сил України”. Вони також будуть корисні при створенні Керівництва з інформаційної та кібербезпеки в інформаційно-телекомунікаційних системах Збройних Сил України, а також Програми розвитку системи захисту інформації та кібербезпеки в цих системах.

Представлений результат дослідження є новим, оскільки у відкритих та таємних наукових матеріалах відсутнє дублювання, що і визначає практичну цінність яку отримано вперше. Достовірність наукових положень, результатів отриманих в роботі підтверджується коректною постановкою задач.

Особистий внесок. Всі дослідження, викладені в дипломній роботі, проведені автором в процесі наукової діяльності. Результати, які виносяться на захист, отримані особисто, запозичений матеріал позначений в роботі посиланнями.

РОЗДІЛ 1
АКТУАЛЬНІСТЬ ТА ОБҐРУНТУВАННЯ ВИБОРУ ТЕМИ

1.1. Аналіз існуючого стану системи кібербезпеки в ІТС ПВЗ різних ланок управління ЗС України

Сьогодні функціонування системи кібербезпеки (далі – СКБ) в інформаційно-телекомунікаційних системах польових вузлів зв'язку (далі – ІТС ПВЗ) на тактичному, оперативному та стратегічному рівнях управління відбувається в умовах активного протистояння збройній агресії та анексії Криму з боку Російської Федерації. Протягом конфлікту на сході України Збройні Сили України (далі – ЗС України) змогли розгорнути досить сучасну і ефективну систему зв'язку, що стала однією з найкращих в історії незалежності держави.

Ця система управління (далі – СУ) забезпечує надійність, стійкість і безперервність управління військами (далі – УВ) у пунктах постійної дислокації та в районах виконання завдань, зокрема під час операції об'єднаних сил (далі – ОС). Керівні органи всіх рівнів управління виконують свої функції за призначенням, незважаючи на оптимізацію та перехід на структури штабів військ НАТО, а також на переоснащення та нарощування системи зв'язку [1].

Реформування та розвиток СУ в ЗС України триває, і посилюються спроможності органів військового управління (далі – ОВУ) з метою підвищення якості оперативного та бойового управління на ПВЗ всіх ланок управління (далі – ЛУ). Ці зусилля ґрунтуються на принципах і стандартах, прийнятих в країнах – членах НАТО [1].

Особлива увага приділяється розвитку та сталому функціонуванню кіберпростору (далі – КП) і електромагнітного спектру для протидії ворогам, які мають значну технічну перевагу та спроможності в веденні гібридних конфліктів. Проте супротивник демонструє вражаючі можливості у

здійсненні кібератак (далі – КА) на ІТС ЗС України, що ставить під загрозу домінування нашої держави в КП. Це, в свою чергу, негативно впливає на сталий розвиток СКБ в ІТС ПВЗ на всіх рівнях управління та їх інтеграцію в загальну СУ ЗС України [1].

У зоні проведення ООС триває розгортання та удосконалення ключових інформаційних систем, зокрема [1]:

- Єдиної інтеграційної платформи ЗС України “Дельта”, призначеної для інтеграції інформаційних ресурсів (далі – ІР) різнотипних автоматизованих систем управління (далі – АСУ). Ця платформа створює єдине геоінформаційне та інформаційно-аналітичне середовище для ОВУ, військових частин та підрозділів ЗС України.

- Інформаційної системи збору, обробки та надання інформації про повітряну і надводну обстановку.

ЗС України також значно наростили зусилля у веденні радіоелектронної боротьби (далі – РЕБ) в районі проведення ООС, дотримуючись кращих світових практик. Це забезпечило [1]:

- Контроль за радіоелектронною обстановкою в визначених районах.

- Вплив засобами РЕБ на безпілотні літальні апарати противника на основних напрямках їх дій.

- Виявлення та придушення радіоліній зв’язку противника, побудованих на цифрових технологіях.

Центр оперативного реагування на інциденти кібербезпеки (далі – ЦОРІ КБ) в ІТС Міністерства оборони України та Генерального штабу ЗС України (далі – ГШ ЗСУ), аналогічний центрам ЗС США та блоку НАТО (DODIN-A), є важливим інструментом для ведення бойових дій (далі – БД) і необхідною умовою успіху сухопутних операцій. Ефективне використання та захист цієї мережі, а також інформації, є критично важливими для успіху ОВУ всіх рівнів [2].

Слід врахувати, що майбутні дії ворога будуть спрямовані на проникнення в наші мережі та намагання використовувати їх у своїх

інтересах або негативно впливати на доступ до даних. Командувач або начальник, що втрачає доступ до СУ під час операції, не лише ризикує втратити конфіденційну інформацію, а й ставить під загрозу життя своїх підлеглих, критично важливі ресурси та можливість успішного виконання завдань.

У майбутньому, з урахуванням зростання спроможностей супротивників, забезпечення переваги в КП та електромагнітному спектрі стане ще більш важливим для успішного проведення військових операцій.

Використання можливостей КП за єдиною методологією планування, інтеграції та синхронізації значно підвищує здатність командирів (начальників) усіх ЛУ адекватно оцінювати обстановку, планувати застосування військових частин (підрозділів) та координувати виконання кількох операцій, що проводяться в одній сфері або середовищі БД. Така координація дій військ (сил), як наступальних, так і захисних, дозволяє швидше реагувати на дії ворогів і супротивників [2].

Будь-яка оперативна потреба, пов’язана з електронною передачею інформації в ІТС ПВЗ на тактичному, оперативному та стратегічному рівнях, повинна враховувати можливості впливу які притаманні КП.

Аналізуючи функціонування СКБ в ІТС країн НАТО на різних рівнях управління, включаючи ПУ та СУ в цілому, важливо зазначити, що для набуття спроможностей у КП, коли основною метою є досягнення стратегічних цілей, необхідно розглядати їх як взаємопов’язані дії, які поділяються на [3]:

- Операції в ІТС ОВУ стратегічного рівня країн НАТО.
- Оборонні кібероперації (далі – КО).
- Наступальні КО.

До засобів протиборства у КП належать апаратні комплекси, програмні засоби та апаратно-програмні комплекси, що можуть включати будь-яке поєднання програмного забезпечення (далі – ПЗ), програмно-апаратних засобів або апаратного забезпечення. Вони призначені для

забезпечення впливу у КП або як наслідок дій, які в ньому здійснюються. На Рисунку 1.1 представлено візуальне взаємопов'язане поєднання КП в СУ всіх ЛУ, а також використання електромагнітного спектру в оперативній обстановці [3].

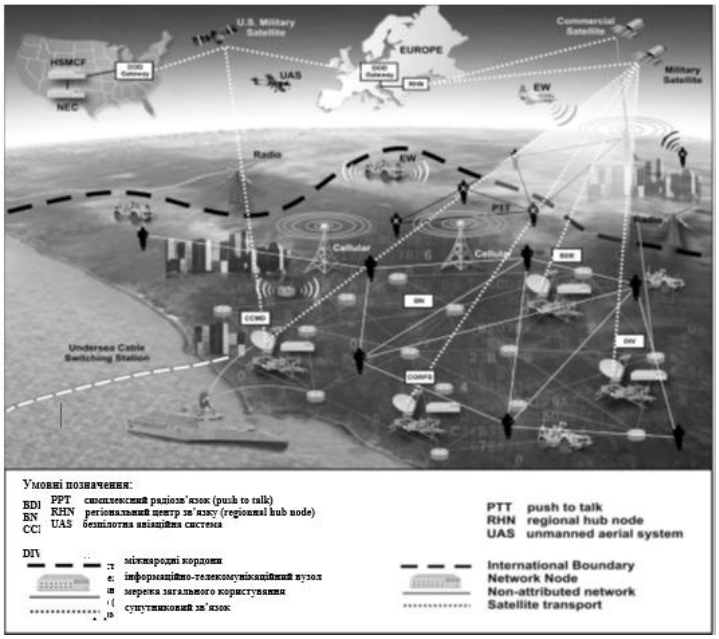


Рисунок 1.1. – Використання КП для досягнення цілей переваги (домінування) в оперативній обстановці

ІТС оперативного управління стратегічної ЛУ є частиною КП країн блоку НАТО (Рис.1.2.). Їхня ключова характеристика полягає в здатності забезпечувати обмін інформацією між військами (силами) у різних сферах ведення БД.

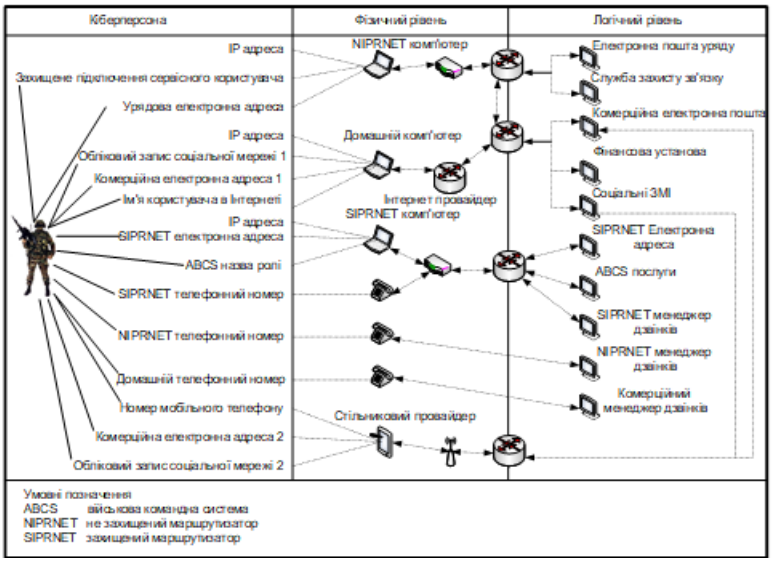


Рисунок 1.2. – Забезпечення обміну інформацією між військами(силами) у різних сферах ведення БД країн блоку НАТО

ІТС ОВУ стратегічної ЛУ складається з інформаційних можливостей та процесів, що дозволяють збирати, обробляти, зберігати, розповсюджувати та управляти інформацією на користь ЗС, починаючи від окремого військовослужбовця до органів державного управління та допоміжного персоналу. Це відбувається незалежно від того, чи є учасники взаємопов'язаними або діють окремо, з використанням як власних, так і орендованих комунікаційних та обчислювальних систем і сервісів, ПЗ (включаючи прикладні програми), даних, сервісів безпеки та інших систем національної безпеки [3].

До інформаційної мережі (далі – ІМ) ІТС ОВУ стратегічної ЛУ входять усі інформаційні технології (далі – ІТ), включаючи системи, платформи, сервіси та матеріально-технічні засоби. На цьому рівні реалізується принцип делегування повноважень (mission command), що залежить від рівня застосування дій у КП для забезпечення комунікації, зберігання інформації, планування операцій та виконання завдань [3].

Операції ЗС країн-членів НАТО значною мірою залежать від КП, особливо в аспектах синхронізації, зберігання, координації та захисту інформації (далі – ЗІ) (Рисунок 1.3.). ОВУ різних ЛУ використовують можливості КП, проте їхня діяльність не обмежується цими можливостями, навіть у випадку зменшення їхньої ефективності при досягненні цілей командувача ОС [3].

Таким чином, свобода маневру у використанні КП для виконання завдань командира реалізується через зосереджене планування бойового застосування (далі – БЗ) КП від стратегічної ЛУ до підрозділів тактичної ЛУ (Рисунок – 1.4). Забезпечуючи реалізацію принципу делегування повноважень та свободи дій у КП, операції, які проводять американські збройні сили та їхні союзники, сприяють досягненню поставлених цілей командувача ОС [2, 3].

ЗС країн-членів НАТО здійснюють як наступальні, так і оборонні КО. До цих операцій входять розгортання та функціонування захищеного зв'язку, виявлення та нейтралізація загроз в ІТС департаменту оборонної ІМ, а також аналіз, реагування, аварійне відновлення та запобігання інцидентам КБ в СУ ЗС.

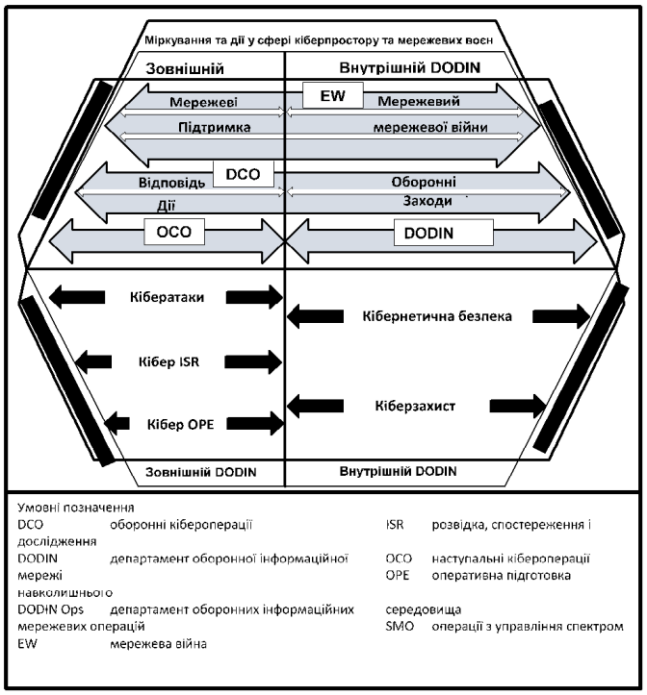


Рисунок 1.3. – Спроможності ЗС країн-членів НАТО у КП щодо синхронізації, зберіганні, координації та ЗІ під час ведення операцій

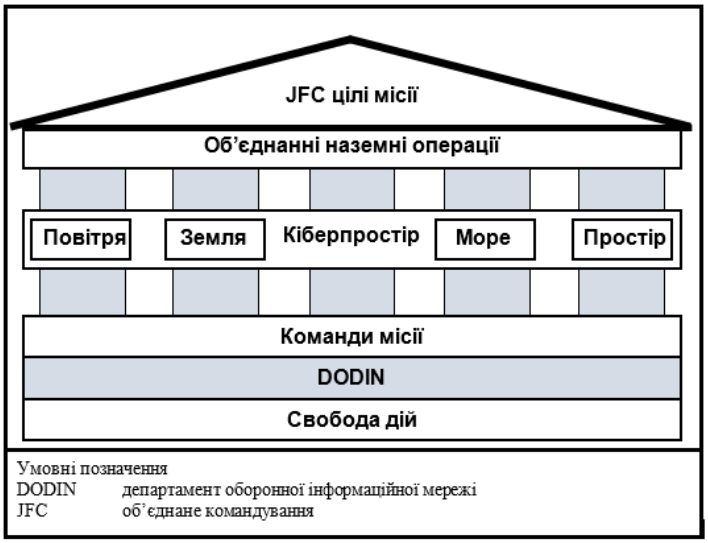


Рисунок 1.4. – Свобода маневру та підтримки цілей командуючого ОС (угрупованням)

Ці операції проводяться в інтересах підрозділів, починаючи з стратегічної та закінчуючи тактичною ЛУ ОС, з метою одночасного перешкоджання ефективному використанню КП та електромагнітного спектру з боку ворогів та супротивників. Сегментом країн-членів НАТО в ІТС департаменту оборонної ІМ є технічна мережа, яка охоплює СУ інформацією та інформаційні системи, що накопичують, обробляють, зберігають, відображають, розповсюджують та забезпечують ЗІ в глобальному масштабі. [3]

КО, що здійснюються, можуть підтримувати або бути підтриманими КО ОС. Взаємна підтримка та тісна координація між ОС під час проведення КО забезпечують керівництву та штабам більші можливості для планування БЗ військових частин та підрозділів [3].

Для виконання завдань у КП здійснюються кілька ключових дій (Рис. 1.5.):

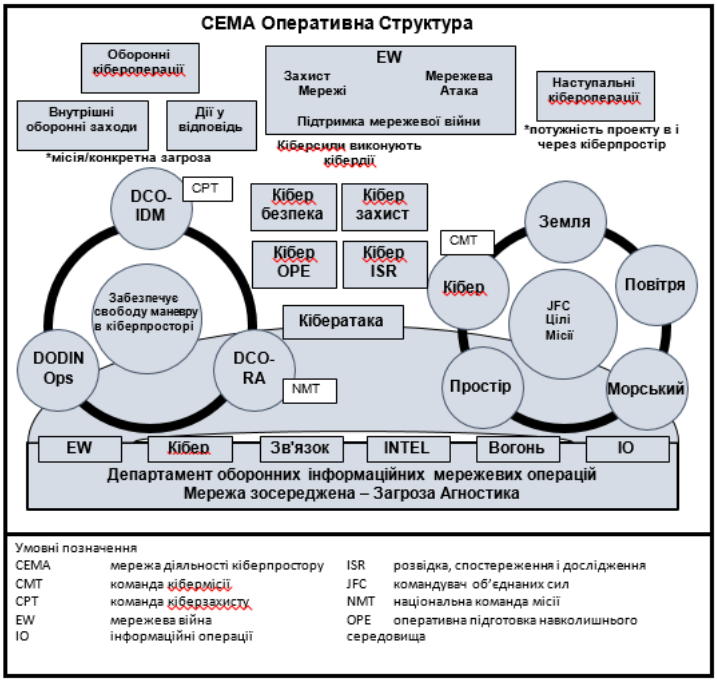


Рисунок 1.5. – Дії у кіберпросторі ЗС країн-членів НАТО

кібероборона (далі – КОб) (cyberspace defense), яка спрямована на захист інформаційних систем від кіберзагроз (далі – Кзаг); розвідка, спостереження та рекогносцирування у КП (cyberspace intelligence, surveillance, and

reconnaissance, ISR), що охоплює процеси збору та аналізу інформації про потенційні загрози; підготовка до проведення КО (cyberspace OPE), яка включає заходи, що передують активним операціям; атака у КП (cyberspace attack), спрямована на ураження противника в кіберсередовищі (далі – КС); та забезпечення КБ (cyberspace security), що містить комплекс заходів для забезпечення конфіденційності, цілісності та доступності інформації [3].

Ці дії є основою для проведення операцій у департаменті оборонної ІМ (DODIN operations), оборонних КО (defensive cyberspace operations, DCO) та наступальних КО (offensive cyberspace operations, OCO), або їх комбінацій. Виконання цих дій на всіх рівнях управління залежить від наявних повноважень, спроможностей та координації. Важливо, що ці дії взаємопов'язані, і для досягнення успіху в КП може знадобитися одночасне застосування кількох з них [3].

ІТС ЗС України – є критично важливим засобом (об'єктом) ведення БД, який забезпечує можливості щодо реалізації принципу делегування підлеглим ОВУ повноважень, щодо прийняття рішень з вибору шляхів виконання завдань, нанесення вогневого ураження, проведення розвідувальної діяльності, всебічного забезпечення, та забезпечує підтримку проведення всіх операцій. Доступ до ІТС МО та ГШ ЗСУ дозволяє командирам (начальникам) моделювати (проектувати) застосування військ (сил), проводити допоміжні операції, та досягати цілей, поставлених Головнокомандувачем ЗС України, командувачами видів ЗС України. Забезпечення КБ та експлуатація зазначеної розгалуженої мережі на ПУ стратегічної ЛУ є одним з найбільш складних та важливих завдань, які на даний час виконуються Головним об'єднаним центром захисту інформації та кібернетичної безпеки ІТС ЗСУ (далі – ГОЦЗІ та КБ ІТС ЗСУ). Наявність навіть однієї вразливості в цій мережі може нести ризики на БЗ військових частин (підрозділів) та також на час проведення операцій, що може привести до зриву виконання бойових завдань.

КБ в ІТС ПВЗ тактичної, оперативної та стратегічної ЛУ включає контроль характеристик каналів зв'язку утворених різними засобами. Дії у КП та використання різних каналів зв'язку пов'язані між собою. Сучасні засоби зв'язку, використовують для обміну даними різні середовища, залишаючи при цьому "сліди" обміну інформації. Виявлення, визначення характеристик, і вплив на зазначену діяльність (в або через КП) може мати негативні наслідки для діяльності ОВУ на ПУ різних ЛУ, під час ведення сеансів зв'язку, обміну інформацією.

Розгалуженість мереж, вузлів, ліній зв'язку ЗС України у поєднанні з телекомунікаційною мережею загального (відомчого, корпоративного) користування, що надає канали (лінії) передачі (телекомунікаційний ресурс) Збройним Силам, інших елементів різного призначення, які створюються (розгортаються) з метою забезпечення обміну інформацією в СУ військами дає змогу забезпечити можливість інтеграції фізичних середовищ шляхом передачі даних по трасам проходження сигналів через ланки та вузли у КП та середі розповсюдження [4].

ІТС ЗС України є критично важливим елементом ведення БД, що забезпечує реалізацію принципу делегування повноважень підлеглим ОВУ у прийнятті рішень щодо виконання завдань, нанесення вогневого ураження, проведення розвідувальної діяльності та всебічного забезпечення операцій. Доступ до ІТС Міністерства оборони та ГШ ЗСУ дозволяє командирам моделювати застосування військ, здійснювати допоміжні операції та досягати цілей, поставлених Головнокомандувачем ЗС України і командувачами видів ЗС [4].

Забезпечення КБ та експлуатація розгалуженої мережі на ПУ стратегічної ЛУ є одним із найскладніших завдань, що виконується ГОЦЗІ та КБ ІТС ЗСУ. Наявність навіть однієї вразливості в цій мережі може призвести до ризиків у БЗ військових частин та зриву виконання бойових завдань під час операцій [4].

Тому надзвичайно важливо здійснювати управління ризиками та забезпечувати захист КП в ІТС ПВЗ на тактичній, оперативній та стратегічній ЛУ. Це необхідно для стійкого функціонування системи зв'язку в будь-яких умовах обстановки.

СКБ в ІТС ПВЗ є складовою частиною загальної СКБ та ЗІ ЗС України. Вона охоплює всі інформаційні можливості ЗС України, які стосуються накопичення, обробки, зберігання, відображення, розповсюдження та забезпечення кіберзахисту (далі – КЗ) інформації під час переміщення пунктів управління, на бар'єрних ділянках, у районах зосередження, вихідному районі операції та в кінцевих районах [4].

СКБ в ІТС ПВЗ забезпечує доступ посадових осіб пунктів управління (груп бойового управління) до необхідної інформації в потрібному місці та в потрібний час. Це стосується командирів, начальників, штабів, солдатів, цивільних осіб, а також спільних, міжвидових або посадових осіб інших військових формувань та правоохоронних органів (далі – ІвФ та ПрО) [4].

ЦОРІ КБ в ІТС Міністерства оборони України, ГШ ЗСУ та ЗС України забезпечує доступ до ІТС ПВЗ на тактичній, оперативній та стратегічній ЛУ. Це можливе як з постійного місця дислокації, так і з тимчасового місця несення служби, через мережі постів, вузлів або станцій, а також розгорнуті мережі оперативної та тактичної ЛУ. Така структура доступу дозволяє виконувати завдання військових частин та підрозділів, що формуються, забезпечуючи доступ до централізованих ресурсів з будь-якої точки під час усіх оперативних фаз [4].

Мережева підтримка може забезпечуватися на постах, у таборах або в військових частинах постійної дислокації, під час переміщення до місць постійної дислокації. Вона може здійснюватися штатними силами та засобами, залежно від організаційно-штатної структури підрозділу та його матеріально-технічного забезпечення [4].

КБ в ІТС ПВЗ на всіх ЛУ включає комплекс заходів, спрямованих на проектування, створення, конфігурування, захист, використання, технічне

обслуговування та підтримку роботи комунікаційних систем і мереж. Це необхідно для забезпечення постійної доступності, цілісності та конфіденційності даних, а також безпомилкової ідентифікації користувачів – посадових осіб ПУ [5].

При реалізації цих заходів враховується потреба протидії широкому спектру загроз, а не лише конкретним. Це забезпечує користувачам ІТС ЗС України на всіх рівнях доступ до end-to-end мережі та інформаційної системи, ЗІ та оперативну передачу даних [5].

Виконання заходів з КБ в ІТС ПВЗ ПУ різних ЛУ забезпечує ефективну комунікацію, співпрацю та обмін інформацією. Особовий склад, що відповідає за ці заходи, здійснює розробку, налаштування, забезпечення безпеки та технічне обслуговування ІТС, що критично важливо для успішного виконання завдань військового управління на стратегічному, оперативному та тактичному рівнях. [5]

Одним з основних напрямів є виконання активних та пасивних заходів з КБ, які спрямовані на збереження можливостей використання ресурсів у КП. Ці заходи реалізуються з урахуванням актуальних загроз і пріоритетності завдань, відповідно до концепції “глибокоешелонованої оборони” (defense-in-depth), що передбачає багаторівневий захист ІТС [4, 5].

У рамках КБ здійснюється реагування на несанкціоновані дії, сповіщення про Кзаг, а також активний пошук загроз, що можуть бути пропущені стандартними заходами. Це включає в себе дії з перехоплення ініціативи у противників, які можуть загрожувати ІТС, а також виявлення внутрішніх загроз, проти яких звичайні засоби безпеки виявляються неефективними [4, 5].

КБ має бути спрямована на протидію атакам, використанню вразливостей та наслідкам впливу шкідливого ПЗ. Реалізація заходів здійснюється за допомогою багаторівневого, адаптивного захисту, що об’єднує цифрові та фізичні елементи захисту, з акцентом на активну фазу дій.

Для підвищення обсягу доступної інформації важливо постійно моніторити та аналізувати активність в ІТС, виявляти нехарактерні події та реагувати на них. Внутрішні захисні заходи включають розвідувальні дії для виявлення загроз у межах ІТС, а контроль загроз може здійснюватися за допомогою спеціальних кібернетичних інструментів.

1.2. Аналіз порушень політик безпеки в інформаційно-телекомунікаційних системах ЗС України

Розвиток сучасних ІТ в ІТС ЗС України суттєво впливає на формування сучасної СКБ на ПУ тактичної, оперативної та стратегічної ЛУ. Це спрямовано на підвищення захищеності КП в мережах цих пунктів [6].

Однак, разом із явними перевагами, цей перехід також приносить ряд викликів, що потребують вирішення, а саме [6]:

- Складність і різноманітність використовуваного програмного та апаратного забезпечення.

На сьогодні мережа ПУ на всіх рівнях ЗС України побудовані на різних ОС. Досвід свідчить, що в ІТС використовуються такі конфігурації: робочі станції працюють під управлінням ОС MS DOS, Windows 95 і Windows NT, при цьому в якості мережевої ОС застосовується Windows NT. Деякі системи з родини UNIX поки що не набули широкого визнання. Велика кількість конфігураційних параметрів використаного програмного та апаратного забезпечення ускладнює їх налаштування та експлуатацію [6].

- Велика кількість ПУ, ПВЗ, ІТС ЗС України, їх територіальна розподіленість та обмежений час для контролю всіх параметрів.

ПУ розгорнуті як у стаціонарних умовах, так і на рухомій базі, охоплюючи не лише одне місто, а й цілий регіон. Ця особливість, разом із браком часу для моніторингу всіх налаштувань, ускладнює адміністраторам КБ можливість особисто та своєчасно контролювати: діяльність користувачів

системи на всіх ПВЗ, а також відповідність налаштувань програмного та апаратного забезпечення заданим критеріям [6].

- Підключення ОВУ на ПВЗ ПУ різних ЛУ та доступ зовнішніх користувачів до мережі глобального Інтернету.

Ця ситуація часто ускладнює визначення меж мережі та всіх користувачів, підключених до неї, що може призвести до спроб несанкціонованого доступу (далі – НСД) до захищеної інформації. Однією з ключових проблем, що виникає внаслідок цих факторів, є збільшення кількості вразливостей в ІТС ПВЗ тактичної, оперативної та стратегічної ЛУ ЗС України [7].

Сукупність правил, законів і практичних рекомендацій, що регулюють забезпечення безпеки та охоплюють всі аспекти обробки інформації та прийняття рішень, називається політикою безпеки.

Для реалізації цього підходу необхідно дотримуватися комплексного підходу, який складається з кількох етапів [7]:

а) Інформаційне обстеження, що включає:

1. Категоризацію ІР за ступенем цінності та важливості.

2. Аналіз найбільш небезпечних і ймовірних загроз.

3. Побудову моделі потенційного порушника.

4. Розробку організаційно-розпорядчих документів, що регламентують питання ЗІ в ІТС.

б) Придбання, установка та налаштування засобів КЗ відповідно до результатів попереднього етапу.

в) Навчання особового складу основам політики безпеки.

г) Постійне оновлення політики безпеки та реконфігурація засобів КЗ відповідно до актуальної ситуації.

Для кожної ЛУ існує своя типова інформаційна система (ІС), яка складається з компонентів, що вирішують специфічні завдання. Загалом ІС включає чотири рівні [6, 7]:

1. Рівень прикладного ПЗ, який відповідає за взаємодію з користувачем. До елементів ІС цього рівня належать текстовий редактор WinWord, редактор електронних таблиць Excel, поштовий клієнт Outlook тощо.

2. Рівень СУБД, який забезпечує зберігання та обробку даних. Прикладами елементів ІС цього рівня є СУБД Oracle, MS SQL Server, Sybase, а також MS Access.

3. Рівень ОС, що забезпечує обслуговування СУБД та прикладного ПЗ. Серед елементів ІС цього рівня можна назвати ОС Microsoft Windows NT, Sun Solaris, Novell Netware.

4. Рівень мережі, відповідальний за взаємодію між ПВЗ ІТС. Прикладами елементів ІС цього рівня є протоколи TCP/IP, IPS/SPX і SMB/NetBIOS.

Виходячи з зазначеного вище, слід зауважити, що до складу типової перспективної схеми розгортання СКБ в ІТС та ПУ тактичної, оперативної та стратегічної ЛУ ЗС України повинні входити такі елементи [7]: робочі станції, що функціонують під управлінням ОС Windows NT, а також файловий сервер для зберігання документів і дистрибутивів ПЗ; бази даних SQL повинні розміщуватися на окремому сервері з MS SQL Server, хоча можливе використання інших платформ, таких як Oracle або Sybase; посадові особи ПВЗ ПУ активно повинні використовувати мережу Internet, причому це не обмежується лише електронною поштою чи переглядом веб-сайтів.

Для захисту внутрішніх ресурсів від зовнішніх загроз застосовується proxy-сервер MS Proxy Server або Novell BorderManager, який обмежує доступ сторонніх користувачів до внутрішньої мережі [7]. Доступ в Internet здійснюється через Dialup-з’єднання з модемом.

З огляду на наведені елементи ІС, можна виділити три основні завдання, що на неї покладаються [7]:

1. Виконання функціональних операцій.

2. Зберігання даних (документів, ПЗ, баз даних тощо).

3. Надання Internet-сервісів (веб-серфінг, електронна пошта тощо).

Однак, використання proxy-сервера часто обмежує всі захисні функції, що надає противнику широкий спектр можливостей для порушення політики безпеки на всіх чотирьох вищезгаданих рівнях ІС. Наприклад, для отримання НСД до інформації в базі даних MS Access зловмисники можуть спробувати реалізувати такі дії [7]:

1. Отримати доступ до записів бази даних через MS Excel (рівень прикладного ПЗ).

2. Читати необхідні дані за допомогою СУБД MS Access (рівень СУБД).

3. Прочитати файли бази даних з розширенням *.mdb безпосередньо на рівні ОС.

4. Надіслати по мережі пакети з запитами на отримання потрібних даних від СУБД (рівень мережі).

Для побудови ефективної системи захисту ІР важливо виділити найбільш критичні ділянки ІС. Для типової ІС такими ділянками є [7]:

- Контролер домену (первинний і резервний) на базі Windows NT або Novell Netware.

- MS Proxy Server на базі Windows NT або Novell Border Manager.

- Поштовий сервер під управлінням MS Exchange.

- Файлові сервери на Windows NT та Netware.

- Сервер бази даних на MS SQL Server.

- Мережа передачі даних.

Додатково в ІС є менш критичні елементи, такі як робочі станції під управлінням Windows 9x і Windows NT.

Не вдаючись до детального аналізу першого етапу побудови СКБ в ІТС ПУ тактичної, оперативної та стратегічної ЛУ ЗС України, розглянемо основні атаки на критичні ділянки ІТС та способи їх запобігання. Увага буде зосереджена на найбільш поширених і типових атаках. Важливо зазначити,

що основним джерелом більшості загроз є авторизовані користувачі (особовий склад, співробітники тощо) [8].

Несанкціоновані дії (НСД). Близько 75-80% усіх комп'ютерних інцидентів пов'язані з невиконанням інструкцій, наказів і керівних документів особовим складом, який працює на ПВЗ ПУ. Ці користувачі, через незнання, випадкові помилки або злого наміру, можуть впровадити в ІС вірус, видалити важливі файли або здійснити інші несанкціоновані дії [7, 8].

Згідно зі статистикою, опублікованою інститутом SANS, до найбільш поширених атак відносяться [8]:

1. НСД до паролів і конфіденційної інформації.
2. Несанкціоноване віддалене виконання команд внаслідок помилок типу "переповнення буферу".
3. Порушення прав доступу.
4. Атаки типу "відмова в обслуговуванні".
5. Завантаження ворожого контенту (такого як "троянські коні", мобільний код Java та ActiveX, віруси).

Розглянемо більш докладно ці атаки, схильні до впливу на компоненти ІС, а також застосовуємі заходи, що дозволяють виявити ці атаки, блокувати їх і запобігти їх поширенню.

НСД до паролю є атакою, що полягає в крадіжці або підборі пароля законного користувача ІС. Така атака може здійснюватися на будь-якому з компонентів ІС. Зловмисник може почати з отримання доступу до облікового запису користувача з обмеженими правами (наприклад, guest), але його кінцевою метою є отримання пароля адміністратора контролера домену, що дасть можливість контролювати всі компоненти ІС [8].

Підбір пароля – це другий спосіб несанкціонованого отримання пароля користувача. Для цього можуть використовуватися як "ручні" методи, засновані на знанні додаткової інформації про користувача, так і автоматизовані методи, які є значно ефективнішими. Наприклад, програма

L0phtCrack для Windows NT може здійснювати підбір паролів як віддалено через мережу, так і локально, де швидкість підбору значно збільшується [8].

Для захисту паролів від зловмисників можна застосувати різноманітні заходи. Серед організаційних заходів – заборона доступу сторонніх осіб у приміщення з обчислювальною технікою та знищення всіх паперів і роздруківок.

Щоб захистити паролі від перехоплення по каналах зв'язку, необхідно використовувати шифрування. Шифрування може бути "вбудованим" в ОС (наприклад, команда `SET ALLOW UNENCRYPTED PASSWORDS = ON` в Novell Netware) або реалізовуватися за допомогою додаткових засобів (програма PGP) або механізмів (захищений HTTP-протокол – HTTPS). Щоб захиститися від програм типу L0phtCrack, слід використовувати шифрування мережевого трафіку або заборонити віддалений доступ до системного реєстру Windows NT [8].

Несанкціоноване виконання команд є однією з найпоширеніших атак, що набула популярності через розповсюдженість ОС Unix. Проте випадки реалізації цієї атаки також зафіксовані для ОС Windows NT. Наприклад, ранні версії Microsoft Internet Information Server мали проблеми з обробкою довгих URL (понад 255 символів), що призводило до виконання команд, які передавалися в таких URL [8].

Ця атака може бути здійснена на будь-якому компоненті ІС, за винятком мережі передачі даних. Проте найчастіше вона реалізується на серверах, які працюють під управлінням Unix, а також на веб- і SMTP-серверах [8].

Для захисту від подібних атак важливо регулярно стежити за інформаційними бюлетенями з безпеки, які публікуються різними організаціями, що спеціалізуються на КБ, такими як X-Force (http://xforce.iss.net). Це дозволить оперативно виявляти та усувати вразливості у системах [8].

Порушення прав доступу є одним із найпоширеніших порушень політики безпеки. Неправильно налаштовані права доступу до ресурсів (файлів, каталогів, логічних та мережевих дисків, модемів тощо) можуть призвести до серйозних проблем. Наприклад, неконтрольоване використання модемів значно знижує ефективність таких захисних механізмів, як proxy-сервери та міжмережеві екрани (firewall) [8].

Невірно задані права доступу до виконуваних файлів або автозавантажувальних скриптів можуть дозволити зловмисникові впровадити в мережу вірус або закладку. Ситуація, що сталася кілька років тому, коли вірус OneHalf через скрипт підключення до сервера Novell Netware інфікував більше 70% ПК у мережі за один день, ілюструє цю загрозу. Використання загальнодоступних ресурсів на контролері домену Windows NT з неправильними правами доступу може також призвести до крадіжки паролів користувачів ІС [8, 9].

Запобігти такій атаці або, принаймні, виявити її, можна за допомогою правильної конфігурації елементів ІС та вбудованих механізмів захисту в ОС. Наприклад, налаштування прав доступу до всіх ресурсів на ПК з контролером домену допоможе захистити систему від багатьох атак на рівні ОС, СУБД та прикладного ПЗ. Налаштування цих прав можна виконати за допомогою [9]:

- Програми User Manager, що входить до складу Windows NT, або nwadmin і syscon для Novell Netware.

- Вкладки Security підпункту Properties меню File в Windows NT Explorer або програми Filer для Novell Netware.

Обов’язковою умовою ефективної системи захисту є реєстрація всіх подій у відповідному журналі (Event Log для Windows NT або журнали аудиту для Netware). Цей журнал необхідно переглядати не рідше ніж раз на добу або налаштувати так, щоб у разі виникнення позаштатних ситуацій адміністратор безпеки або мережі отримував оповіщення [9].

Атаки типу “відмова в обслуговуванні”. Атаки типу “відмова в обслуговуванні” (Denial of Service, DoS) є цікавим видом порушень, що призводять до тимчасового або постійного порушення функціонування компонентів ІТ системи. Прикладом таких атак є атаки WinNuke або SynFlood, суть яких полягає в надсиланні неправильно сформованих мережевих пакетів або великої кількості спеціальних пакетів, що перевантажують ресурси контролера домену, унеможливлюючи обробку інших санкціонованих запитів [9].

Атака SYN-Flood – це специфічний випадок, коли для встановлення з’єднання між вузлами мережі ПВЗ ПУ за протоколом TCP спочатку надсилається пакет з встановленим прапором SYN від одного вузла (клієнта) до іншого (сервера). Сервер відповідає пакетам з прапорами SYN і ACK. Якщо підтвердження від клієнта не надходить, сервер виділяє ресурси під з’єднання, очікуючи відповіді. У випадку атаки SYN-Flood зловмисник надсилає велику кількість SYN-пакетів без підтвердження, що призводить до перевантаження ресурсів сервера на неіснуючі з’єднання та ускладнює обробку справжніх запитів [8, 9].

Для захисту компонентів ІС від атак типу “відмова в обслуговуванні” можуть використовуватися спеціальні системи виявлення атак або міжмережеві екрани, які здатні виявляти велику кількість атак, включаючи ті, що здійснюються авторизованими користувачами. Як приклад, системи виявлення атак на рівні мережі, такі як RealSecure, встановлюються на вузлах під управлінням Windows NT або Solaris і не лише виявляють атаки, але й запобігають їх негативному впливу на функціонування елементів системи. Міжмережеві екрани також допомагають у захисті, але їхня ефективність може бути меншою порівняно з системами виявлення атак [9].

Завантаження ворожого змісту. Ворожий вміст зазвичай включає програми типу “троянський кінь”, мобільний код (Java та ActiveX), а також віруси. Зловмисники можуть використовувати такі технології, щоб реалізувати різноманітні загрози, включаючи [9]:

- Модифікацію інформації під час її передачі, обробки або зберігання.

- Порушення конфіденційності даних.

- Знищення інформації.

- Атаки типу “відмова в обслуговуванні”.

- Несанкціоноване використання ресурсів ПК.

- Запис довільних даних на локальний ПК.

- Інші дії, що призводять до роздратування користувача.

Мобільний код може бути представлений у вигляді:

- Вірусів, які вражають систему і модифікують свої коди, ускладнюючи їх виявлення.

- Агента, що перехоплює паролі.

- Програм, що копіюють конфіденційні файли.

Ці загрози часто маскуються під анімаційні банери, інтерактивні ігри, звукові файли тощо.

Мобільний код, як правило, використовується для атак типу “відмова в обслуговуванні”, які можуть здійснюватися через [9]:

- Створення високопріоритетних процесів, що виконують несанкціоновані дії.

- Генерацію великої кількості вікон.

- “Захоплення” значного обсягу пам’яті.

- Завантаження процесора нескінченним циклом.

Троянські коні. Програми типу “троянський кінь” стали широко відомими і включають більше 50 основних варіантів, які виконують різноманітні функції, починаючи від перехоплення введення з клавіатури і закінчуючи віддаленим керуванням. Основна небезпека таких програм полягає в тому, що вони діють непомітно для користувача [10].

Відомі приклади: Back Orifice та NetBus – ці програми надають можливість віддаленого адміністрування і виконують безліч шкідливих дій, часто без відома користувача.

Для запобігання атакам з використанням ворожого вмісту слід [10]:

- Використовувати антивірусні програми і системи виявлення вторгнень.

- Регулярно оновлювати ПЗ та системи безпеки.

- Застосовувати фільтрацію контенту, щоб блокувати небезпечні аплети та скрипти.

- Навчати користувачів безпечному поводженню в мережі.

Для захисту від ворожого мобільного коду існує кілька механізмів, які можуть бути впроваджені. Найбільш простим є правильна конфігурація вузлів ІС. Наприклад, заборона використання Java, ActiveX і JavaScript у браузерах на робочих станціях допоможе уникнути багатьох проблем. Регулярне оновлення ПЗ, особливо продуктів Microsoft, за допомогою патчів, гарантує, що зловмисники не зможуть скористатися вразливостями в браузерах і поштових програмах [10].

Також важливо заборонити несанкціоновані зміни системного реєстру, що запобігає запуску багатьох “троянців” на ПК. В Інтернеті є безкоштовні інструменти, які можуть виявляти і видаляти відомі “трояни”, такі як NukeNabber або TrojanCleaner [9, 10].

Додатковими засобами захисту є [10]:

- Міжмережеві екрани, які блокують використання Java і ActiveX.

- Антивірусні системи, що виявляють “троянські коні”.

- Системи контролю мобільного коду Java та ActiveX (наприклад, продукти Finjan, Security-7 Software або Digivity).

- Системи виявлення атак.

- Системи аналізу захищеності.

Таким чином, лише комплексний підхід до захисту інформаційних систем від ворожого мобільного коду, що охоплює технічні, організаційні та навчальні заходи, зможе значно знизити ризики та забезпечити безпеку ІР.

1.3. Заходи кібероборони. Форми застосування ЗС України у національному сегменті кіберпростору

Внутрішні захисні заходи в ІТС ПВЗ ПУ різних ЛУ орієнтовані на динамічне відновлення, захист, перемаршрутизацію, перебудову або ізоляцію локальних мереж з погіршеними характеристиками обслуговування або скомпрометованих мереж. Це забезпечує необхідний доступ до КП в ІТС ЗС України [2].

Успішна реалізація цих заходів можливе лише за умови якісного планування (Рисунок – 1.6.). Важливо розробити детальні плани, які враховують всі можливі загрози і варіанти реагування, що, в свою чергу, підвищує стійкість та ефективність КБ в ІТС ПВЗ ПУ [2].

Передумовою для застосування заходів реагування в рамках КБ в ІТС ПВЗ ПУ є отримання сигналів від різноманітної апаратури, зокрема сенсорів, або відповідних комплексів, що виявляють ідентифікують ознаки неминучих або поточних КА. У випадку підтвердження таких загроз, ГОЦЗІ та КБ ІТС ЗСУ (Додатки – 9, 10), а також Центри захисту інформації та кібернетичної безпеки, які діють в інтересах оперативних командувань, вживають відповідні заходи для захисту своїх військ у КП [11].

Дії супротивників, зокрема хакерських груп або цивільних осіб, можуть вимагати проведення контрзаходів, що передбачають створення впливів поза межами ІТС ЗС України. Це потребує планування наступальних кібернетичних дій (далі – КД), які полягають у виконанні неруйнівних контрзаходів для визначення джерел загрози та застосування методів, що не передбачають безпосередній вплив, з метою нейтралізації або пом’якшення загрози [11].

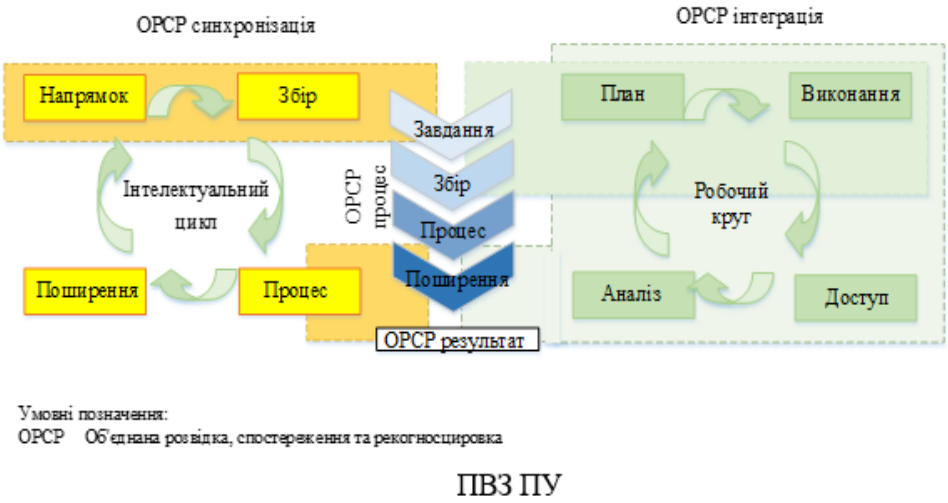


Рисунок 1.6. – Планування виконання заходів КБ в ІТС

Завдання з КБ в ІТС ПВЗ ПУ різних ЛУ ЗС України вимагають застосування різноманітних дій для створення спеціальних впливів у КП. Це передбачає активну взаємодію з іншими відомствами та установами для максимально ефективного вирішення питань, пов'язаних із Кзаг, в рамках нормативно-правового поля. Завдання з КБ в ІТС ПВЗ ПУ різних ЛУ ЗС України вимагають застосування різноманітних дій щодо створення спеціальних впливів у КП (Рисунок – 1.7.) [11].

КБ в ІТС ПВЗ ПУ різних ЛУ ЗС України є критично важливим елементом, який забезпечує захист від сучасних Кзаг. Ця система включає кілька ключових компонентів, а саме [11]:

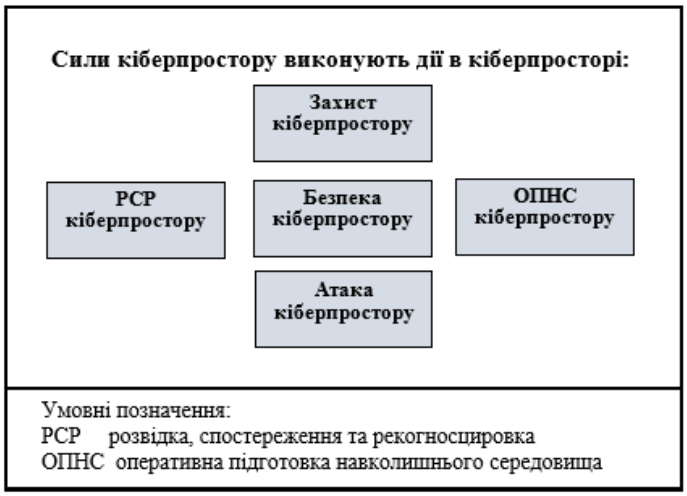


Рисунок 1.7. – Дії у кіберпросторі

1. КОб (cyberspace defense) – заходи, спрямовані на виявлення та нейтралізацію атак на ІТС, що забезпечують безпеку військових операцій.

2. Розвідка, спостереження, рекогносцирування у КП (cyberspace ISR) – збір та аналіз інформації про потенційні загрози, що допомагає у стратегічному плануванні.

3. Підготовка до проведення КО (cyberspace OPE) – навчання та тренування військових підрозділів для підвищення їхньої готовності до дій у КП.

4. ДІї у КП (cyberspace attack) – активні дії, що здійснюються з метою ураження ворожих інформаційних систем.

5. Забезпечення КБ (cyberspace security) – комплекс заходів, що охоплюють збереження цілісності, конфіденційності та доступності інформації.

Для успішного виконання завдань у сфері КБ важливо розуміти відмінності між цими компонентами та їхні конкретні цілі. Це дозволяє ефективно інтегрувати різні аспекти КБ, забезпечуючи стійкість і надійність ІТС ПВЗ ПУ під час виконання військових завдань у сучасному КП [11].

КОб в ІТС ПВЗ ПУ [12].

КОб в ІТС ПУ стратегічної ЛУ включає заходи, спрямовані на захист, використання та оборону систем від конкретних загроз у КП. Основною метою КОб є виявлення, визначення, протидія, зниження ризиків і захист інформаційних систем від загроз.

Ці оборонні заходи, як правило, виконуються ГОЦЗІ та КБ ІТС ЗСУ. Важливо зазначити, що ці дії можуть бути обмежені, якщо вони можуть вплинути на роботу мереж, які знаходяться поза межами відповідальності ІТС ЗС України.

Таким чином, КОб є критичним елементом у забезпеченні безпеки ІТС, що підтримують військові операції, і потребує постійного моніторингу та адаптації до нових загроз у КП.

Розвідка, спостереження, рекогносцирування у КП в ІТС ПВЗ ПУ.

Розвідка, спостереження та рекогносцирування в ІТС ПУ здійснюються через проведення розвідувальної діяльності, що виконується Центрами ЗІ та кібернетичної безпеки ГОЦЗІКБ ІТС ЗС України. Ці центри функціонують в інтересах оперативних командувань за територіальним принципом.

Зокрема, діють такі центри [12]:

- 3-й Центр у м. Дніпро, що обслуговує оперативне командування “Схід”;

- 7-й Центр у м. Рівне, що підтримує оперативне командування “Захід”;

- 8-й Центр у м. Одеса, що працює в інтересах оперативного командування “Південь”;

- 9-й Центр у м. Вінниця, що обслуговує командування Повітряних Сил;

- 4-й Центр у м. Чернігів, що підтримує оперативне командування “Північ”;

- 6-й Центр у м. Миколаїв, що працює на користь командування Військово-Морських Сил.

Ця мережа центрів забезпечує ефективну координацію та виконання розвідувальних завдань, що критично важливо для успішного функціонування військових операцій в умовах сучасних загроз (Рисунок – 1.8.) [12].

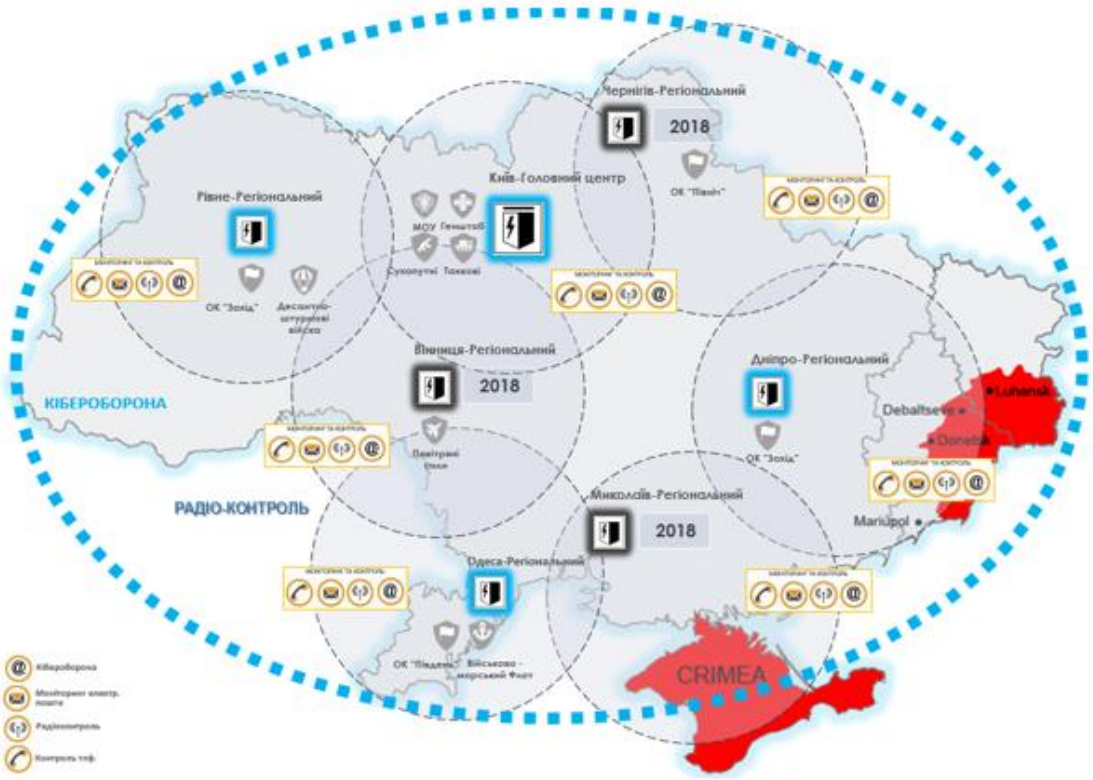


Рисунок 1.8. – Розвідка, спостереження, рекогносцирування у КП

Розвідка, спостереження та рекогносцирування в ІТС ПУ включають заходи, що проводяться в КП для збору інформації, необхідної для підтримки наступальних або оборонних КД у майбутньому. Ці заходи грають ключову роль у плануванні та реалізації поточних і майбутніх КО [12].

Основна увага під час виконання розвідки, спостереження та рекогносцирування зосереджується на [12]:

- Аналізі тактичної та оперативної ланки управління.

- “Відпрацюванні карти” сегменту КП ворогів та супротивників (mapping enemy and adversary cyberspace), що сприяє ефективному плануванню БЗ загальновійськових підрозділів.

Розвідка у КП (cyberspace ISR) вимагає належних повноважень і вирішення спірних питань з організації взаємодії. Вона проводиться в рамках відповідних повноважень щодо здійснення військової діяльності та повинна враховувати аспекти координації та співпраці з іншими учасниками сектору безпеки та оборони, а також організаціями, що займаються відповідними

питаннями. Це забезпечить ефективність спільних дій воєнного характеру [12].

Підготовка до проведення КО [13].

Підготовка до проведення КО (cyberspace OPE) здійснюється в рамках відповідних повноважень, що регулюють військову діяльність у цій сфері. Основною метою підготовки є дезорганізація СУ противника та створення умов для ефективного виконання КО [12, 13].

Цей процес включає врахування аспектів координації та вирішення спірних питань, пов'язаних із організацією взаємодії між різними учасниками, такими як, військові формування та правоохоронні органи, суб'єками сектору безпеки та оборони, включаючи органи державної влади (далі – ОДВ) та приватним сектором, зокрема DATA-групи, CERT, центри КБ різних форм власності та провайдери зв'язку [13].

Підготовка також охоплює нерозвідувальні заходи, що сприяють плануванню організаційно-структурних підрозділів (ОВУ) для підготовки БЗ військових частин у найближчому майбутньому. Це забезпечує всебічну готовність до виконання запланованих КО.

Дії у КП [13].

Дії у КП можуть призводити до різних очевидних обмежуючих наслідків, таких як погіршення, дезорганізація, виведення з ладу, порушення або знищення інформаційних систем. Це може впливати на фізичні сфери ведення БД, проявляючись у прихованих обмеженнях або безпосередніх наслідках.

Основною метою атак у КП є проекція сили для забезпечення БД власних військ, здобуття переваги в КС або фізичних сферах БД. Наприклад, атака може бути націлена на інформацію, що обмінюється між ПУ вищого штабу та підпорядкованих командирів чи начальників. Такі дії спрямовані на недопущення використання відповідних ресурсів ворогами або ворожими суб'єктами, що суттєво впливає на оперативні можливості противника [13].

Забезпечення КБ в захищеній ІТС ПВЗ ПУ різних ЛУ ЗС України.

Це дії, що виконуються в захищеній ІТС з метою недопущення НСД до, використання, або пошкодження комп'ютерів, систем електронного зв'язку, а також інших комп'ютерних систем ПВЗ ПУ різних ЛУ ЗС України, включаючи спеціалізовані комп'ютерні системи та наявну в них інформацію, для забезпечення її доступності, цілісності, автентифікації, конфіденційності, та достовірності. Аспект забезпечення КБ не має прив'язки до ворогів та супротивників. Заходи з забезпечення КБ спрямовані на захист мереж і систем на всіх етапах планування та побудови мереж. До забезпечення КБ відносяться оцінка та аналіз вразливостей (vulnerability assessment and analysis), реагування на вразливості (vulnerability management), обробка інцидентів (incident handling), постійний моніторинг, а також засоби виявлення та відновлення для забезпечення захисту та збереження інформації та інформаційних систем [13].

Дії з КБ в ІТС ПВЗ різних ЛУ, що здійснюються в КП або через нього, мають наслідки в КП ІТС ЗС України. Впливи можуть здійснюватися шляхом або за допомогою проведення наступальних КО або заходів з реагування в рамках оборонних КО. Зазначені впливи сприяють проведенню операцій в цілому та досягненню цілей командуючого (ОУВ, ОТУ). Підрозділи проведення КО (cyber mission forces), що здійснюють дії у КП, забезпечують реалізацію впливів у КП та через КП [13].

Дії з КБ в ІТС ПВЗ різних ЛУ вимагають проведення різних прямих обмежуючих впливів у КП, а саме: погіршення (degradation), дезорганізації, виведення з ладу, порушення (disruption), або знищення (destruction). Слід зазначити, що маніпулювання (manipulation) призводить до обмеження (denial) прихованого або явного у будь-якій сфері ведення БД [12, 13].

Зазначеними конкретними діями є [13]:

- Обмеження (deny), погіршення (degrade), дезорганізація, виведення з ладу, порушення (disrupt), або відключення – доступу до, функціонування, або доступність ПВЗ ПУ різних ЛУ на визначений рівень протягом

визначеного часу. Обмеження перешкоджає ворогу або супротивникам використовувати ресурси.

- Погіршення (degrade), обмеження доступу (функція кількості) до, або функціонування об'єкта до рівня представленого у відсотках від загальної спроможності. Рівень погіршення має визначатись. Якщо є необхідність у певному часі, він може не визначатись.

- Дезорганізація, виведення з ладу, порушення (disrupt). Повністю або тимчасове обмеження (функція часу) доступу до, або функціонування ПВЗ ПУ різних ЛУ протягом певного періоду часу. Бажаний час початку та завершення (зупинки, паузи) зазвичай вказуються. Дезорганізація, виведення з ладу, порушення (disruption) можуть розглядатися як особливий випадок погіршення (degradation), коли погіршення визначається на рівні 100 відсотків.

- Знищення (destroy). На весь час, повністю, та незворотне обмеження (час і обсяг максимізуються) доступу, або функціонування ПВЗ ПУ різних ЛУ.

- Маніпулювання (manipulate). Контроль та внесення змін до інформації, інформаційних систем та/або мереж ворогів або противників у відповідності до цілей командувача (старшого начальника).

- Обмежуючі заходи (denial operations) – заходи щодо перешкоджання або обмеження використання противником місцевості, особового складу, всебічного (логістичного) забезпечення, приміщень, обладнання. Прикладом реалізації впливу "обмеження" є використання спроможностей у сфері РЕБ для радіоелектронного подавлення конкретних частот протягом попередньо визначеного періоду часу, або блокування порта передачі даних маршрутизатора протягом попередньо визначеного періоду часу використовуючи спроможності у КП; однак, тривалість обмеження (denial) залежатиме від здатності ворога здійснити відновлення.

- Погіршення (degrade) – застосування засобів нелетального або тимчасового впливу для зменшення результативності або ефективності

систем УВ (силами) противника та його засобів та зусиль щодо накопичення і обробки інформації. Прикладом реалізації впливу “погіршення” (degrade) є уповільнення швидкості з’єднання у КП, впливаючої на можливість ефективно спілкуватися або своєчасно передавати дані.

- Дезорганізація, виведення з ладу, порушення (disrupt) – тактичне завдання в рамках якого командир (начальник) інтегрує ведення вогню прямою або непрямою наводкою (direct and indirect fires), особливості місцевості та наявність перешкод з метою внесення розладу в бойовий порядок ворога або зниження швидкості його просування, порушення його запланованих дій, або примушення ворога здійснити передчасну атаку або атакувати розрізненими силами. Заважаючий вплив, шляхом планування нанесення вогневого ураження та створення штучних перешкод, з метою дезорганізації бойового порядку ворога та зниження швидкості його пересування, порушення його запланованих дій, передчасного введення в бій його підрозділів, та атаки розрізненими силами. Прикладом реалізації впливу “дезорганізація, виведення з ладу, порушення” (disrupt) є переривання з’єднання у КП, дротового або бездротового, впливаючого на можливість спілкування або передачі даних між ПВЗ ПУ різних ЛУ.

- Знищення (destroy) – тактичне завдання, що полягає у фізичному виведенні з боєздатного стану сил противника до моменту завершення їх відновлення. В іншому випадку, знищити бойову систему означає завдати їй настільки сильного ураження, що виконання нею будь-яких функцій або відновлення працездатності є неможливими без цілковитого створення цієї бойової системи заново. Знищення (destroy) – це застосування летальних бойових спроможностей проти противника для усунення можливості виконання ним будь-яких бойових завдань, функцій. Противником не може бути відновлено працездатність своїх засобів без цілковитого створення їх заново. Прикладом реалізації впливу “знищення” (destroy), використовуючи спроможності у КП, є спричинення втрати системою всієї інформації, яка в

ній циркулює, або спричинення перегріву цієї системи до моменту втрати її подальшої працездатності.

- Маніпулюваня (manipulate) – контроль або внесення зміни до інформації, інформаційних систем та/або мереж противника у відповідності до цілей командира (начальника).

- Виконання заходів, щодо введення противника в оману (deceive) – спроби військового керівництва направити керівництво сторони, від якої надходить загроза, по невірному шляху при прийнятті рішень маніпулюючи їх сприйняттям реальності. Прикладом реалізації впливу “введення в оману” (deceive) є внесення змін до повідомлення, що, як наслідок, спричинило дислокацію противника у місці, яке попередньо не було визначене його власною вертикаллю управління.

Впливи в КП та через нього можуть мати такі ж самі наслідки, як і інші види традиційних впливів. Впливи під час операцій включають летальні та нелетальні дії та можуть бути прямими або непрямими. Прямі впливи є наслідками першого порядку, непрямі впливи є наслідками другого, третього або вищого порядку. Подібні характеристики прямих та непрямих впливів у КП можуть бути кумулятивними або каскадними, за необхідності. Ці впливи плануються та контролюються відповідно до цілей командуючого. Кумулятивність відноситься до сукупності ефектів, а каскадність відноситься до ефекту “ланцюгової реакції” внаслідок впливу на інші системи. Результати здійснення відповідних впливів у КП можуть сприяти проведенню операцій, будучи ще одним шляхом досягнення сприятливої оперативної обстановки спрямованим на забезпечення переваги.

РОЗДІЛ 2
РОЗРОБКА ПЕРСПЕКТИВНИХ СХЕМ РОЗГОРТАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ІТС ПВЗ ТАКТИЧНОЇ, ОПЕРАТИВНОЇ ТА СТРАТЕГІЧНОЇ ЛАНОК УПРАВЛІННЯ ЗС УКРАЇНИ

2.1. Типові схеми розгортання системи кібербезпеки в ІТС ПВЗ тактичної, оперативної та стратегічної ланок управління ЗС України.

Типові схеми розгортання СКБ в ІТС ПВЗ для тактичної, оперативної та стратегічної ЛУ ЗС України представлені на рисунку 2.1. Детальніше розглянуто загальну схему на рисунку 2.2. на прикладі ІТС ПУ тактичної ЛУ.

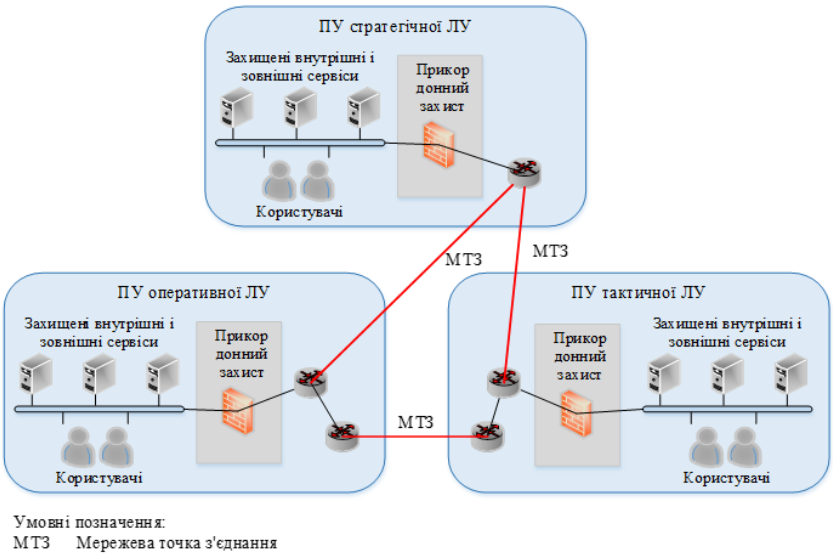


Рисунок 2.1. – Схема розгортання КБ в ІТС ПВЗ тактичної, оперативної та стратегічної ЛУ ЗС України

Стійке функціонування СКБ в ІТС ПВЗ оперативної ЛУ ЗС України, яке наведено як варіант у кваліфікаційній роботі, досягається через узгоджене функціонування обладнання та ПЗ на ПВЗ різних ЛУ, що входять до її складу. Загальна вимога до обладнання, яке буде розгорнуто на ПВЗ, полягає в тому, що комплекси КБ мають формувати збалансований та взаємодіючий комплект засобів управління інфраструктурою КБ в

інформаційно-технічних системах (далі – ІТехС) Міністерства оборони України та ЗС України на стратегічному, оперативному та тактичному рівнях [14].

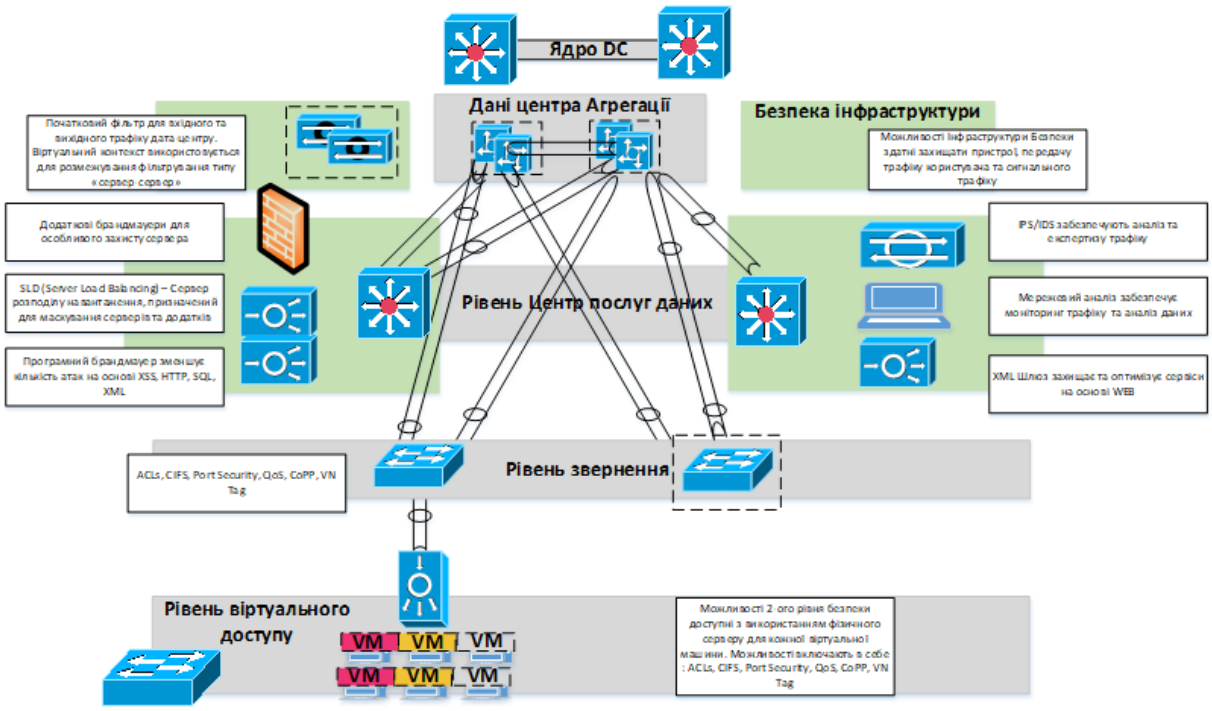


Рисунок 2.2. – Типова схема розгортання КБ в ІТС ПВЗ тактичної ланки управління ЗС України

Отже, остаточний варіант схем розгортання СКБ в ІТС ПВЗ для всіх ЛУ ЗС України буде представлений після завершення переведення ОВУ на структури штабів військ НАТО та вдосконалення організаційної структури УВ через перехід на моделі типу J, G, A, N.

Висвітлений варіант схем розгортання СКБ в ІТС ПВЗ для тактичної, оперативної та стратегічної ЛУ ЗС України є формалізованим і відкриває можливості для подальших досліджень у цій сфері БЗ [14].

Оскільки час не стоїть на місці, розвиток ІТС ЗС України вимагає сучасних підходів до КБ, особливо в умовах активних БД на території нашої країни. Проте, поступовий перехід, переоснащення, зміна топології мережі та удосконалення організаційної структури УВ уповільнюють цей процес. У зв’язку з цим важливо розглянути окремі складові та елементи типових схем розгортання СКБ, а також детально зупинитися на реалізації послідовності

правил впровадження, які можуть суттєво поліпшити функціонування мережі ПВЗ. Серед цих елементів можна виділити [14]:

а) міжмережеві екрани;

б) технології віртуальних приватних мереж;

в) інфраструктуру відкритих ключів.

Міжмережеві екрани. Однією з основних задач міжмережевих екранів в ІТС ПВЗ (Рисунок – 2.3.) для будь-якої ЛУ є захист мережевих сегментів або окремих хостів від НСД, зокрема через вразливості в протоколах мережевої моделі OSI або ПЗ на ПК. Міжмережеві екрани аналізують трафік, порівнюючи його характеристики з попередньо визначеними шаблонами, що дозволяє пропускати або блокувати дані в залежності від встановлених правил [15].

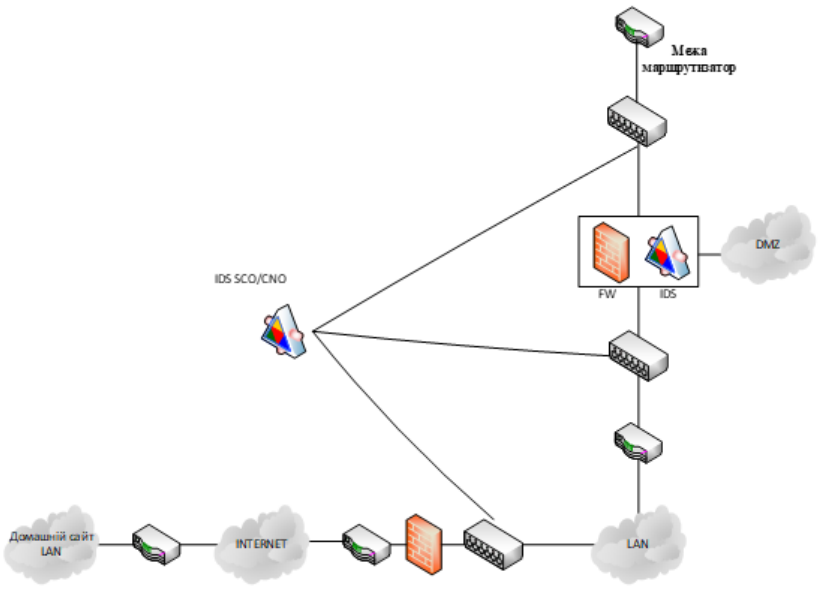


Рисунок 2.3. – Міжмережеві екрани в ІТС ПВЗ РУ

Найбільш поширеним місцем для встановлення міжмережевих екранів є межа периметра локальної мережі, що дозволяє захистити внутрішні хости від зовнішніх атак. Проте важливо враховувати, що атаки можуть починатися і з внутрішніх вузлів ІТехС. У таких випадках, якщо атакований хост знаходиться в тій же мережі, трафік не перетне межу мережевого периметра, і міжмережевий екран не зможе виконати свою функцію [15]. Тому доцільно

розміщувати міжмережеві екрани не лише на кордоні, а й між різними сегментами мережі, що створює додатковий рівень безпеки.

Фільтрація трафіку в міжмережевих екранах відбувається на основі набору попередньо налаштованих правил, відомих як ruleset. Уявляти міжмережевий екран можна як послідовність фільтрів, кожен з яких обробляє інформаційний потік відповідно до конкретного правила. Послідовність цих правил має значний вплив на продуктивність брандмауера [15]. Наприклад, міжмережеві екрани порівнюють трафік з правилами до тих пір, поки не знайдуть відповідність. Тому правила, що відповідають найбільшій кількості трафіку, слід розміщувати якомога вище в списку, що дозволяє підвищити продуктивність.

У ІТехС ПВЗ ПУ діють два принципи обробки вхідного трафіку. Перший принцип – “Що явно не заборонено, те дозволено”, означає, що якщо міжмережевий екран отримує пакет, який не відповідає жодному правилу, він передається далі. Протилежний принцип – “Що явно не дозволено, те заборонено” – забезпечує більшу безпеку, оскільки забороняє весь трафік, який не дозволений правилами. Однак цей підхід створює додаткове навантаження на адміністратора мережі ПВЗ ПУ [14, 15].

У підсумку міжмережеві екрани виконують одну з двох основних операцій: або пропускають пакет далі (allow), або відкидають його (deny). Деякі міжмережеві екрани також реалізують операцію reject, при якій пакет відкидається, але відправнику надсилається повідомлення про недоступність запитуваного сервісу. У випадку deny, відправник не отримує жодної інформації, що робить цей метод більш безпечним [15].

На сьогоднішній день не існує єдиної класифікації міжмережевих екранів, проте в багатьох країнах їх класифікують за рівнем підтримуваної моделі OSI. Виходячи з цієї моделі, можна виділити такі типи міжмережевих екранів, які можна використовувати в ІТехС ЗС України [16]:

1. Керовані комутатори.

2. Пакетні фільтри.

3. Шлюзи сеансового рівня.

4. Посередники прикладного рівня.

5. Інспектори стану.

Існують два основні варіанти реалізації міжмережевих екранів: програмний і програмно-апаратний. Останній може бути реалізований як окремий модуль у комутаторі або маршрутизаторі, або у вигляді спеціалізованого пристрою.

На сьогоднішній день в ІТехС ПВЗ ПУ зазвичай застосовують програмні рішення, які на перший погляд виглядають зручніше. Це пояснюється тим, що для їх реалізації достатньо придбати програму захисту мережі і встановити її на будь-який ПК у мережі. Однак на практиці вільних ПК може не виявитися, а ті, що є, часто не відповідають вимогам за системними ресурсами. Якщо ж ПК знайдено, потрібно провести налаштування ОС та брандмауера. Виявляється, що використання звичайного ПК є значно складнішим, ніж це здається спочатку [16].

Тому все частіше набувають популярності спеціалізовані програмно-апаратні комплекси, звані security appliance, які зазвичай базуються на системах FreeBSD або Linux, оптимізованих для виконання лише необхідних функцій. Переваги таких рішень включають [16]:

- Простоту впровадження: ці пристрої постачаються з уже налаштованою ОС, що потребує мінімальних налаштувань під час інтеграції в мережу.

- Легкість управління: ними можна керувати з будь-якої точки (на різних рівнях управління) через стандартні протоколи, такі як SNMP або Telnet, а також через захищені протоколи, такі як SSH або SSL.

- Високу продуктивність: ці пристрої працюють ефективніше, оскільки з їх ОС виключені всі непотрібні сервіси.

- Надійність та високу доступність: вони створені для виконання конкретних завдань з високою доступністю.

2.2. Застосування технології віртуальних приватних мереж на ПВЗ ПУ різних ланок управління ЗС України

Технологія віртуальних приватних мереж. Адміністратори мереж, розгорнутих на ПВЗ ПУ різних ЛУ ЗС України, часто бачать у VPN ефективний засіб забезпечення КБ. Проте на практиці реалізація цієї технології може виявитися більш складною, ніж очікувалося. Після впровадження VPN часто виявляються особливості, які не були враховані раніше, і які можуть суттєво вплинути на сталу роботу мережі [17].

Основними завданнями цього розділу є вивчення проблем, що виникають після впровадження VPN, та надання рекомендацій щодо вибору оптимальних рішень. Реалізація КБ в ІТС ПВЗ ПУ через VPN (Рисунок 2.4).

Суть технології. Принцип роботи віртуальних приватних мереж полягає в тунелюванні трафіку через телекомунікаційні мережі, такі як мережа ЗС України або Інтернет. Реалізація технології здійснюється за допомогою спеціальних пристроїв – кріптошлюзів. Ці пристрої не лише забезпечують захист локальної мережі від зовнішніх загроз, але й здійснюють маршрутизацію трафіку. VPN відрізняється від традиційних рішень на основі виділених каналів завдяки своїй гнучкості, масштабованості та нижчій вартості, а також високому рівню ЗІ [17].

ІТехС ЗС України швидко розвиваються, і пристрої VPN пропонуються майже всіма великими виробниками телекомунікаційного обладнання. Однак впровадження віртуальних мереж має свої особливості.

Оцінка ступеня впливу [17]. Коли віртуальні мережі функціонують, кріптошлюзи здійснюють перетворення трафіку, внаслідок чого багато характеристик роботи мережі можуть погіршитися з точки зору кінцевого користувача. Інтеграція VPN може призвести до таких змін у роботі мережі:

- Зниження пропускної здатності мережі.
- Накладні витрати на перетворення трафіку.
- Затримки при передачі пакетів.

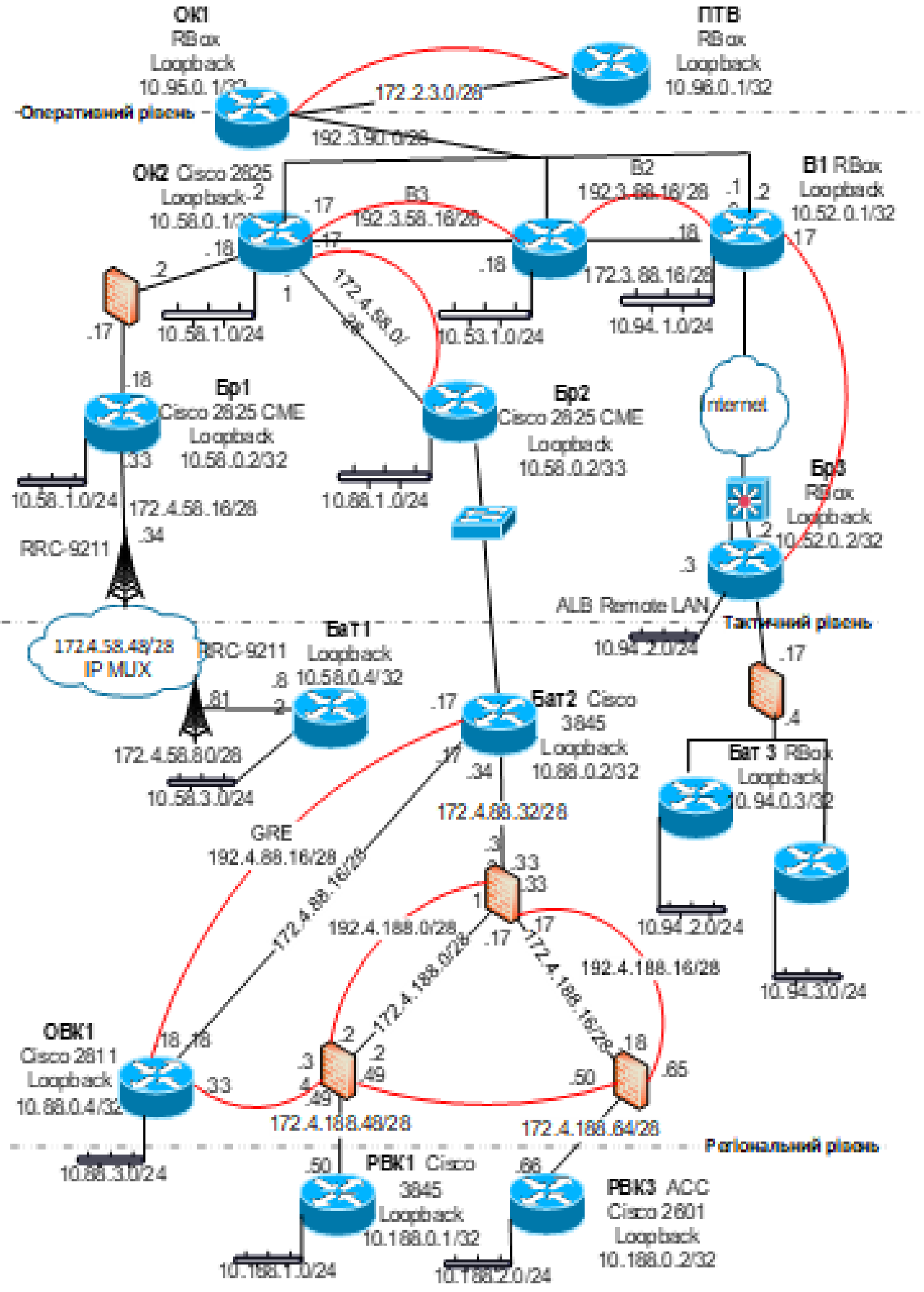


Рисунок 2.4. – Реалізація КБ в ІТС ПВЗ ПУ через VPN

Зниження пропускної здатності може виникати з різних причин. Одна з них – недостатня продуктивність самого кріптошлюза. Хоча зазвичай при виборі таких пристроїв цьому параметру надається велике значення, важливо, щоб VPN-пристрої мали достатню пропускну здатність для мінімізації їхнього впливу на передачу інформації в мережі [18].

Друга причина зниження пропускної здатності мережі пов’язана з типом трафіку та накладними витратами на його обробку. Ці витрати виникають внаслідок додавання нового IP-заголовка до тунельованого пакета, що залежить від обраного протоколу. Наприклад, протокол IPsec додає мінімум 54 байта до пакета. Для стандартного IP-пакета обсягом 1500 байт приріст складе близько 4%, тоді як для пакета обсягом 56 байт (наприклад, в IP-телефонії) накладні витрати можуть досягати 100% [18].

Виробники з Російської Федерації пропонують власні протоколи, такі як протокол шифрування “Континент-К”, які зазвичай мають менше недоліків у порівнянні з IPsec, знижуючи приріст довжини пакета і часто впроваджуючи стиснення заголовків [18].

Затримки при передачі пакетів можуть бути спричинені багатьма факторами. Хоча VPN може відігравати певну роль, затримки також залежать від роботи різних вузлів мережі, зокрема вузлів доступу до Інтернету та шлюзів між провайдерами. Пристрої VPN можуть викликати два типи затримок: пряму, що обумовлена часом обробки пакета, і непряму, яка виникає через збільшення трафіку внаслідок накладних витрат при тунелюванні [18].

Рекомендації при виборі VPN. При виборі VPN важливо враховувати вплив на існуючу інфраструктуру ІТехС ЗС України. Перед проектуванням VPN слід ретельно оцінити, як ця технологія вплине на вже діючі або плановані сервіси, особливо в контексті систем збору технологічних параметрів і диспетчерського управління, де критично важливі тимчасові затримки [18].

Інший важливий приклад – IP-телефонія. Незважаючи на початковий скепсис, ця технологія активно розвивається в ІТС ЗС України. При інтеграції VPN в мережу з короткими пакетами (наприклад, 56 байт для IP-телефонії) накладні витрати можуть суттєво знижувати пропускну здатність. Для протоколу IPsec, наприклад, розмір пакета може збільшитися більше ніж на 100% [18, 19].

Проблеми, пов’язані з впровадженням VPN, можна вирішити двома шляхами. Перший варіант – збільшення пропускної здатності каналу. Це може усунути багато проблем, але витрати на оренду можуть зрости вдвічі. Другий варіант – вибір протоколів з мінімальними накладними витратами на тунелювання, при цьому інші параметри VPN-обладнання повинні відповідати вимогам користувача [19].

Функціонування ІТС після інтеграції VPN не обмежується лише етапом установки. Важливо враховувати концепцію роботи системи, зокрема вибір протоколів та алгоритмів шифрування, оскільки це впливає на безпеку та зручність управління мережею. Пошук компромісу між безпекою і зручністю експлуатації є критично важливим [19].

Крім того, необхідно враховувати, як мережа реагує на аварійні ситуації. Важливо, щоб кріптошлюзи, особливо в тактичній ЛУ, були надійними і легкими в обслуговуванні. Деякі пристрої можуть вимагати введення ключової інформації для відновлення з’єднання після перезавантаження, що може призвести до тривалих відключень сегмента VPN та втрат у роботі додатків [19].

Отже, ретельне планування і врахування всіх цих факторів підвищать ефективність впровадження VPN у мережу ЗС України.

2.3. Розгортання інфраструктури відкритих ключів (PKI)

Інфраструктура відкритих ключів (PKI) (Рисунок – 2.5.) являє собою комплекс засобів – технічних, матеріальних та людських — а також

розподілених служб і компонентів, які використовуються для забезпечення криптографічних задач на основі закритих і відкритих ключів. Ця система підтримує безпечний обмін інформацією, аутентифікацію користувачів та забезпечує цілісність даних [20].

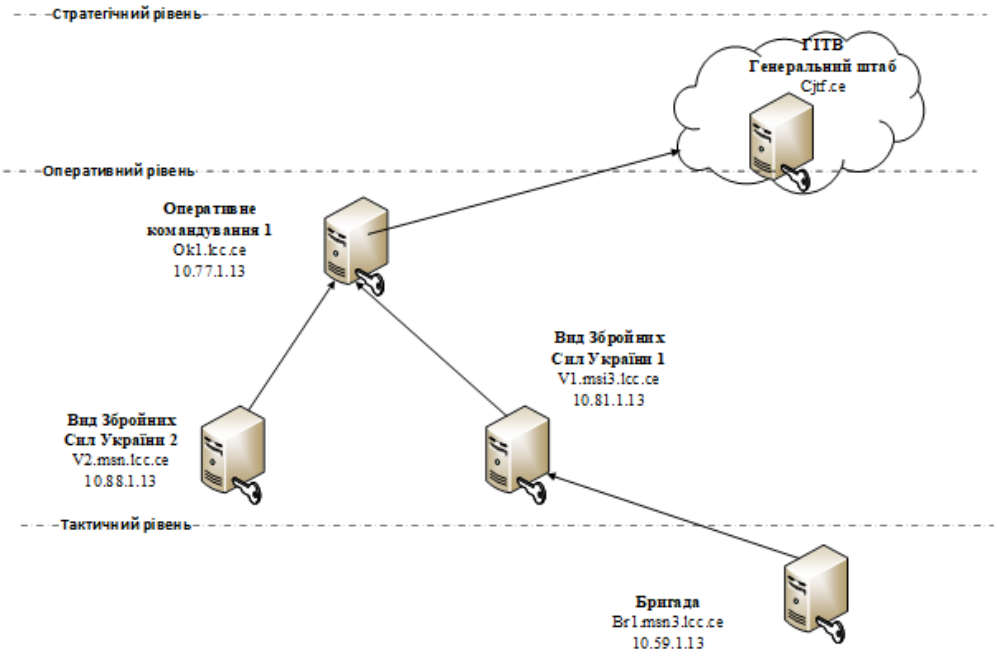


Рисунок 2.5. – Інфраструктура відкритих ключів системи КБ в ІТС ПВЗ ПУ різних ЛУ

В основі інфраструктури відкритих ключів (PKI) лежить використання криптографічної системи з відкритим ключем, що базується на кількох основних принципах [20]:

1. Закритий ключ (private key) відомий лише його власнику.

2. Сертифікат відкритого ключа підтверджує, що закритий (секретний) ключ належить тільки його власнику, тоді як відкритий ключ (public key) вільно передається в сертифікаті.

3. Довіра між сторонами не є автоматичною; всі довіряють лише засвідчувальному центру.

4. Засвідчувальний центр (CA) підтверджує або спростовує належність відкритого ключа певній особі, яка має відповідний закритий ключ.

Основні завдання СКБ в ІТС ПВЗ ПУ, які реалізує PKI, включають:

- Забезпечення конфіденційності інформації.

- Гарантія цілісності даних.

- Аутентифікація користувачів і ресурсів, до яких вони звертаються.

- Можливість підтвердження дій користувачів з інформацією.

PKI складається з кількох ключових компонентів, основним з яких є перевірка ідентичності користувачів через засвідчувальний центр. Обмін інформацією між центром і користувачами відбувається за допомогою сертифікатів. Функціонування PKI базується на регламенті системи та принципах криптографії з відкритим ключем. До складу інфраструктури входять центр сертифікації (засвідчувальний центр), кінцеві користувачі, а також додаткові елементи, такі як центр реєстрації і мережевий довідник [20].

Основні функції PKI включають [20]:

- Перевірку особистості користувачів, які звертаються за сертифікатами.

- Видачу сертифікатів користувачам.

- Анулювання сертифікатів у разі потреби.

- Ведення та публікацію списків відкликаних сертифікатів (Certificate Revocation List / CRL), які допомагають клієнтам ухвалювати рішення про довіру до сертифікатів.

Додаткові функції засвідчувального центру (ЗЦ) [20]:

- Генерація пар ключів, один з яких включається в сертифікат.

- Перевірка достовірності електронного підпису власника сертифіката за запитом, особливо у випадках конфліктів.

Сертифікат є електронним документом, що містить відкритий ключ користувача, дані про власника, електронний підпис центру сертифікації, термін дії сертифіката та інші атрибути. Він не може бути безстроковим і завжди включає дату початку та завершення дії [20].

Основні причини дострокового анулювання сертифікатів [20]:

- Компрометація закритого ключа.

- Зміна інформації про власника сертифіката.

- Добровільне прохання власника сертифіката.

- Зміна повноважень власника сертифіката.

Ключова пара складається з двох ключів: закритого (private key) і відкритого (public key). Ці ключі створюються разом і є комплементарними. Інформацію, зашифровану відкритим ключем, можна розшифрувати тільки за допомогою закритого ключа. Водночас електронний підпис, створений за допомогою закритого ключа, можна перевірити, використовуючи відкритий ключ [21].

Ключова пара може бути створена або центром видачі сертифікатів (засвідчувальним центром) на запит користувача, або самим користувачем за допомогою спеціального ПЗ. Після ідентифікації користувача, ЗЦ видає сертифікат, підписаний цим центром, підтверджуючи його легітимність [21].

Відкритий ключ є доступним для всіх, тоді як закритий ключ зберігається в таємниці. Власник закритого ключа зобов'язаний оберігати його від зловмисників. Якщо закритий ключ стає відомим стороннім, він вважається скомпрометованим, і сертифікат, пов'язаний із ним, має бути відкликаний. Тільки власник закритого ключа має можливість підписувати дані та розшифровувати інформацію, зашифровану відкритим ключем [21].

Дійсний електронний підпис підтверджує авторство даних і їх цілісність під час передачі, а підпис коду гарантує, що ПЗ не містить шкідливого коду. Закритий ключ використовується для підпису даних, а також для розшифрування інформації, отриманої від інших учасників PKI. Відкритий ключ з сертифіката іншого учасника може бути використаний для перевірки електронного підпису та шифрування інформації, яку планується надіслати [21].

Варто зазначити, що процес шифрування асиметричними алгоритмами є повільнішим у порівнянні з симетричними, тому його зазвичай не застосовують для шифрування великих обсягів даних.

Сертифікати відкритих ключів використовуються для встановлення захищеного зв'язку з веб-сайтами, такими як інтернет-магазини або банки, тоді як для подальшого обміну даними зазвичай використовуються симетричні ключі [20, 21].

Одним із ключових елементів інфраструктури відкритих ключів (ІВК) є електронний підпис, який представляє собою результат використання алгоритму підпису на хеш даних (документів, повідомлень або файлів).

Перевірка справжності електронного підпису відбувається за наступними етапами [22]:

1. Одержувач отримує дані (в зашифрованому або відкритому вигляді) разом із електронним підписом.

2. Дані розшифровуються або за допомогою узгодженого симетричного ключа, або закритого ключа одержувача (якщо дані були зашифровані його відкритим ключем).

3. Одержувач обчислює хеш розшифрованого документа (алгоритм хешування зазначений у сертифікаті).

4. З електронного підпису застосовується алгоритм зняття підпису (вказаний у сертифікаті), що дозволяє отримати хеш вихідного документа.

5. Одержувач порівнює отримані хеші: якщо вони збігаються, електронний підпис вважається дійсним, за умови, що сертифікат активний і використаний згідно з його політиками.

Серед застосувань, що підтримують PKI, можна виділити: захищену електронну пошту, платіжні протоколи, електронні чеки, електронний обмін інформацією, захист даних у мережах з протоколом IP, а також електронні документи з цифровим підписом [20-22].

У зв'язку з цим, під час розробки та впровадження СКБ в ІТС ПВЗ ПУ різних логістичних управлінь ЗС України важливо врахувати використання ПЗ розподілених підсистем (далі – РП) для забезпечення заходів кіберрозвідки (далі – КР), КЗ та КО, а також КОб під час спільних дій ЗС України, ІвФ та ПрО в умовах воєнного стану та в особливий період [20-22] .

РОЗДІЛ 3
РОЗРОБКА ПРОЕКТІВ ОПЕРАТИВНО-ТАКТИЧНИХ ВИМОГ ДО СИСТЕМ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ІТС ПВЗ ПУ РІЗНИХ ЛАНОК УПРАВЛІННЯ ЗС УКРАЇНИ

3.1 Розробка проекту оперативно-тактичних вимог до систем кібернетичної безпеки в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ланок управління ЗС України

Цільове призначення: СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України.

Основні завдання обладнання: СКБ розгорнутого в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України повинно утворювати поєднання єдиної технічної СКБ в рамках сталого функціонування СУ ЗС України та реалізовувати виконання комплексу технічних заходів із КР, КЗ, контролю КБ і здійснення дій у КП на всіх рівнях управління [23].

СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України повинна забезпечувати безперервний, стійкий, якісний, КЗ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України.

Склад СКБ в ІТС ПВЗ ПУ стратегічної, оперативної та тактичної ЛУ ЗС України.

Склад СКБ в ІТС ПВЗ ПУ стратегічної ЛУ ЗС України стратегічної, оперативної та тактичної ЛУ ЗС України [23]:

- підсистема КЗ периметру Додаток 1 (Таблиця 1);

- підсистема відображення обстановки та керування інфраструктурою КБ в ІТС СКБ в ІТС ПВЗ ПУ стратегічної, оперативної та тактичної ЛУ ЗС України з підтримкою віртуалізації Додаток 2 (Таблиця 2);

- сервер КЗ Додаток 3 (Таблиця 3);

- підсистема комутації Додаток 4 (Таблиця 4);

- джерело безперебійного живлення UPS 220V, 50Hz, 1000VA, 19” вбудовуємий Додаток 5 (Таблиця 5);

- монтажний кейс на 19”, 6U Додаток 6 (Таблиця 6).

В цілому склад СКБ в ІТС ПВЗ ПУ різних ЛУ ЗС України розроблений за функціональними завданнями, як самостійно, так і у складі кожної ЛУ.

Сукупність складових СКБ в ІТС ПВЗ ПУ стратегічної, оперативної та тактичної ЛУ ЗС України, якісних характеристик та кількісних показників за яких забезпечується виконання завдань які покладаються на ЗС України може змінюватись з врахуванням розвитку та модернізації озброєння та військової техніки, що визначається від моменту розробки ОТВ до моменту постачання зразка (комплекса, системи) та погоджуються із заінтересованими структурними підрозділами ГШ ЗСУ (Замовником проекту)[24].

В розробленому проекті оперативно-тактичних вимог до СКБ ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України кількісні та якісні показники запропоновані, як варіант СКБ в ІТС ПВЗ ПУ стратегічної, оперативної та тактичної ЛУ ЗС України за умов оптимізації та послідовного переведення ОВУ, як складової СУ, на структури штабів військ НАТО, переоснащення та нарощування системи зв’язку [24].

Розроблений варіант спрямований на посилення спроможностей складових СКБ в ІТС ПВЗ ПУ різних ЛУ ЗС України, що до [25]:

- забезпечення захищеності КП та створення сталого цифрового комунікативного середовища, своєчасного виявлення, запобігання і нейтралізації реальних і потенційних загроз в ІТС під час надання інформаційно-телекомунікаційних сервісів на ПУ польових (стаціонарних) умовах;

- реагування на інциденти КБ та КА в ІТС ПВЗ ПУ;

- запобігання можливому витоку інформації, що циркулює в ІТС ПВЗ ПУ;

- збору, аналізу та обробки журналів подій із засобів забезпечення КБ, мережевих пристроїв, автоматизованих робочих місць (далі – АРМ) в ІТС ПВЗ ПУ, підключених до ІТС ЗС України та, з метою виявлення КА, інцидентів КБ, передумов та випадків витоку інформації;

- накопичення інформації про інциденти КБ та КА з метою її аналізу та подальшого використання для своєчасного реагування на загрози інформації, що обробляється в ІТС МО України та ЗС України (на ПУ різних ЛУ в польових (стаціонарних) умовах).

3.1.1. Основні бойові завдання СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ланок управління ЗС України. Основні бойові завдання СКБ ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України [26]:

- налаштування політик КБ СКБ в ІТС ПВЗ ПУ на всіх рівнях управління ЗС України;

- реалізація політик КБ СКБ в ІТС ПВЗ ПУ;

- контроль за засобами КБ СКБ ІТС ПВЗ ПУ;

- ефективне запобігання Кзаг та кібервтручанням в ІТС ПВЗ ПУ військових частин та підрозділів ЗС України;

- контроль за файлами, протоколами, вузлами, додатками та кібернетичними інцидентами безпеки в ІТС ПВЗ ПУ всіх ЛУ ЗС України, ІТС ПВЗ ПУ військових частин та підрозділів, приданих та взаємодіючих військ;

- захист ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України від дій шкідливого ПЗ;

- відстеження, ізоляція та знешкодження заражених об’єктів в ІТС ПВЗ ПУ на всіх рівнях управління ЗС України;

- реалізація ефективного фільтрування інформаційного потоку, управління обігом пакетів, контролем за додатками, користувачами та адміністраторами мереж ІТС ПВЗ ПУ ЗС України;

- організація постійного моніторингу трафіку та стану безпеки КП ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України;

- унеможливлення реалізації противником плану позбавлення ресурсів та блокування в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України за допомогою атак типу “відмова в обслуговуванні” (DoS або DDoS);

- забезпечення захисту конфігурації засобів ІТС ПВЗ ПУ всіх ЛУ ЗС України від загроз пов’язаних з помилками в конфігурації та налаштуваннях телекомунікаційного обладнання;

- контроль за ліцензіями та оновленнями ОС, додатків, BIOS, резервними копіями налаштувань телекомунікаційних засобів та засобів КБ в ІТС ПВЗ ПУ органів управління (далі – ОУ), військових частин та підрозділів ЗС України;

- захист ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України від НСД до інформації;

- боротьба проти застосування противником заходів “соціальної інженерії” до особового складу підрозділів зв’язку, користувачів та адміністраторів ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України;

- можливість проводити необхідні КД та КО в визначених соціальних мережах та зовнішніх секторах КП;

- контроль за наявністю визначеного наказами та інструкціями переліку обладнання, додатками та СПЗ в ІТС ПВЗ ПУ ЗС України;

- контроль досвідченості та спроможності особового складу виконувати завдання за призначенням в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України (навчання та тестування);

- можливість проведення ретельного та ефективного аналізу стану КБ в ІТС ПВЗ ПУ всіх ЛУ ЗС України та складання і надання зручних про стан КБ.

3.1.2. Об’єкти (цілі) ураження на які зосереджені дії СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ланок управління ЗС України. Обладнанням, СКБ розгорнути в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України сконцентрувати основні зусилля в інтересах забезпечення заходів з КР, ведення КД (КО) та КОб [26].

Відповідні КД спрямувати [26]:

- по об’єктах критичної інфраструктури ІТС, АСУ, системам зв’язку і управління зброєю противника, військовим та хакерським угрупуванням противника, а також по системам електропостачання у визначених операційних районах;

- на здійсненні КР акаунтів в соціальних мережах та інформаційних сайтів з метою виявлення в мережі Інтернет джерел ІР, які містять негативну інформацію про ЗС України;

- під час проведення прихованого сканування ІТС ЗС противника з метою виявлення уразливостей телекомунікаційного обладнання;

- на виявленні нових ІР-адрес в інформаційно-телекомунікаційних мережах противника (на вузлах зв’язку, які розгортаються), уразливостей мережевих конфігурацій телекомунікаційного обладнання;

- на час проведення КД для виявлення за демаскуючими ознаками ІТВ ЗС противника з метою визначення приналежності до ОВУ;

- на виборі засобів та заходів в залежності від результатів КР та створення сприятливих умов для проведення КА на інформаційні, ІТС противника;

- на час проведення КА, ударів на інформаційні, ІТС противника за окремою командою по визначених цілях:

а) НСД до програмних налаштувань (блокування роботи, отримання ID станцій, кодів доступу, частот роботи) ретрансляторів транкінгового зв’язку, які працюють в мережі, організованої за технологією IP Site Connect;

б) впровадження шкідливого ПЗ через поштові повідомлення на (далі – АРМ розгорнуті в мережах противника, з використанням підмінених електронних скриньок та локальне впровадження ШПЗ через змінні носії;

в) блокування роботи абонентів відомчих мереж телефонного зв'язку шляхом впливу на програмно-апаратне забезпечення VoIP-шлюзів, які працюють по протоколу прикладного рівня SIP

г) проведення DOS (DDOS) атак на веб-сервери (кореневі маршрутизатори) ІТВ ЗС противника.

3.1.3. Умови бойового застосування СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ланок управління ЗС України. Умови БЗ СКБ в ІТС ПВЗ ПУ різних ЛУ визначаються характером застосування ЗС, завданнями військ (сил), які беруть участь, використанню спроможностей сил і засобів з кібернетичного впливу (далі – КВ), що проводяться за єдиним замислом і у тісній взаємодії з іншими діями військ (сил) ЗС, ІВФ, ПрО, Державною службою спеціального зв'язку та захисту інформації та Службою безпеки України для виконання в КП програмно-математичних завдань, спрямованих на захист повсякденної діяльності і підтримку воєнних (бойових) дій та операцій ЗС України [27].

БЗ СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України залежить від умов обстановки, мети, складу і можливостей сил і засобів, об'єктів впливу, методів та способів ведення КД у КП та порядку КЗ КП власних військ (сил) з використанням усіх можливих методів і способів КВ.

Методи і способи впливів визначаються нормами міжнародного права, а також нормативно-правовими актами в області забезпечення КБ України.

3.1.4. Бойові можливості СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ланок управління ЗС України. Характер БЗ СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України

повинен бути зосередженим на виконанні наступних заходів, в залежності від умов виконання ним бойових завдань [26-27]:

- посилені бойових спроможностей СУ військами (силами) ЗС та інших суб'єктів сектору безпеки та оборони під час виконання ними спільних дій воєнного характеру;

- захоплені і утримані технологічної ініціативи на об'єктах критичної інфраструктури ІТС, АСУ, системі зв'язку і управління зброєю, інформаційно-телекомунікаційним мережам і системам ЗС України, у визначеній операційній смузі, зоні (районі), напрямку інформаційної інфраструктури;

- дестабілізаціїї СУ противника, створені сприятливих умов, щодо повної реалізації оперативних (бойових) спроможностей військ (сил), які ускладнять дії угруповань військ (сил) агресора;

- забезпечені сталого функціонування СУ підпорядкованих та взаємодіючих військ (сил), об'єктів критичної інфраструктури Держави, системі ПУ: ЗС України, ОДВ, ІВФ та ПрО, їх елементах, системі зв'язку військового призначення, системі автоматизації управління військами (далі – АУВ) під час КВ противника;

- забезпечені передачі сигналів оповіщення та попередження військ під час виявлення КА та кіберінцидентів;

- забезпечені обміну інформації між пунктами управління сил та засобів КБ Збройних сил та взаємодіючими пунктами управління ІВФ та ПрО, ОДВ.

3.1.5. Вимоги, що до взаємодії СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України з взаємодіючими ПУ ІВФ та ПрО, ОДВ та іншими суб'єктами національної СКБ (Державний центр КЗ та протидії Кзаг ДССЗІ України, Ситуаційний центр протидії Кзаг СБ України, Національна поліція, Національний банк України). Для організації взаємодії всіх служб та сервісів Системи інформаційного обміну у

режимі реального часу між суб'єктами забезпечення КБ під час виявлення КА та кіберінцидентів необхідно використовувати захищену транспортну мережу (захищене з'єднання) між суб'єктами забезпечення КБ України [26-27].

Обмін оперативною інформацією здійснювати по мережі обміну службовою інформацією ЗС України через мережу Інтернет, маршрутизатори та міжмережеві екрани. Маршрутизатори суб'єктів КБ з'єднуються між собою через мережу Інтернет використовуючи IPsec VPN-тунель. Забезпечення захисту внутрішніх ІТС суб'єктів здійснюється за допомогою міжмережевих екранів [26-27].

Безпосередньо за мирного часу та в особливий період взаємодію суб'єктів забезпечення КБ України здійснювати постійно та цілодобово через ГОЦЗІ та КБ ІТС ЗСУ (ЦОРІ КБ).

Обмеження щодо використання СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України зазначаються виключно у відповідності до норм міжнародного права, щодо методів ведення кібервійни, проведення КО проти критичної інфраструктури тієї чи іншої держави або КА, які захоплюють системи військового управління (ІВФ і ПрО), систем управління державного сектору, СУ противника (Керівництво з міжнародного права - "Талліннське керівництво") [26-27].

3.2 Розробка проекту тактико-технічних вимог до ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ланок управління ЗС України

Цільове призначення ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України.

Основним завданням ПЗ РП СКБ в інтересах забезпечення заходів з

КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України є утворення єдиної технічної системи спрямованої на реалізацію комплексу технічних заходів із КР, КЗ, контролю КБ та здійснення дій у КП в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України [28].

ПЗ РП СКБ повинно забезпечувати безперервний, стійкій, якісний, КЗ (далі КЗ) в ІТС ПВЗ ПУ різних ЛУ Міністерства оборони та Збройних сил України (далі ІТС МО та ЗСУ).

Склад ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України.

ПЗ РП СКБ з КЗ для забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ повинно включати в себе [27-28]:

- пакет оновлення сигнатур системи виявлень вторгнень – Cisco FirePower, а також системи моніторингу, аналізу мережевої поведінки та виявлення аномалій – NBAD у складі:

- ПЗ, основні характеристики складових ПЗ та порядок продовження сервісної підтримки для існуючих міжмережевих екранів в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України Додаток 7 (Таблиця – 7);

- ПЗ, основні характеристики складових ПЗ моніторингу, аналізу мережевої поведінки та виявлення аномалій в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України Додаток 8 (Таблиця – 8).

В розробленому проекті тактико-технічних вимог до ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України кількісні та якісні показники запропоновані, як варіант ПЗ РП СКБ в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України за умов оптимізації та послідовного переведення (удосконаленні організаційної структури) ОВУ

шляхом їх переходу на структури типу J, G, A, N., як складової СУ, організаційно-штатні структури за принципами та підходами, що застосовують держави – члени НАТО [13, 28]].

Остаточні якісні та кількісні показники ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ різних ЛУ ЗС України мають бути реалізовані та адаптовані за остаточним варіантом переоснащення та подальшим нарощуванням Системи оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR) та її інтеграції в Єдину ІС управління оборонними ресурсами (DRMIS) [29].

Наведене ПЗ повинно відповідати вимогам, що зазначені в Таблицях – 7, 8.

Основні завдання ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України.

Основні завдання ПЗ РП СКБ в ІТС ПВЗ ПУ [29]:

- участь у налаштуванні та реалізації політик безпеки ПЗ РП СКБ в ІТС ПВЗ ПУ різних ЛУ;

- забезпечення моніторингу, аналізу мережевої поведінки та виявлення аномалій в ПЗ РП СКБ в ІТС ПВЗ ПУ;

- запобігання кібернетичним втручанням до ІТС МО та ЗСУ;

- відстеження, ізоляція та знешкодження заражених об'єктів виявлених на ПУ стратегічної, оперативної та тактичної ЛУ;

- контроль за файлами, протоколами, вузлами, додатками та інцидентами безпеки;

- захист ІТС МО та ЗС України від дій шкідливого ПЗ;

- фільтрація URL-адрес за репутацією та категоріями, комплексне сповіщення та контроль над підозрілим веб-трафіком;

- реалізації ефективного фільтрування інформаційного потоку та управління обігом пакетів;

- організація моніторингу стану КП ІТС МО та ЗС України;

- контроль та унеможливлення реалізації противником (порушником) плану позбавлення ресурсів та блокування ІТС МО та ЗС України за допомогою атак типу відмова в обслуговуванні (DoS або DDoS);

- захист від НСД користувачів до інформації;

- масштабоване та централізоване керування мережевими операціями багатьох пристроїв навіть у разі розгалуженої, відмовостійкої, георознесеної інфраструктури;

- визначення стану мережі та мережевих елементів для з'ясування нормального рівня мережевого трафіку і його подальшого використання з метою створення політик безпеки та аналізу поведінки мережі.

- участь в аналізі та складанні звітів про стан КБ в ІТС МО та ЗСУ.

Спеціальні завдання ПЗ РП СКБ в ІТС ПВЗ ПУ [28]:

- забезпечення виявлення загроз шляхом профілювання хостів, мережевого трафіку/активності та оповіщення на наявність аномалій в залежності від нормального трафіку, профілів послуг, політики безпеки або перевищення хостом заявлених поведінкових порогів;

- забезпечення виявлення поліморфних, шифрованих, модифікованих і Zeroday (невідомих) атак;

- виявлення та класифікація мережевого трафіку додатків прикладного рівня;

- забезпечення захисту від злоякісного ПЗ з можливістю ретроспективного аналізу, пошуку та відображення шляхів розповсюдження;

- виконання заходів щодо оцінки ефективності захищеності елементів ІТС ПВЗ ПУ (серверне та мережеве обладнання, ПЕОМ, веб-сайтів, веб-додатків тощо) від КА;

- забезпечення емуляції основних видів Кзаг, тестування ефективності систем виявлення/попередження вторгнень, тестування ефективності політик безпеки між мережевих екранів, тестування комп'ютерних мереж, побудованих на основі ОС сімейств Windows, Linux, на наявність

вразливостей;

- тестування: веб-сайтів та веб-додатків на наявність вразливостей, стійкості паролів облікових записів користувачів;

- автоматизоване виявлення елементів комп'ютерних мереж, автоматизація процедур виявлення та експлуатації їх вразливостей;

- оцінка можливості отримання доступу через скомпроментовані вузли до інших вузлів;

- налаштування (підготовка) системних звітів, їх експорт у різних форматах даних та відправлення по e-mail для подальшого аналізу.

Об'єкти (цілі) дій ПЗ РП СКБ в процесі забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України.

Об'єктами (цілями) дій ПЗ РП СКБ в ІТС ПВЗ ПУ різних ЛУ ЗС України є [29]:

- проведення регулярних КА направлених на виявлення вразливостей в ІТС ЗС противника, блокуванні роботи мережевого обладнання розгорнутого на робочих місцях посадових осіб ПУ противника, перехват УВ (силами) противника, збір та викрадення (змінення) інформації про діяльність противника у визначеній операційній смузі, зоні (районі);

- впровадження розробленого шкідливого спеціального ПЗ (експлойтів, загроз "нульового дня", програм віддаленого управління та ін.) на підприємствах, установах та організаціях незалежно від форми власності, які проводять діяльність у сфері електронних комунікацій, ЗІ та/або є власниками (розпорядниками) об'єктів критичної інфраструктури Держави противника;

- руйнування, дезорганізація (проведення збоїв в сталому функціонуванні) об'єктів критичної інфраструктури Держави противника, системі ПУ (ОДВ, ІВФ та ПрО, хакерських угрупувань), їх елементів, системі зв'язку військового призначення, системі АУВ противника з використанням:

- КА типу “розподілена відмова в обслуговувані” проти IP ІТС ЗС противника;

- інфікування АРМ та викрадення службової інформації шляхом надсилання інфікованих шкідливим ПЗ повідомлень на адреси електронної пошти керівного складу ОВУ (ІВФ та ПрО) противника;

- інфікування ШПЗ елементів ІТС ЗСУ, ІВФ та ПрО противника;

- несанкціонованого підключення до ІТС ЗС противника телекомунікаційного обладнання (ноутбуки, 3G та CDMA-модеми, Wi-Fi точки доступу).

Умови застосування ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України.

Основними умовами застосування ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України є [29]:

- склад ПЗ РП СКБ в ІТС ПВЗ ПУ в інтересах виконання заходів КБ у ході проведення КО, першочергові та подальші завдання, які мають на меті проведення КА, ударів, заходів КР та КЗ, які спрямовані на здійснення впливу на КП противника та на захист власного КП;

- спроможність сил і засобів КВ які знаходяться в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ досягти бажаного рівня КВ на АСУ, системи зв’язку і управління зброєю, інформаційно-телекомунікаційні мережі і системи противника, а також створити сприятливі умови для забезпечення КОб;

Технічно-технологічна розгалуженість території противника, а саме[30]:

- наявність об’єктів критичної інфраструктури та розвиненість транспортної мережі (волоконно-оптичної та мультисервісної транспортної мережі на основі технологій DWDM, CWDM);

- ступінь надійності та резервування ліній зв'язку, мереж мобільного зв'язку 3G, мереж широкосмугового доступу до транспортної мережі з високошвидкісним транзитом трафіку за кордон;

- з'єднання з точками, вузлами зв'язку з метою обміну трафіку з найбільшими міжнародними операторами зв'язку, що надасть змогу безпосередньо впливати на кібернетичні активи (стаціонарні ПУ частин та підрозділів противника які знаходяться в пунктах постійної дислокації (далі ППД), ОВУ, ОУ ІВФ та ПрО, ОДВ) в СУ та телекомунікаційних мережах противника включаючи і застосування методів та способів КВ на СУ противника в бездротовому доступі;

- протяжність та розгалуженість міжміських волоконно-оптичних, бездротових мереж приватного сектору, телекомунікаційних компаній (DATA-груп, CERT, провайдерів зв'язку);

Можливості ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України.

Характерні можливості ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ різних ЛУ ЗС України [31]:

- централізоване управління пристроями, ліцензіями, подіями та політиками безпеки ПВЗ ПУ різних ЛУ ЗС України;

- управління на основі ролей (сегментоване та ізольоване представлення мережі і задачі на основі ролі адміністратора або групи);

- всебічна звітність і повідомлення про загальні і спеціальні події які циркулюють в ІТС ПУ ЗС України;

- надання інформації про події та контексти, які відбулись в ІТС ПВЗ ПУ різних ЛУ ЗС України, що відображаються в зв'язаних таблицях, на схемах і графіках;

- контроль поведінки і продуктивності мережі в ІТС ПУ тактичної, оперативної та стратегічної ЛУ;

- забезпечення функції зіставлення подій і усунення загроз в реальному часі;

- управління журналами, подіями та інформацією про безпеку (SIEM), паспортизацію несправностей і управління пакетами виправлень;

- виявлення загроз шляхом профілювання хостів, мережевого трафіку / активності та оповіщення на наявність аномалій в залежності від нормального трафіку, профілів послуг, політики безпеки або перевищення хостом заявлених поведінкових порогів;

- виявлення поліморфних, шифрованих, модифікованих і Zeroday (невідомих) атак, виявлення атак типу відмова в обслуговуванні (DDoS);

- протидія загрозам за рахунок таких видів дій, як Block Source, Block Destination, Block Port, Block Service, Custom;

- підтримка інтеграції з мережевими пристроями захисту (наприклад, маршрутизатор, міжмережевий екран і т.д.) з метою подальшого конфігурації для протидії виявленим атакам на ПУ всіх ЛУ ЗС України;

- емуляція основних видів Кзаг та тестування ефективності систем виявлення/попередження вторгнень (IDS/IPS);

- тестування ефективності політик безпеки між мережевих екранів; тестування комп'ютерних мереж, побудованих на основі ОС сімейств Windows, Linux, на наявність вразливостей;

- тестування веб-сайтів та веб-додатків на наявність вразливостей;

- оцінка можливості отримання доступу через скомпрометовані вузли зв'язку ПУ до інших ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ.

Вимоги щодо взаємодії в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України між собою, щодо функціонування ПЗ РП СКБ в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб [31].

Обмін оперативною інформацією, щодо функціонування ПЗ РП СКБ здійснювати по мережі обміну службовою інформацією ЗС України через мережу Інтернет, маршрутизатори та міжмережеві екрани здійснювати постійно та цілодобово через ГОЦЗІ та КБ ІТС ЗСУ (ЦОРІ КБ) [31].

Маршрутизатори підпорядкованих регіональних центрів ЗІ та КБ з’єднуються між собою через мережу Інтернет використовуючи IPsec VPN-тунель. Забезпечення захисту внутрішніх ІТС суб’єктів здійснюється за допомогою міжмережевих екранів.

ВИСНОВОК

Основною вимогою, що висувається під час створення та розгортання системи кібербезпеки в ІТС ПУ різних ЛУ ЗС України, є еволюційність. Ця вимога передбачає здатність системи до адаптації та модифікації своїх параметрів і технологій кіберзахисту під впливом зовнішніх та внутрішніх кіберзагроз протягом усього життєвого циклу. Системи повинні мати можливість швидко реагувати на зміни в середовищі, забезпечуючи стійкість і ефективність захисту. Обладнання апаратно-програмних комплексів кібербезпеки, що використовується в ІТС польових вузлів зв'язку ПУ ЗС України, повинно гарантувати захист в реальному часі від усіх відомих кіберзагроз, а також забезпечувати можливість виявлення та блокування нових, ще невідомих загроз. Це вимагає постійного оновлення та вдосконалення системи захисту.

Важливо підкреслити, що виключно технічними засобами неможливо побудувати комплексну та ефективну систему кібербезпеки для ІТС польових вузлів зв'язку, включаючи тактичні, оперативні та стратегічні ланку управління ЗС України. Для цього необхідний комплекс організаційних, нормативних, фізичних і технічних заходів, які будуть взаємопов'язані і створюватимуть цілісну систему захисту. Інтеграція апаратно-програмних комплексів кібербезпеки в діючі мережі ЗС України є складним і відповідальним процесом. Правильний вибір продуктів, які найкраще відповідають вимогам функціонування цих мереж, має велике значення. Будь-які помилки на цьому етапі можуть призвести до значних фінансових і репутаційних втрат.

Система кібербезпеки в ІТС ПУ різних ЛУ ЗС України повинні мати модульну структуру, що дозволяє зручно їх розгортати та модернізувати відповідно до актуальних кіберзагроз. У разі необхідності, системи мають бути здатні швидко трансформуватися від апаратно-програмних комплексів тактичної ЛУ до стратегічної, що забезпечить гнучкість і адаптивність.

Для досягнення цієї мети важливо використовувати обладнання від різних виробників, таких як Cisco, MicroTic, HP, IBM, Juniper тощо. Це дозволить організувати взаємоконтроль між різними компонентами та сприяти обміну ідеями та напрацюваннями, що підвищить загальну ефективність системи. В умовах інтенсивного розвитку ринку апаратно-програмних комплексів кібербезпеки необхідно приділяти увагу основним характеристикам продуктів, таким як продуктивність, алгоритми шифрування, ключові схеми тощо. Ці аспекти безпосередньо впливають на ефективність захисту системи.

До системи кібербезпеки в ІТС польових вузлів зв'язку ПУ різних ЛУ ЗС України необхідно обмежити коло осіб, допущених до налаштування та втручання в стабільну роботу системи. Важливо також використовувати таке обладнання, яке не потребує постійної присутності оператора і автоматично підключається до мережі після відновлення штатних умов роботи. Це дозволить забезпечити безперервність функціонування системи та знизити ризики, пов'язані з людським фактором.

Отже, у даній роботі розглянуто ключові вимоги до створення та розгортання системи кібербезпеки в ІТС ПУ ЗС України. Основною вимогою стала еволюційність системи, яка повинна адаптуватися до змін у кіберсередовищі протягом усього життєвого циклу. Підкреслено, що для ефективного захисту необхідний комплексний підхід, що включає технічні, організаційні та нормативні заходи.

Також акцентовано на важливості інтеграції різноманітного обладнання від різних виробників, що забезпечить гнучкість і можливість модернізації системи. Необхідно також обмежити коло осіб, допущених до налаштування системи, та використовувати автоматизовані рішення для зниження ризиків, пов'язаних з людським фактором. Загалом, підкреслюється важливість комплексного і адаптивного підходу до кібербезпеки в умовах сучасних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Затверджено Начальником Генерального штабу Збройних Сил України – Головнокомандувачем Збройних Сил України Технічне завдання на створення інформаційно-телекомунікаційної системи "Центр оперативного реагування на інциденти кібернетичної безпеки" від 23.04.2018 № 2437дск.

2. Постанова Кабінету Міністрів України "Про затвердження Положення про порядок обліку, зберігання, списання та використання військового майна у Збройних Силах" від 04.08.2000 р. № 1225, Офіційний вісник України, 25.08.2000, № 32, 297 с.

3. Закон України "Про державну таємницю" від 21.01.1994 № 3855-XII (зі змінами), Відомості Верховної Ради України, 19.04.1994, №16, 422 с.

4. Закон України "Про інформацію" від 02.10.1992 № 2657-XII (зі змінами), Голос України,13.11.1992, 14с.

5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 19.04.2014 № 80/94-ВР, Відомості Верховної Ради України,02.08.1994, № 31, стаття 286.

6. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII, Відомості Верховної Ради України,09.05.2018, № 45, 403с.

7. Постанова Кабінету Міністрів України від 29.03.2006 № 373 "Про затвердження правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" (зі змінами), www.dut.ua.

8. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" від 15 березня 2016 року № 96/2016", https://www.president.gov.ua

9. Постанова Кабінету Міністрів України № 736, жовтень 2016 р. "Про затвердження Типової інструкції про порядок ведення обліку, зберігання,

використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію", Офіційний вісник України,04.11.2016, № 85, 102с.

10. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99. – [Чинний від 28.04.1999]. – К.: ДСТСЗІ СБ України, 1999. 28 с.

11. "Рішення Ради національної безпеки і оборони України", від 04.03.2016 "Про Концепцію розвитку сектору безпеки і оборони України", підстава Указ Президента України № 92/2016, від 14.03.2016, Голос України, 14.04.2016, № 144.

12. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД СТЗІ 1.1-003-99. – [Чинний від 28.04.1999]. – К.: ДСТСЗІ СБ України, 1999. 24 с.

13. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99- [Чинний від 28.04.1999]. – К.: ДСТСЗІ СБ України, 1999. 26 с.

14. ENISA: Cyber Excrcises – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

15. Critical Information Infrastructure Protection Course. – Режим доступу: https.//ccdcoe.org/critical-information-ifrastructure-protection-course-2021.html.

16. Military and Security Deployments Involving the People's Republic of China – Режим доступа: http:// www.defense.gov/pubs/pdfs/2020_CMPR_Final.pdf.

17. China's Secret Cyberterrorism [Електроннийресурс]. – Режим доступу: http:// www.t hedailybeast.com/blogs-and-stories/2020-01-13/chinas-secret-cyber-terrorism/full.

18. Remarks on Internet Freedom [Russian] [Electronic resource] / H.Clinton. – Режим доступа:

http://www.state.gov/documents/organization/135878.pdf.

19. Foreign Ministry Spokesperson Ma Zhaoxu's Remarks on China-related Speech by US Secretary of State on "Internet Freedom" [Електронний ресурс]. – Режим доступу: http://www.fmprc.gov.cn/eng/xwfw/s2510/2535/t653351.htm.Joint Publication 3-13 Information Operations – 2022 – 117 с.

20. Andress J., Winterfeld S. Cyber Warfare, 2021 – 321 с.

21. Secretary of State Hillary Rodham Clinton On the Release of President Obama Administration's International Strategy for Cyberspace. May 16, 2021 [Електронний ресурс]. – Режим доступу : http://www.state.gov/secretary/rm/2011/05/163523.htm.

22. The Comprehensive National Cybersecurity Initiative. National Security Council [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity.

23. Конвенція Ради Європи „Про кіберзлочинність", від 23.11.2001 Ратифікація від 07.09.2005, підстава 2824-15, Офіційний вісник України, 10.09.2017, № 65, С.107.

24. Лужецький В.А. Основи інформаційної безпеки : навч. посібник / Лужецький В.А., Кожухівський А.Д., Войтович О.П. – Вінниця : ВНТУ, 2006. – 115 с.

25. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник / Ліпкан В.А. МаксименкоЮ.Є., Желіховський В.М. – К. : КНТ, 2006. – 280 с.11.

26. Рекомендація МСЭ-Т X.1205. Обзор кібербезпеки. – Женева: МСЕ, 2010 рік. – С. 55. –[Електронний ресурс]. – Режим доступу: www.itu.int/ITU-T/recommendations/rec.aspx?rec=91364;

27. Рекомендації міжнародна союзу електрозв'язку. Мережі передачі даних, взаємозв'язок відкритих мереж та безпека. Безпека кіберпростору – кібербезпека. МСЕ-Х.1208 2014 року р. ISO/IEC 27000. Режим доступу: [б-ISO/IEC27000].

28. FM 3-12 Cyberspace and Electronic Warfare Operations, April 2017;
29. JP 3-12 Cyberspace Operations, 8 June 2018;
30. NIST 800 – 30 Risk Management Guide for Information Technology Systems;
31. PEN-103: Kali Linux Revealed // https://www.offsec.com/courses/pen-103/;

ДОДАТОК А

Розділ 2 (англійська версія)

SECTION 2
DEVELOPMENT OF PERSPECTIVE SCHEMES OF CYBERSECURITY SYSTEM DEPLOYMENT IN ITS PVS TACTICAL, OPERATIONAL AND STRATEGIC LINKS OF THE ARMED FORCES OF UKRAINE

2.1 Typical schemes of deployment of the cybersecurity system in ITS PVZ of tactical, operational and strategic links of the Armed Forces of Ukraine.

Typical schemes of SCS deployment in ITS PVZ for tactical, operational and strategic LU of the Armed Forces of Ukraine are presented in Figure 2.1. The general scheme in Figure 2.2 is discussed in more detail. on the example of ITS PU tactical LN.

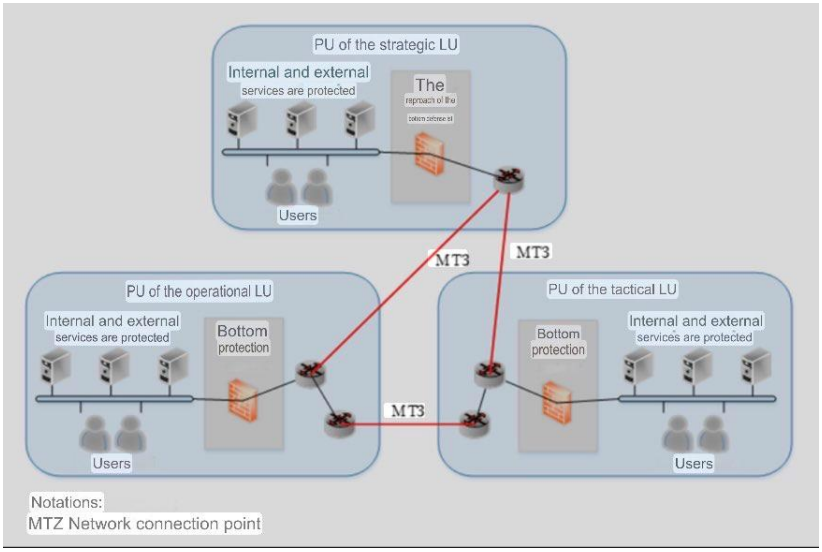


Figure 2.1. - Scheme of KB deployment in ITS PVZ tactical, operational and strategic LU of the Armed Forces of Ukraine

Stable functioning of SCS in ITS PVZ operational license area of the Armed Forces of Ukraine, which is given as an option in the qualification work, is achieved through the coordinated functioning of equipment and software on the PVZ of various license areas included in its composition. The general requirement for the equipment to be deployed on PVZ is that KB complexes should form a balanced and interacting set of KB infrastructure management tools in information

and technical systems (hereinafter - ITexS) of Ukraine and the Armed Forces of Ukraine at the strategic, operational and tactical levels [14].

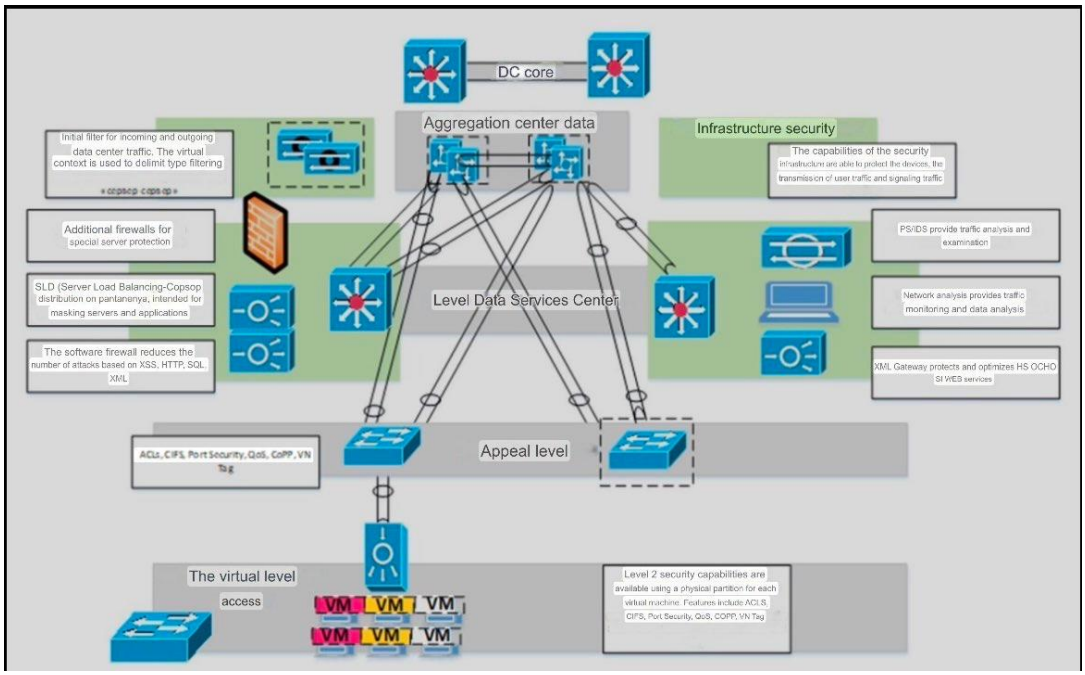


Figure 2.2. - Typical scheme of deployment of CB in ITS PVZ tactical management of the Armed Forces of Ukraine

So, the final version of the schemes of deployment of the SCS in ITS PVZ for all LUs of the Armed Forces of Ukraine will be presented after the completion of the transfer of the OMU to the structures of the headquarters of NATO troops and the improvement of the organizational structure of the OMU through the transition to models of type J, G, A, N.

The illuminated version of the schemes of deployment of SCS in ITS PVZ for tactical, operational and strategic LU of the Armed Forces of Ukraine is formalized and opens up opportunities for further research in this field of FP [14].

Since time does not stand still, the development of ITS of the Armed Forces of Ukraine requires modern approaches to design bureaus, especially in the conditions of active databases in our country. However, the gradual transition, re-equipment, change in the network topology and improvement of the organizational structure of HC slow down this process. In this regard, it is important to consider the individual components and elements of typical SCS deployment schemes, as

well as to dwell in detail on the implementation of a sequence of implementation rules that can significantly improve the functioning of the PVZ network. Among these elements are [14]:

a) firewalls;

b) virtual private network technologies;

c) public key infrastructure.

Firewalls. One of the main tasks of firewalls in ITS PVZ (Figure - 2.3.) for any LN is to protect network segments or individual hosts from the NSD, in particular due to vulnerabilities in the protocols of the OSI network model or software on the PC. Firewalls analyze traffic by comparing its characteristics with predefined patterns, which allows you to skip or block data depending on the established rules [15].

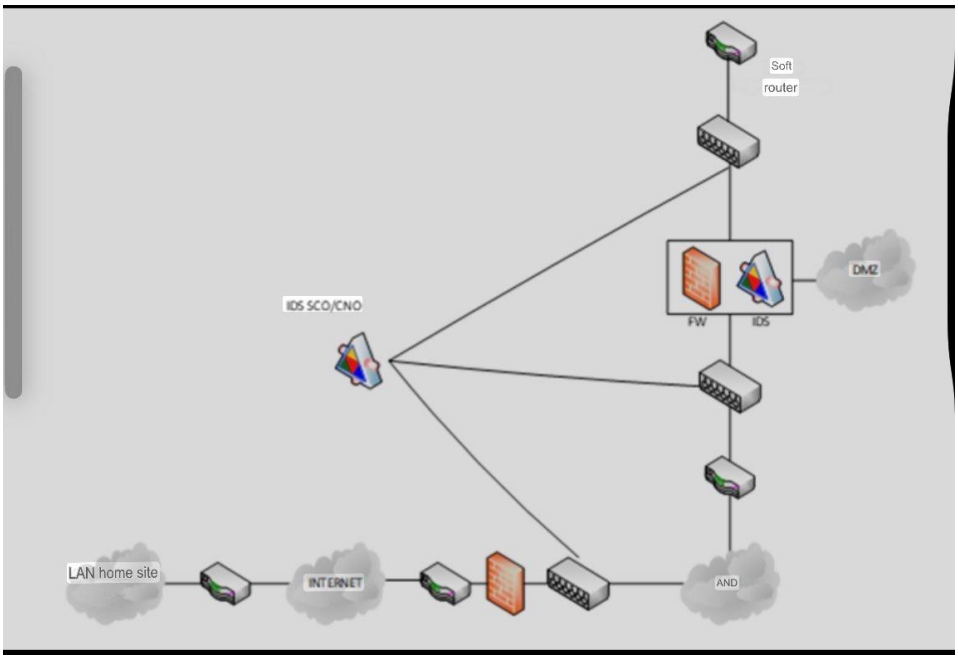


Figure 2.3. - Firewalls in IT PVZ RU

The most common place to install firewalls is the perimeter of the local network, which allows you to protect internal hosts from external attacks. However, it is important to note that attacks can also start from internal IT nodes. In such cases, if the attacked host is on the same network, the traffic will not cross the network perimeter boundary, and the firewall will not be able to perform its function [15]. Therefore, it is advisable to place firewalls not only at the border,

but also between different network segments, which creates an additional level of security.

Traffic filtering in firewalls is based on a set of preconfigured rules known as ruleset. You can represent a firewall as a series of filters, each of which processes the information flow according to a specific rule. The consistency of these rules has a significant impact on firewall performance [15]. For example, firewalls compare traffic with rules until they find a match. Therefore, the rules corresponding to the largest amount of traffic should be placed as high as possible in the list, which can improve performance.

There are two principles for processing incoming traffic in the ITexS of the PVZ PU. The first principle, "What is not explicitly forbidden is allowed," means that if the firewall receives a packet that does not match any rule, it is passed on. The opposite principle - "What is clearly not allowed is forbidden" - provides greater security, since it prohibits all traffic that is not allowed by the rules. However, this approach creates an additional burden on the PU PVZ network administrator [14, 15].

As a result, firewalls perform one of two main operations: either skip the packet further (allow), or drop it (deny). Some firewalls also implement a reject operation, in which a packet is dropped, but a message is sent to the sender that the requested service is unavailable. In the case of deny, the sender does not receive any information, which makes this method more secure [15].

To date, there is no single classification of firewalls, but in many countries they are classified according to the level of the supported OSI model. Based on this model, we can distinguish the following types of firewalls that can be used in ITexS of the Armed Forces of Ukraine [16]:

1. Managed switches.
2. Batch filters.
3. Session-level gateways.
4. Intermediaries of the application level.
5. State inspectors.

There are two main options for implementing firewalls: software and software and hardware. The latter can be implemented as a separate module in a switch or router, or as a specialized device.

To date, ITexS PVZ PU usually uses software solutions that at first glance look more convenient. This is because for their implementation it is enough to purchase a network protection program and install it on any PC on the network. However, in practice, free PCs may not be available, and those that are, often do not meet the requirements for system resources. If the PC is found, you need to configure the OS and firewall. It turns out that using a regular PC is much more difficult than it first seems [16].

Therefore, specialized hardware and software complexes called security appliances, which are usually based on FreeBSD or Linux systems optimized to perform only the necessary functions, are increasingly gaining popularity. Advantages of such solutions include [16]:

- Ease of implementation: These devices come with an already configured OS that requires minimal setup during network integration.

- Ease of management: they can be managed from anywhere (at different management levels) through standard protocols such as SNMP or Telnet, as well as through secure protocols such as SSH or SSL.

- High performance: these devices work more efficiently, since all unnecessary services are excluded from their OS.

- Reliability and high availability: they are designed to perform specific tasks with high availability.

2.2 Application of the technology of virtual private networks on PVZ PU of various links of the Armed Forces of Ukraine

Virtual private network technology. Administrators of networks deployed on PVZ PU of various LUs of the Armed Forces of Ukraine often see a VPN as an effective means of providing KB. However, in practice, the implementation of this

technology may be more difficult than expected. After the introduction of VPNs, features are often identified that were not taken into account earlier and that can significantly affect the stable operation of the network [17].

The main tasks of this section are to study the problems that arise after the implementation of the VPN and provide recommendations for choosing the best solutions. Implementation of CB in ITS PVZ PU via VPN (Figure 2.4).

The essence of technology. The principle of operation of virtual private networks is to tunnel traffic through telecommunication networks, such as the network of the Armed Forces of Ukraine or the Internet. The implementation of the technology is carried out using special devices - crypto locks. These devices not only protect the local network from external threats, but also route traffic. VPN differs from traditional solutions based on dedicated channels due to its flexibility, scalability and lower cost, as well as a high level of DP [17].

ITex of the Armed Forces of Ukraine is developing rapidly, and VPN devices are offered by almost all major manufacturers of telecommunications equipment. However, the introduction of virtual networks has its own characteristics.

Impact assessment [17]. When virtual networks are functioning, the gateways perform traffic conversion, as a result of which many network performance characteristics may deteriorate from the point of view of the end user. VPN integration can lead to the following network changes:

- Reduced network bandwidth.
- Traffic conversion overhead.
- Packet transmission delays.

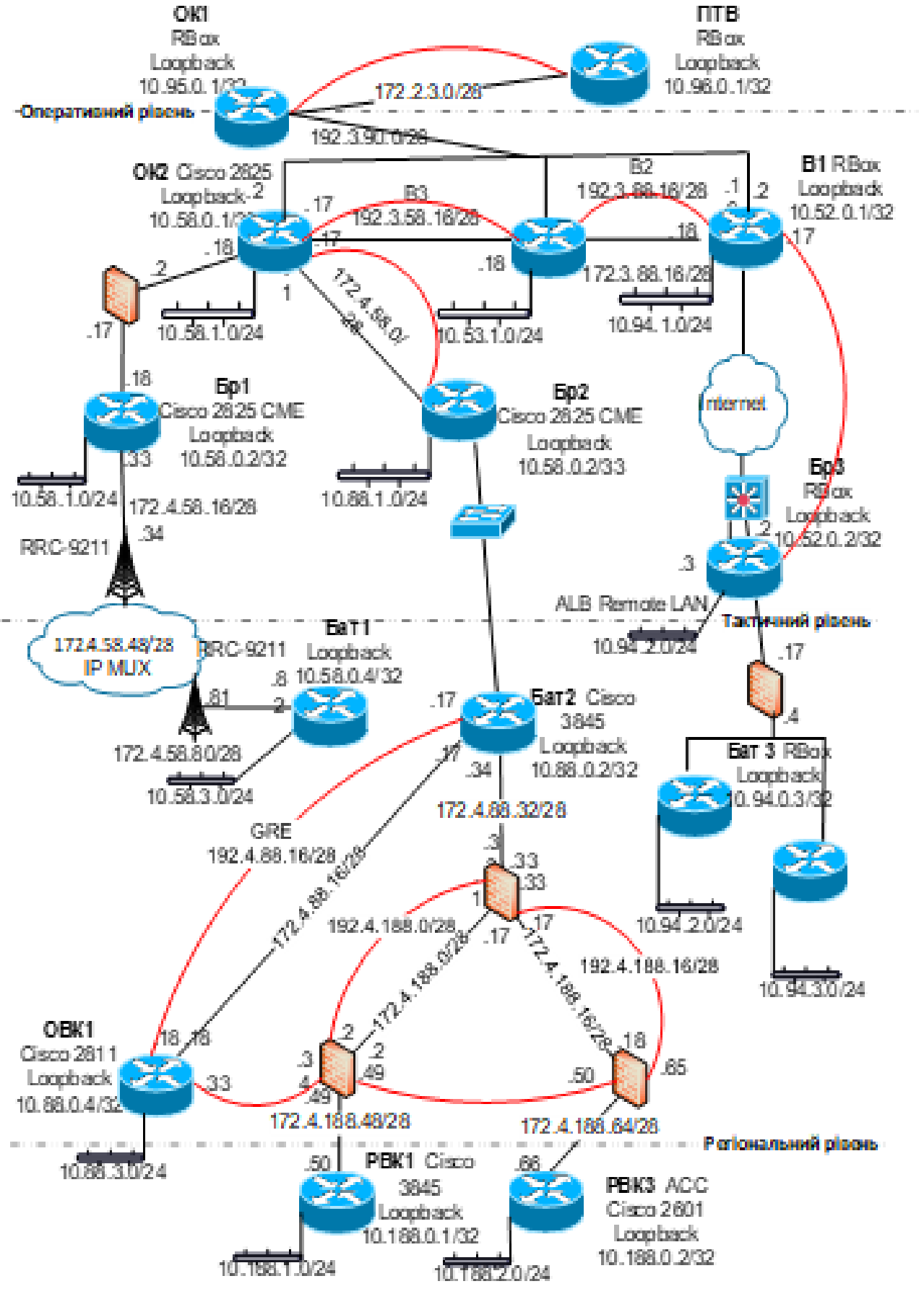


Figure 2.4. - Implementation of CB in ITS PVZ PU via VPN

Reduced throughput can occur for a variety of reasons. One of them is the insufficient performance of the crypto gateway itself. Although this parameter is usually important when choosing such devices, it is important that VPN devices have sufficient bandwidth to minimize their impact on the transmission of information in the network [18].

The second reason for the decrease in network bandwidth is related to the type of traffic and the overhead of its processing. These costs are incurred by adding a new IP header to the tunneled packet, depending on the protocol selected. For example, IPsec adds a minimum of 54 bytes to the packet. For a standard 1500-byte IP packet, the increase will be about 4%, while for a 56-byte packet (for example, in IP telephony), the overhead can reach 100% [18].

Manufacturers from the Russian Federation offer their own protocols, such as the Continent-K encryption protocol, which usually have fewer drawbacks compared to IPsec, reducing packet length gain and often introducing header compression [18].

Delays in packet transmission can be caused by many factors. While a VPN may play a role, delays also depend on the operation of various network nodes, in particular Internet access nodes and gateways between providers. VPN devices can cause two types of delays: forward, which is due to packet processing time, and indirect, which occurs due to increased traffic due to tunnel overhead [18].

Recommendations when choosing a VPN. When choosing a VPN, it is important to consider the impact on the existing IT infrastructure of the Armed Forces of Ukraine. Before designing a VPN, you should carefully evaluate how this technology will affect existing or planned services, especially in the context of technological parameter collection and dispatch control systems, where time delays are critical [18].

Another important example is IP telephony. Despite the initial skepticism, this technology is actively developing in ITS of the Armed Forces of Ukraine. When you integrate a VPN into a short packet network (for example, 56 bytes for

IP telephony), overhead can significantly reduce bandwidth. For the IPsec protocol, for example, the packet size can increase by more than 100% [18, 19].

The problems associated with implementing a VPN can be solved in two ways. The first option is to increase the bandwidth of the channel. This can eliminate many problems, but rental costs can double. The second option is to choose protocols with minimal tunneling overhead, while other parameters of the VPN equipment must meet the requirements of the user [19].

The operation of ITS after VPN integration is not limited to the installation stage. It is important to take into account the concept of the system, in particular the choice of protocols and encryption algorithms, as this affects the security and convenience of network management. Finding a compromise between safety and usability is critical [19].

In addition, it is necessary to consider how the network responds to emergency situations. It is important that the crypto locks, especially in tactical LUs, are reliable and easy to maintain. Some devices may require you to enter key information to reconnect after rebooting, which can lead to prolonged disconnections of the VPN segment and loss of application operation [19].

So, careful planning and consideration of all these factors will increase the efficiency of VPN implementation in the network of the Armed Forces of Ukraine.

2.3 Deploying Public Key Infrastructure (PKI)

Public key infrastructure (PKI) (Figure - 2.5.) is a set of tools - technical, material and human - as well as distributed services and components that are used to provide cryptographic tasks based on private and public keys. This system supports secure information exchange, user authentication and ensures data integrity [20].

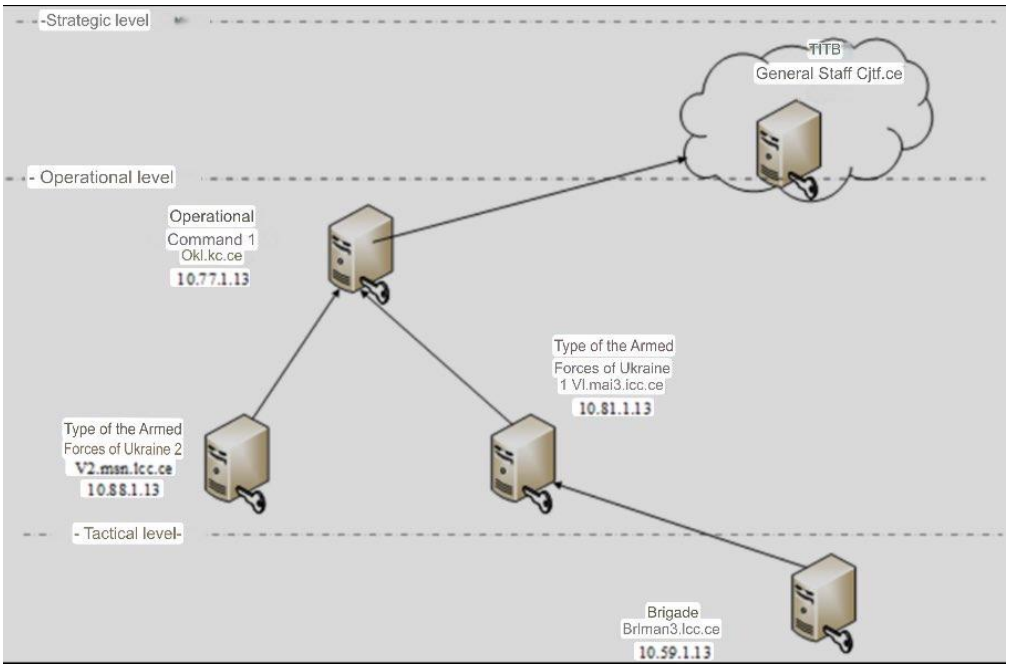


Figure 2.5. - Public key infrastructure of the CB system in IT PVZ PU of different license areas

The public key infrastructure (PKI) is based on the use of a public key cryptographic system based on several basic principles [20]:

1. The private key is known only to its owner.

2. The public key certificate confirms that the private (secret) key belongs only to its owner, while the public key is freely transmitted in the certificate.

3. Trust between the parties is not automatic; everyone trusts only the certification center.

4. The Certification Authority (CA) confirms or denies that the public key belongs to a certain person who has the corresponding private key.

The main tasks of SCS in IT PVZ PU implemented by PKI include:

- Ensuring the confidentiality of information.

- Guarantee data integrity.

- Authenticate users and the resources they access.

- Ability to confirm user actions with information.

PKI consists of several key components, the main of which is to verify the identity of users through a certification center. Information is exchanged between

the center and users using certificates. The functioning of PKI is based on the rules of the system and the principles of public key cryptography. The infrastructure includes a certification authority (certification authority), end users, as well as additional elements such as a registration authority and a network directory [20].

The main functions of PKI include [20]:

- Verification of the identity of users who apply for certificates.
- Issuing certificates to users.
- Cancellation of certificates if necessary.
- Maintain and publish Certificate Revocation Lists (CRLs) that help clients make trust decisions about certificates.

Additional functions of the certification center (CC) [20]:

- Generation of key pairs, one of which is included in the certificate.
- Verification of the authenticity of the electronic signature of the certificate holder upon request, especially in cases of conflict.

The certificate is an electronic document containing the user's public key, owner data, electronic signature of the certification authority, certificate validity period and other attributes. It cannot be indefinite and always includes the start and end date of the action [20].

The main reasons for early cancellation of certificates [20]:

- Compromise of the private key.
- Change the certificate owner information.
- Voluntary request of the certificate holder.
- Change the authority of the certificate holder.

A key pair consists of two keys: a private key and a public key. These keys are created together and are complementary. Information encrypted with a public key can only be decrypted using a private key. At the same time, an electronic signature created using a private key can be verified using a public key [21].

The key pair can be created either by the certificate issuing center (certification center) at the request of the user, or by the user himself using special

software. After identifying the user, the CC issues a certificate signed by this center, confirming its legitimacy [21].

A valid electronic signature confirms the authorship of the data and its integrity during transmission, and the code signature ensures that the software does not contain malicious code. The private key is used to sign data, as well as to decrypt information received from other PKI participants. The public key from the certificate of another participant can be used to verify the electronic signature and encrypt the information that is planned to be sent [21].

It is worth noting that the encryption process by asymmetric algorithms is slower compared to symmetric algorithms, so it is not usually used to encrypt large amounts of data. Public key certificates are used to establish secure communication with websites such as online stores or banks, while symmetric keys are usually used for subsequent data exchange [20, 21].

One of the key elements of the public key infrastructure (PKI) is an electronic signature, which is the result of using the signature algorithm on the hash of data (documents, messages or files).

Authentication of electronic signature is performed by the following stages [22]:

1. The recipient receives the data (in encrypted or clear form) along with the electronic signature.

2. The data is decrypted either using a consistent symmetric key or the recipient's private key (if the data was encrypted with his public key).

3. The recipient calculates the hash of the decrypted document (the hash algorithm is specified in the certificate).

4. The electronic signature algorithm is used to remove the signature (specified in the certificate), which allows you to get the hash of the original document.

5. The recipient compares the received hashes: if they match, the electronic signature is considered valid, provided that the certificate is active and used according to its policies.

Among the applications that support PKI are: secure e-mail, payment protocols, electronic checks, electronic information exchange, data protection in networks with IP protocol, as well as electronic documents with digital signature [20-22].

In this regard, during the development and implementation of SCS in ITS PVZ PU of various logistics departments of the Armed Forces of Ukraine, it is important to take into account the use of software distributed subsystems (hereinafter - RP) to provide cyber intelligence measures (hereinafter - KR), KZ and KOb, as well as KOb during joint actions of the Armed Forces of Ukraine, IvF and PrO under martial law and during a special period [20-22].

ДОДАТОК Б

Організаційна структура системи кібербезпеки в ІТС польових вузлів зв'язку ПУ різних ланок управління Збройних Сил України
(Стаття)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами X Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ: ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

20 грудня 2024 року

Полтава 2024

УДК 004.89 + 681.51

Збірник наукових праць за матеріалами X Всеукраїнської науково-практичної конференції «Електронні та мехатронні системи: теорія, інновації, практика», 20 грудня, 2024 р. / Національний університет «Полтавська політехніка імені Юрія Кондратюка».

Редколегія: О.В. Шефер (головний редактор) та ін. – Полтава: НУ «Полтавська політехніка імені Юрія Кондратюка», 2024. – 124 с.

У збірнику представлені результати наукових досліджень та розробок в області сучасних електромеханічних систем та автоматизації, електричних машини і апаратів, моделювання та методів оптимізації, енергозбереження в електромеханічних системах, управління складними технічними системами, проблем аварійності та діагностики в електромеханічних системах та електричних машинах, інформаційно-комунікаційних технологіях та засобах управління. Призначений для наукових й інженерно-технічних працівників, аспірантів і магістрів.

Матеріали відтворено з авторських оригіналів та рекомендовано до друку IX Всеукраїнської науково-практичної конференції «Електронні та мехатронні системи: теорія, інновації, практика». Редакція не обов'язково поділяє думку автора і не відповідає за фактичні помилки, яких він припустився.

Відповідальний за випуск - д.т.н., професор О.В. Шефер.

здійснювалась за допомогою FPV RACING RUSH. У якості контролера використано Arduino UNO. Для керування двигунами розглядалось кілька драйверів CNC SHIELD та L298N та електромагнітне реле ZMPT101B, що можуть керувати двигунами Usongshine Stepping Motor Model: 17HS4401.

Реалізація моделі наземної робототехнічної платформи для усунення надзвичайних ситуацій у галузі електроенергетики потребує розробки цифрового двійника. Поглиблене дослідження цифрового двійника заплановано на жовтень – листопад 2024 року.

ЛІТЕРАТУРА:

1. Radiomaster Boxer [Електронний ресурс] – Режим доступу до ресурсу: https://www.radiomasterrc.com/products/boxer-radio-controller-m2.

2. Usongshine Stepping Motor Model: 17HS4401 [Електронний ресурс] – Режим доступу до ресурсу: http://www.baolai-cn.com/en/?gad_source=1&gclid=EAIaIQobChMItMfowZPZiQMVjadoCR2cjyn6EAAYASAAEgI8j_D_BwE.

A MODEL OF A GROUND ROBOTIC PLATFORM FOR EMERGENCY RESPONSE IN THE POWER INDUSTRY

***A. Fedorenko**, Master's Student*
National University "Yuri Kondratyuk Poltava Polytechnic"

УДК 004.9

С.С. Голубцов
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ОРГАНІЗАЦІЙНА СТРУКТУРА СИСТЕМИ КІБЕРБЕЗПЕКИ В ІТС ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ ПУ РІЗНИХ ЛАНОК УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Підготовка та ефективне застосування Збройних Сил України, а також інших військових формувань і правоохоронних органів спеціального призначення, є критично важливими для забезпечення національної безпеки. Це залежить від визначених функцій і завдань, які покладені на ці організації згідно з законодавством України, а також від умов воєнно-політичної і воєнно-стратегічної обстановки, тенденцій її розвитку та потенційних загроз.

У 2024 році тривала реформа системи управління Збройних Сил України (далі – ЗС України), що передбачає посилення можливостей органів військового управління та підвищення якості оперативного і бойового управління [1]. У рамках цієї реформи було проведено оптимізацію системи управління угрупованнями сил, зокрема перехід від трьох до двох оперативно-тактичних угруповань, що сприяє ефективнішій організації та управлінню [2].

Структура пунктів управління різних рівнів регламентується директивами Генерального штабу, що визначає їх склад, призначення та функції в контексті загальної системи управління військами. Одним із важливих аспектів є оптимізація органів військового управління відповідно до стандартів НАТО, переоснащення системи зв'язку на цифрову платформу та впровадження сучасних інформаційних технологій. Зважаючи на недостатню надійність існуючих інформаційно-телекомунікаційних систем, питання захисту інформації та кібербезпеки набуває особливої актуальності. Це стосується не лише конфіденційності та цілісності даних, але й їх доступності в умовах збройного конфлікту [3]. Управління у готовності до виконання завдань вимагає чіткої організації та належного забезпечення інформаційної безпеки.

Основною вимогою, що висувається під час створення та розгортання системи кібербезпеки в інформаційно-телекомунікаційних системах пунктів управління (далі – ІТС ПУ) різних ланок управління (далі – ЛУ) ЗС України, є еволюційність. Ця вимога передбачає здатність системи до адаптації та модифікації своїх параметрів і технологій кіберзахисту під впливом зовнішніх та внутрішніх кіберзагроз протягом усього життєвого циклу. Системи повинні мати можливість швидко реагувати на зміни в середовищі, забезпечуючи стійкість і ефективність захисту [4]. Обладнання апаратно-програмних комплексів кібербезпеки, що використовується в ІТС польових вузлів зв'язку ПУ ЗС України, повинно гарантувати захист в реальному часі від усіх відомих кіберзагроз, а також забезпечувати можливість виявлення та блокування нових, ще невідомих загроз. Це вимагає постійного оновлення та вдосконалення системи захисту.

Важливо підкреслити, що виключно технічними засобами неможливо побудувати комплексну та ефективну систему кібербезпеки для ІТС польових вузлів зв'язку, включаючи тактичні, оперативні та стратегічні ланку управління ЗС України. Для цього необхідний комплекс організаційних, нормативних, фізичних і технічних заходів, які будуть взаємопов'язані і створюватимуть цілісну систему захисту. Інтеграція апаратно-програмних комплексів кібербезпеки в діючі мережі ЗС України є складним і відповідальним процесом [5]. Правильний вибір продуктів, які найкраще відповідають вимогам функціонування цих мереж, має велике значення. Будь-які помилки на цьому етапі можуть призвести до значних фінансових і репутаційних втрат.

Система кібербезпеки в ІТС ПУ різних ЛУ ЗС України повинні мати модульну структуру, що дозволяє зручно їх розгортати та модернізувати відповідно до актуальних кіберзагроз. У разі необхідності, системи мають бути здатні швидко трансформуватися від апаратно-програмних комплексів тактичної ЛУ до стратегічної, що забезпечить гнучкість і адаптивність.

Для досягнення цієї мети важливо використовувати обладнання від різних виробників, таких як Cisco, MicroTic, HP, IBM, Juniper тощо. Це дозволить організувати взаємоконтроль між різними компонентами та сприяти обміну ідеями та напрацюваннями, що підвищить загальну ефективність системи. Стрімкий розвиток ринку програмного та апаратного забезпечення для

кібербезпеки вимагає уваги до ключових характеристик продуктів, таких як продуктивність, алгоритми шифрування та ключові схеми. Ці аспекти безпосередньо впливають на ефективність захисту системи.

ЛІТЕРАТУРА:

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 19.04.2014 № 80/94-ВР, Відомості Верховної Ради України,02.08.1994, № 31, стаття 286.

3. "Рішення Ради національної безпеки і оборони України", від 04.03.2016 "Про Концепцію розвитку сектору безпеки і оборони України", підстава Указ Президента України № 92/2016, від 14.03.2016, Голос України, 14.04.2016, № 144.

4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99. – [Чинний від 28.04.1999]. – К.: ДСТСЗІ СБ України, 1999. 28 с.

5. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД СТЗІ 1.1-003-99. – [Чинний від 28.04.1999]. – К.: ДСТСЗІ СБ України, 1999. 24 с.

6. *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99- [Чинний від 28.04.1999]. – К.: ДСТСЗІ СБ України, 1999. 26 с.*

ORGANIZATIONAL STRUCTURE OF THE CYBERSECURITY SYSTEM IN THE INFORMATION AND TELECOMMUNICATION SYSTEMS OF FIELD COMMUNICATION NODES OF THE COMMAND AND CONTROL LINKS OF THE ARMED FORCES OF UKRAINE

S. Holubtsov
National University "Yuri Kondratyuk Poltava Polytechnic"

УДК 621.391

***С.В. Волоський**, магістрант,*
***М.А. Штомпель**, д.т.н., професор*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

АНАЛІЗ ЗАСТОСУВАННЯ ПАСИВНИХ ОПТИЧНИХ МЕРЕЖ В УМОВАХ ТРИВАЛИХ ВІДКЛЮЧЕНЬ ЕЛЕКТРОЕНЕРГІЇ

Постійні відключення електроенергії, спричинені пошкодженням енергооб'єктів через масовані ракетно-дронові атаки, становлять серйозну загрозу для функціонування телекомунікаційних систем. Критично важливі об'єкти, такі як медичні заклади, фінансові установи, військові структури, потребують стабільного доступу до мережі незалежно від умов.

ДОДАТОК В

Презентаційний матеріал

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

НАВЧАЛЬНО НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА РОБОТОТЕХНІКИ

КАФЕДРА АВТОМАТИКИ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

Кваліфікаційна робота магістра

«ДОСЛІДЖЕННЯ ШЛЯХІВ СТВОРЕННЯ ТА РОЗГОРТАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ВУЗЛІВ ЗВ'ЯЗКУ»

Виконав:
Студент групи д6ТТ Голубцов С.С.
Керівник:
к.т.н., доцент Фомін О. С.

МЕТА ТА ЗАВДАННЯ ДИПЛОМНОЇ РОБОТИ

МЕТА:

ПОЛЯГАЄ В ОБҐРУНТУВАННІ ТА РОЗРОБЦІ ПЕРСПЕКТИВНИХ СХЕМ РОЗГОРТАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЛЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ, ЩО ФУНКЦІОНУЮТЬ В ПУНКТАХ УПРАВЛІННЯ РІЗНИХ ЛАНОК ЗБРОЙНИХ СИЛ УКРАЇНИ.

ЗАВДАННЯ:

1.РОЗРОБЛЕНО ПРОЄКТ ОПЕРАТИВНО-ТАКТИЧНИХ ВИМОГ ДО СИСТЕМ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ ПУНКТІВ УПРАВЛІННЯ ТАКТИЧНОЇ, ОПЕРАТИВНОЇ ТА СТРАТЕГІЧНОЇ ЛАНОК УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ.

1. РОЗРОБЛЕНО ПРОЕКТ ТАКТИКО-ТЕХНІЧНИХ ВИМОГ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ РОЗПОДІЛЕНИХ ПІДСИСТЕМ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ІНТЕРЕСАХ ЗАБЕЗПЕЧЕННЯ ЗАХОДІВ З КІБЕРРОЗВІДКИ, КІБЕРЗАХИСТУ, ВЕДЕННЯ КІБЕРДІЙ (КІБЕРОПЕРАЦІЙ) ТА КІБЕРОБОРОНИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ ПУНКТІВ УПРАВЛІННЯ ТАКТИЧНОЇ, ОПЕРАТИВНОЇ ТА СТРАТЕГІЧНОЇ ЛАНОК УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ.

ОБ'ЄКТ ДОСЛІДЖЕННЯ: Є СИСТЕМА КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ ПУНКТІВ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ.

ПРЕДМЕТ: Є РОЗРОБКА, ОПТИМІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ МЕХАНІЗМІВ І ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ, ЩО ЗАСТОСОВУЮТЬСЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ ПУНКТІВ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ.

НАУКОВА НОВИЗНА РОБОТИ: ПОЛЯГАЄ В РОЗРОБЛЕННІ КОМПЛЕКСНОГО СЦЕНАРІЮ DDOS ІЗ МНОЖИННИМ ОБХОДОМ В НАВЧАЛЬНИХ ЦІЛЯХ.

МЕТОДИ ДОСЛІДЖЕННЯ: ДЛЯ ВИРІШЕННЯ ПОСТАВЛЕНИХ ЗАДАЧ В ДИПЛОМНІЙ РОБОТІ ВИКОРИСТОВУВАЛИСЬ ЗАГАЛЬНОНАУКОВІ ПІДХОДИ ДОСЛІДЖЕННЯ: СИСТЕМНИЙ, ІСТОРИЧНИЙ, МІЖДИСЦИПЛІНАРНИЙ; МЕТОДИ: АНАЛІЗ, СИНТЕЗ, ІНДУКЦІЯ, ДЕДУКЦІЯ, ПОРІВНЯЛЬНИЙ, ВІЗУАЛЬНИЙ (ГРАФІЧНИЙ).

НАУКОВА НОВИЗНА

ОСНОВНІ РЕЗУЛЬТАТИ, ОТРИМАНІ В РОБОТІ ЩО ВИНОСЯТЬСЯ НА ЗАХИСТ:

1. ПРОЕКТ ОПЕРАТИВНО-ТАКТИЧНИХ ВИМОГ ДО СИСТЕМ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ ПУНКТІВ УПРАВЛІННЯ ТАКТИЧНОЇ, ОПЕРАТИВНОЇ ТА СТРАТЕГІЧНОЇ ЛАНОК УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ.

2. СХЕМИ РОЗГОРТАННЯ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ ТАКТИЧНОЇ, ОПЕРАТИВНОЇ ТА СТРАТЕГІЧНОЇ ЛАНОК УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ.

НАУКОВИЙ РЕЗУЛЬТАТ

У ПЕРШОМУ РОЗДІЛІ :

ПРОВЕДЕНО АНАЛІЗ УРАЗЛИВОСТЕЙ, МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ, СИСТЕМ АВТЕНТИФІКАЦІЇ ТА ПРОЦЕДУР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В КОНТЕКСТІ ВІЙСЬКОВИХ ОПЕРАЦІЙ. ТАКОЖ РОЗГЛЯНУТО ФУНКЦІОНУВАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ НА ТАКТИЧНОМУ, ОПЕРАТИВНОМУ ТА СТРАТЕГІЧНОМУ РІВНЯХ УПРАВЛІННЯ, А ТАКОЖ ЇЇ ВПЛИВ НА СИСТЕМУ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ ТА АВТОМАТИЗОВАНЕ УПРАВЛІННЯ ВІЙСЬКАМИ.

Сьогодні функціонування системи кібербезпеки (далі – СКБ) в інформаційно-телекомунікаційних системах польових вузлів зв'язку (далі – ІТС ПВЗ) на тактичному, оперативному та стратегічному рівнях управління відбувається в умовах активного протистояння збройній агресії та анексії Криму з боку Російської Федерації. Протягом конфлікту на сході України Збройні Сили України (далі – ЗС України) змогли розгорнути досить сучасну і ефективну систему зв'язку, що стала однією з найкращих в історії незалежності держави.

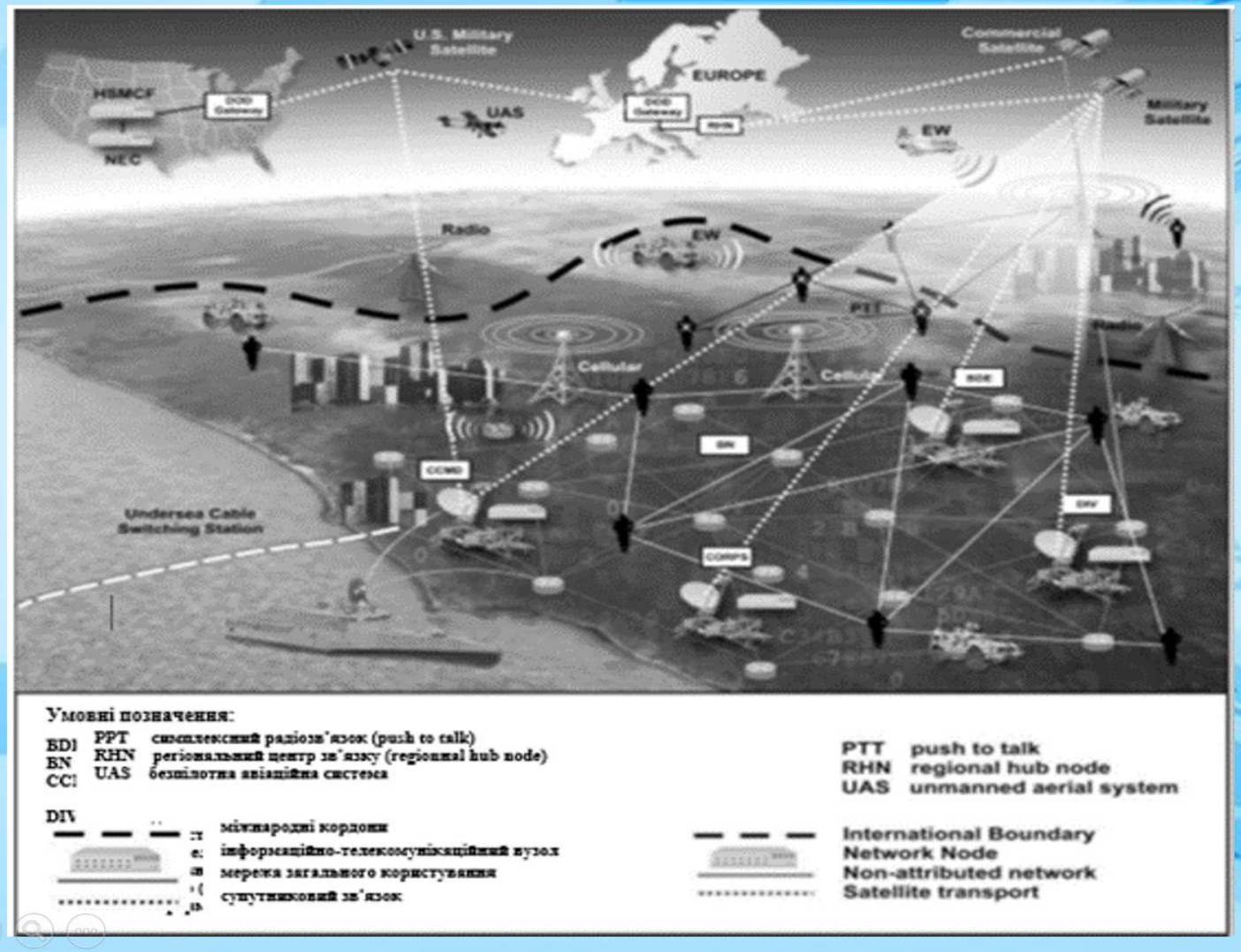
Ця система управління (далі – СУ) забезпечує надійність, стійкість і безперервність управління військами (далі – УВ) у пунктах постійної дислокації та в районах виконання завдань, зокрема під час операції об'єднаних сил (далі – ОС). Керівні органи всіх рівнів управління виконують свої функції за призначенням, незважаючи на оптимізацію та перехід на структури штабів військ НАТО, а також на переоснащення та нарощування системи зв'язку.

Аналізуючи функціонування СКБ в ІТС країн НАТО на різних рівнях управління, включаючи ПУ та СУ в цілому, важливо зазначити, що для набуття спроможностей у КП, коли основною метою є досягнення стратегічних цілей, необхідно розглядати їх як взаємопов'язані дії, які поділяються на [3]:

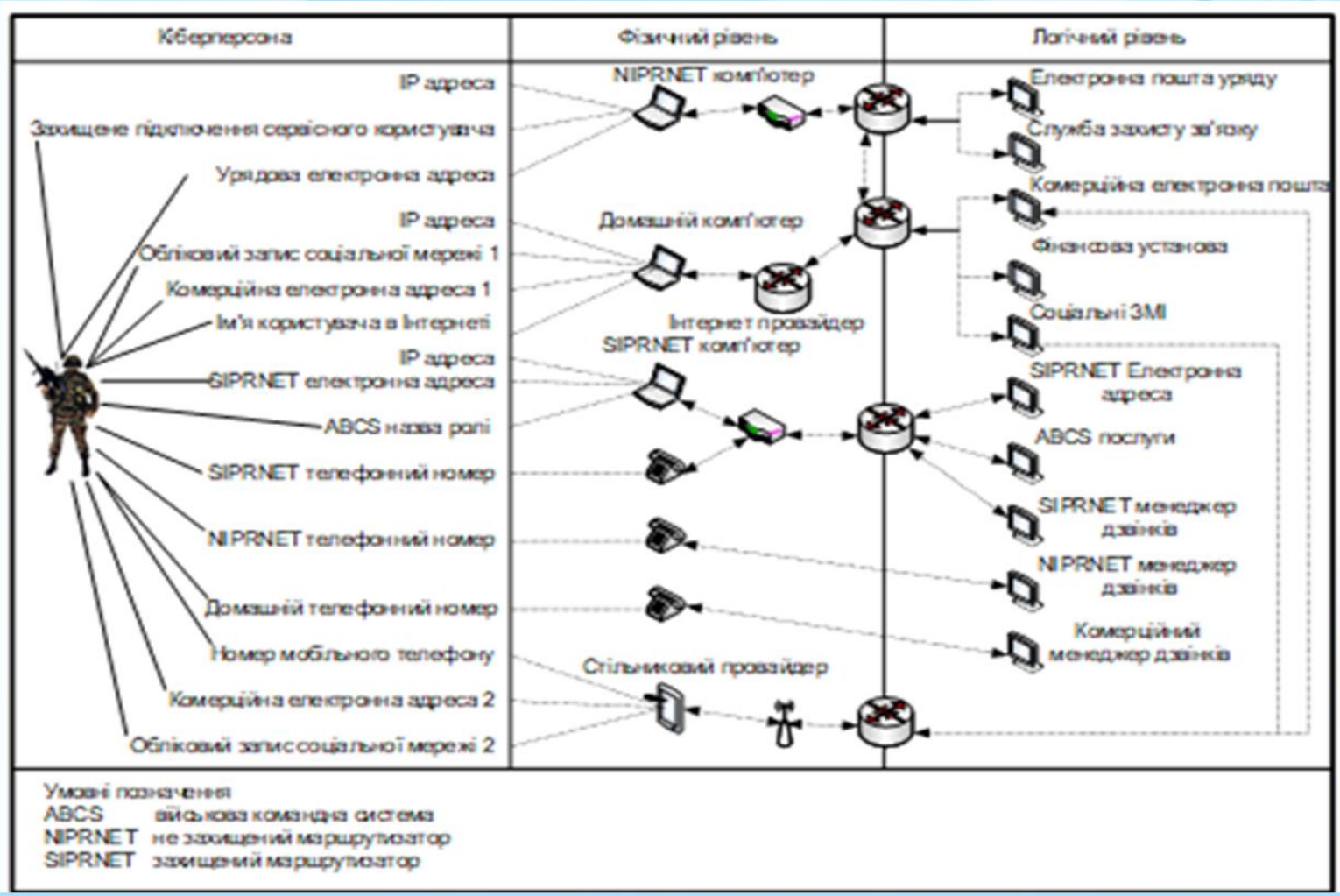
- Операції в ІТС ОВУ стратегічного рівня країн НАТО.
- Оборонні кібероперації (далі – КО).
- Наступальні КО.

До засобів протиборства у КП належать апаратні комплекси, програмні засоби та апаратно-програмні комплекси, що можуть включати будь-яке поєднання програмного забезпечення (далі – ПЗ), програмно-апаратних засобів або апаратного забезпечення.

Вони призначені для забезпечення впливу у КП або як наслідок дій, які в ньому здійснюються. На Рисунку 1.1



ІТС оперативного управління стратегічної ЛУ є частиною КП країн блоку НАТО (Рис.1.2.). Їхня ключова характеристика полягає в здатності забезпечувати обмін інформацією між військами (силами) у різних сферах ведення БД.



Операції ЗС країн-членів НАТО значною мірою залежать від КП, особливо в аспектах синхронізації, зберігання, координації та захисту інформації (далі – ЗІ) (Рисунок 1.3.). ОВУ різних ЛУ використовують можливості КП, проте їхня діяльність не обмежується цими можливостями, навіть у випадку зменшення їхньої ефективності при досягненні цілей командувача ОС [3].

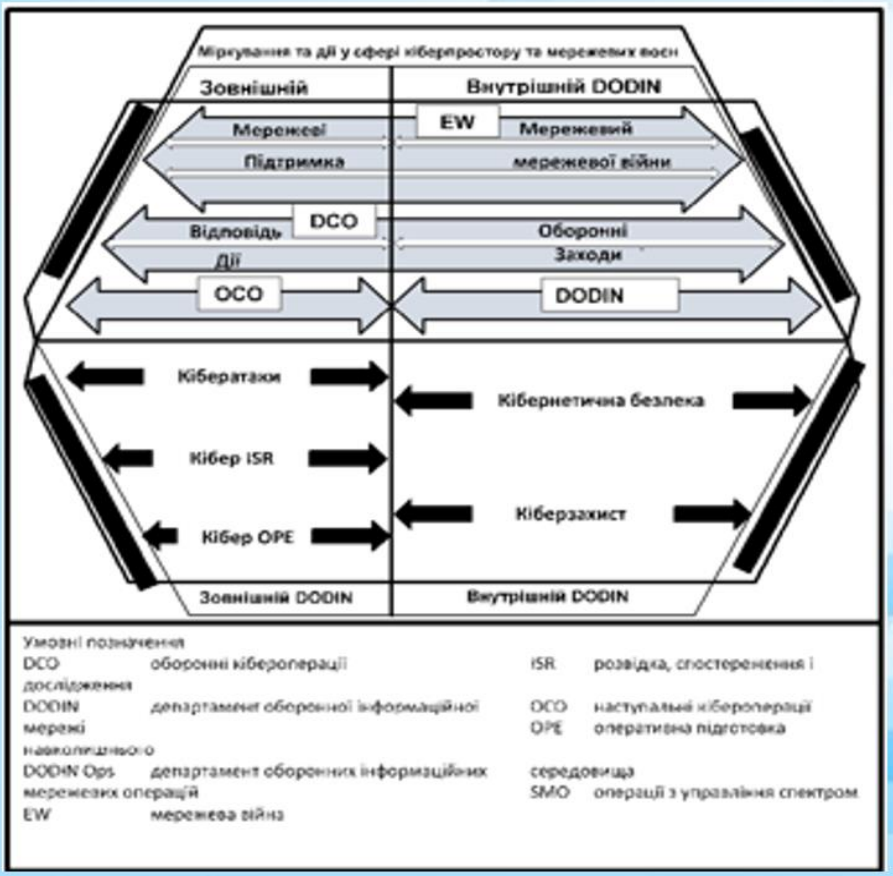


Рисунок 1.3. – Спроможності ЗС країн-членів НАТО у КП щодо синхронізації, зберіганні, координації та ЗІ під час ведення операцій

Таким чином, свобода маневру у використанні КП для виконання завдань командира реалізується через зосереджене планування бойового застосування (далі – БЗ) КП від стратегічної ЛУ до підрозділів тактичної ЛУ (Рисунок – 1.4). Забезпечуючи реалізацію принципу делегування повноважень та свободи дій у КП, операції, які проводять американські збройні сили та їхні союзники, сприяють досягненню поставлених цілей командувача ОС

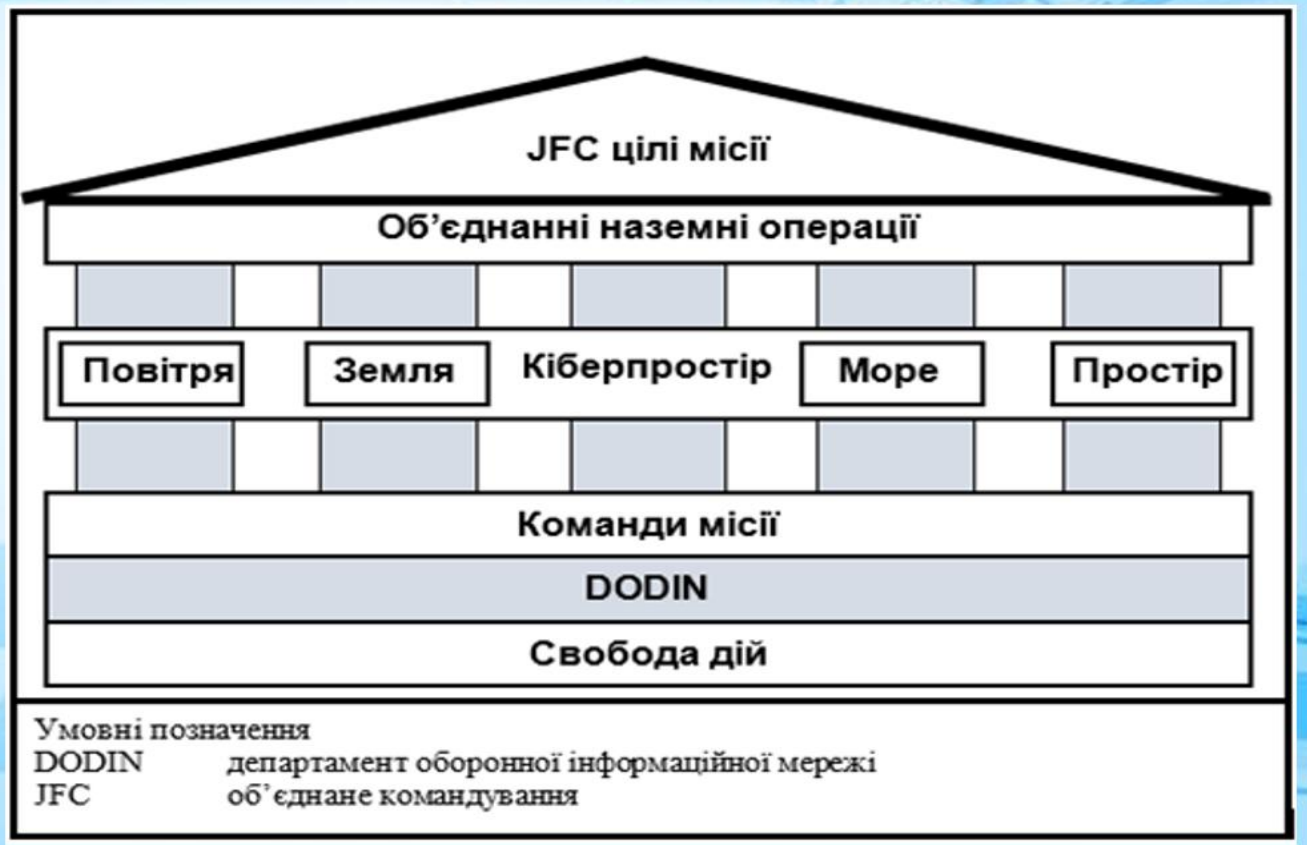


Рисунок 1.4. – Свобода маневру та підтримки цілей командуючого ОС (угрупованням)

Сегментом країн-членів НАТО в ІТС департаменту оборонної ІМ є технічна мережа, яка охоплює СУ інформацією та інформаційні системи, що накопичують, обробляють, зберігають, відображають, розповсюджують та забезпечують ЗІ в глобальному масштабі.

КО, що здійснюються, можуть підтримувати або бути підтриманими КО ОС. Взаємна підтримка та тісна координація між ОС під час проведення КО забезпечують керівництву та штабам більші можливості для планування БЗ військових частин та підрозділів.

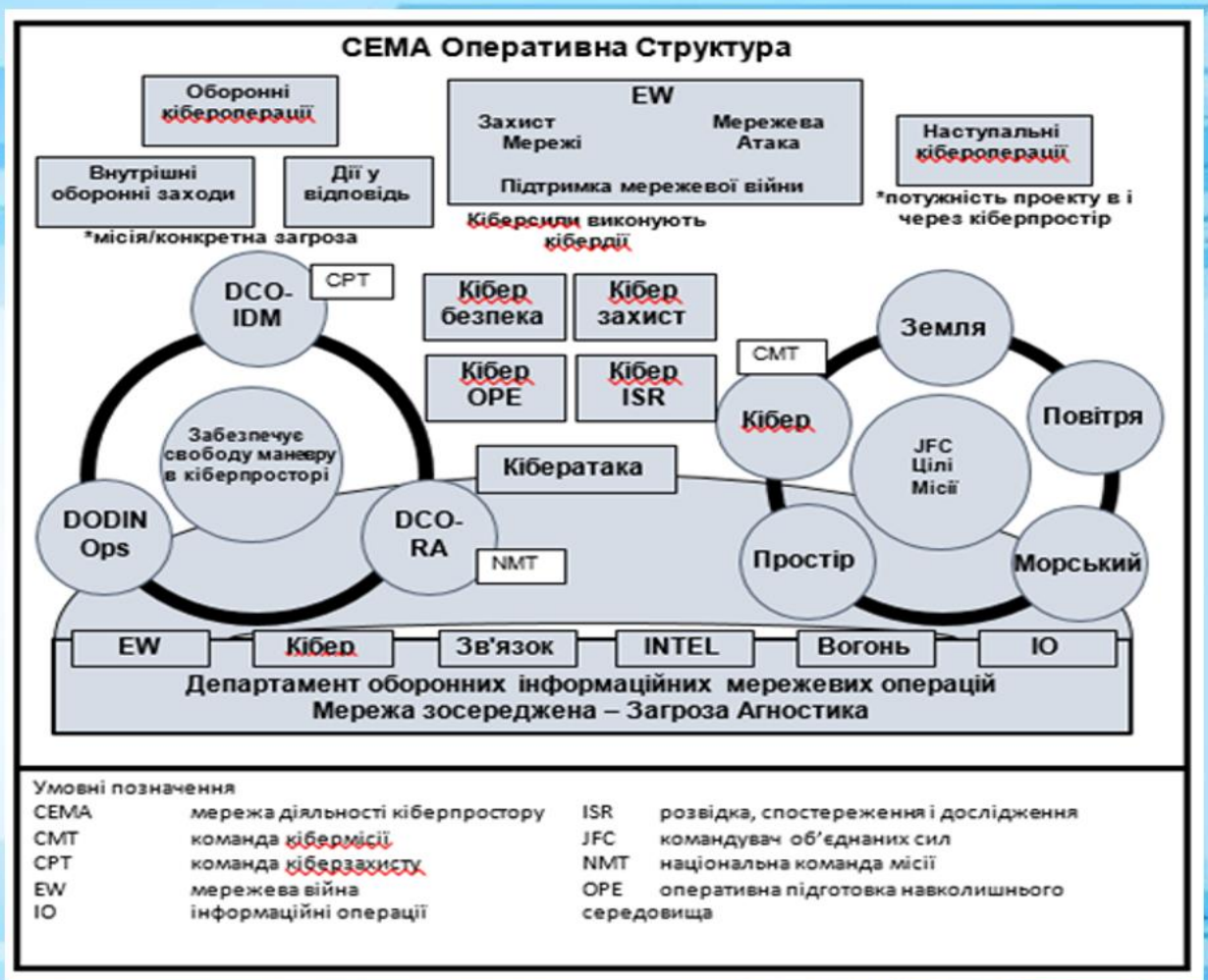


Рисунок 1.5. – Дії у кіберпросторі ЗС країн-членів НАТО

НАУКОВИЙ РЕЗУЛЬТАТ

Розроблено заходи кібероборони. Форми застосування ЗС України у національному сегменті кіберпростору.

Успішна реалізація цих заходів можливе лише за умови якісного планування (Рисунок – 1.6.). Важливо розробити детальні плани, які враховують всі можливі загрози і варіанти реагування, що, в свою чергу, підвищує стійкість та ефективність КБ в ІТС ПВЗ ПУ.

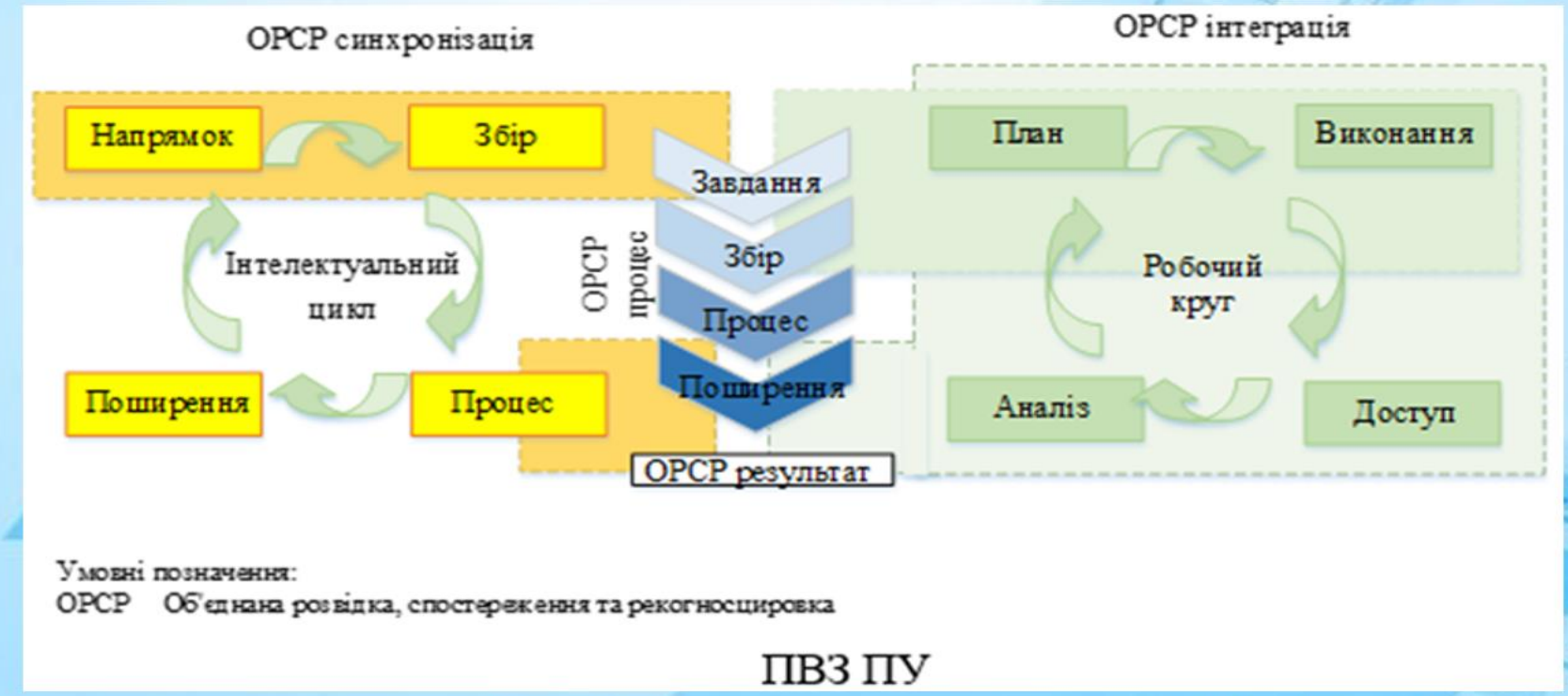


Рисунок 1.6. – Планування виконання заходів КБ в ІТС

Завдання з КБ в ІТС ПВЗ ПУ різних ЛУ ЗС України вимагають застосування різноманітних дій для створення спеціальних впливів у КП. Це передбачає активну взаємодію з іншими відомствами та установами для максимально ефективного вирішення питань, пов'язаних із, Кзаг в рамках нормативно-правового поля. Завдання з КБ в ІТС ПВЗ ПУ різних ЛУ ЗС України вимагають застосування різноманітних дій щодо створення спеціальних впливів у КП (Рисунок – 1.7.)

Рисунок 1.7. – Дії у кіберпросторі

КОб в ІТС ПУ стратегічної ЛУ включає заходи, спрямовані на захист, використання та оборону систем від конкретних загроз у КП. Основною метою КОб є виявлення, визначення, протидія, зниження ризиків і захист інформаційних систем від загроз.

Ці оборонні заходи, як правило, виконуються ГОЦЗІ та КБ ІТС ЗСУ. Важливо зазначити, що ці дії можуть бути обмежені, якщо вони можуть вплинути на роботу мереж, які знаходяться поза межами відповідальності ІТС ЗС України.

Розвідка, спостереження та рекогносцирування в ІТС ПУ здійснюються через проведення розвідувальної діяльності, що виконується Центрами ЗІ та кібернетичної безпеки ГОЦЗІКБ ІТС ЗС України. Ці центри функціонують в інтересах оперативних командувань за територіальним принципом.

Зокрема, діють такі центри [12]:

- 3-й Центр у м. Дніпро, що обслуговує оперативне командування “Схід”;
- 7-й Центр у м. Рівне, що підтримує оперативне командування “Захід”;
- 8-й Центр у м. Одеса, що працює в інтересах оперативного командування “Південь”;
- 9-й Центр у м. Вінниця, що обслуговує командування Повітряних Сил;
- 4-й Центр у м. Чернігів, що підтримує оперативне командування “Північ”;
- 6-й Центр у м. Миколаїв, що працює на користь командування Військово-Морських Сил.

Ця мережа центрів забезпечує ефективну координацію та виконання розвідувальних завдань, що критично важливо для успішного функціонування військових операцій в умовах сучасних загроз (Рисунок – 1.8.)

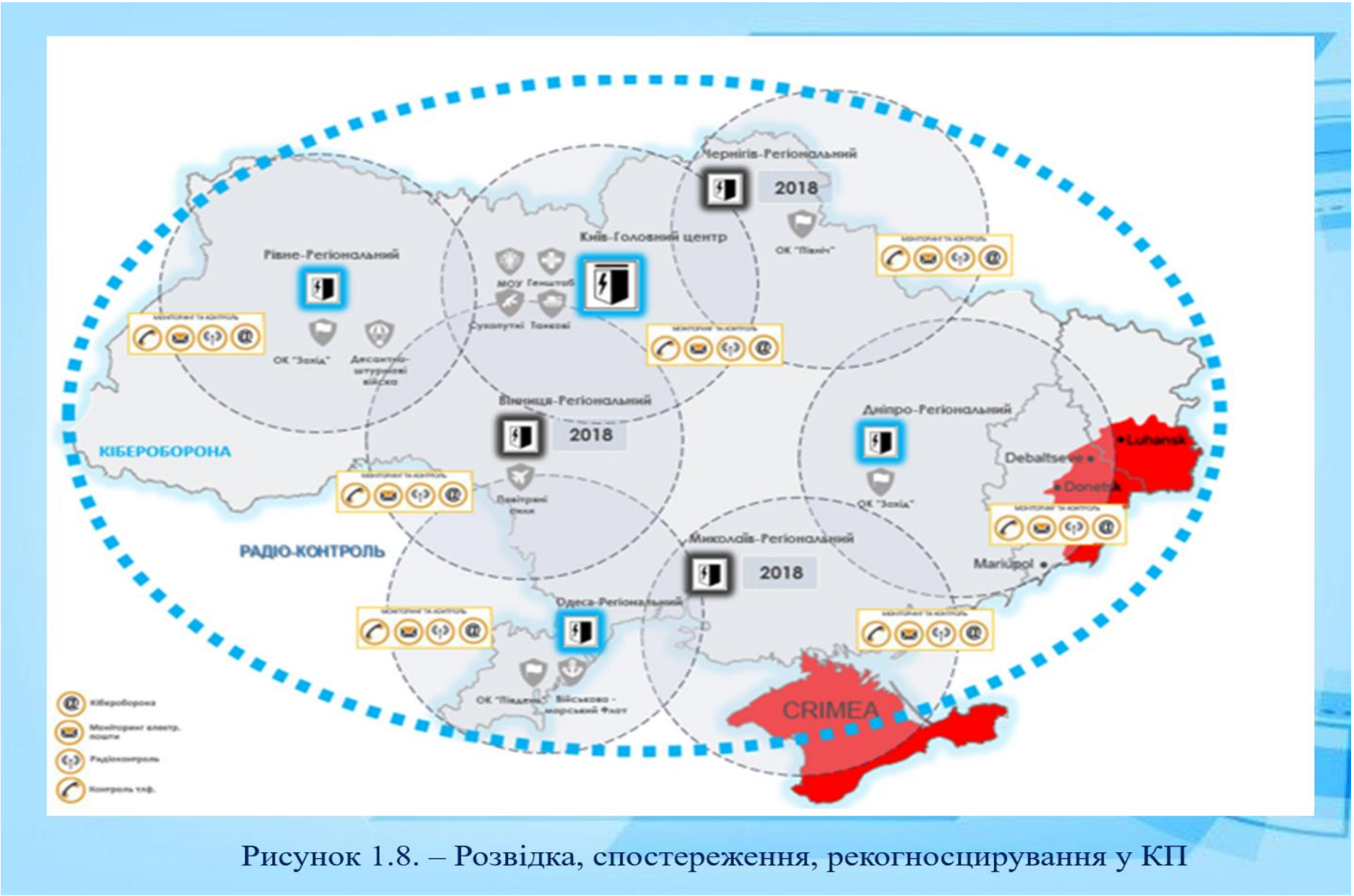
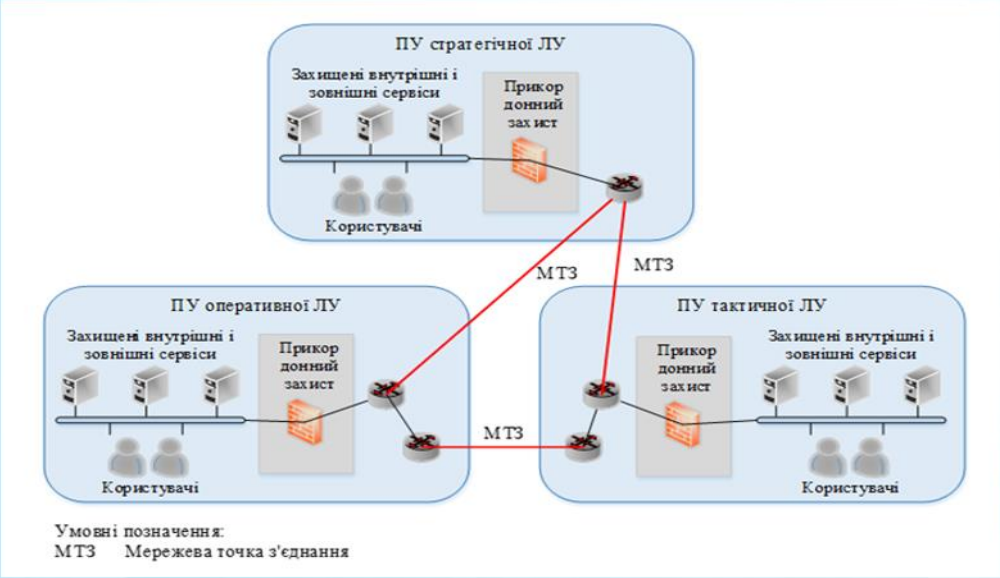


Рисунок 1.8. – Розвідка, спостереження, рекогносцирування у КП

НАУКОВИЙ РЕЗУЛЬТАТ

ДРУГИЙ РОЗДІЛ КВАЛІФІКАЦІЙНОЇ РОБОТИ ПРИСВЯЧЕНИЙ РОЗРОБЦІ ПРОЕКТУ ОПЕРАТИВНО-ТАКТИЧНИХ ВИМОГ ДО СИСТЕМИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ НА ТАКТИЧНОМУ, ОПЕРАТИВНОМУ ТА СТРАТЕГІЧНОМУ РІВНЯХ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ.



Загальна вимога до обладнання, яке буде розгорнуто на ПВЗ, полягає в тому, що комплекси КБ мають формувати збалансований та взаємодіючий комплект засобів управління інфраструктурою КБ в інформаційно-технічних системах (далі – ІТехС) Міністерства оборони України та ЗС України на стратегічному, оперативному та тактичному рівнях.

Рисунок 2.1. – Схема розгортання КБ в ІТС ПВЗ тактичної, оперативної та стратегічної ЛУ ЗС України

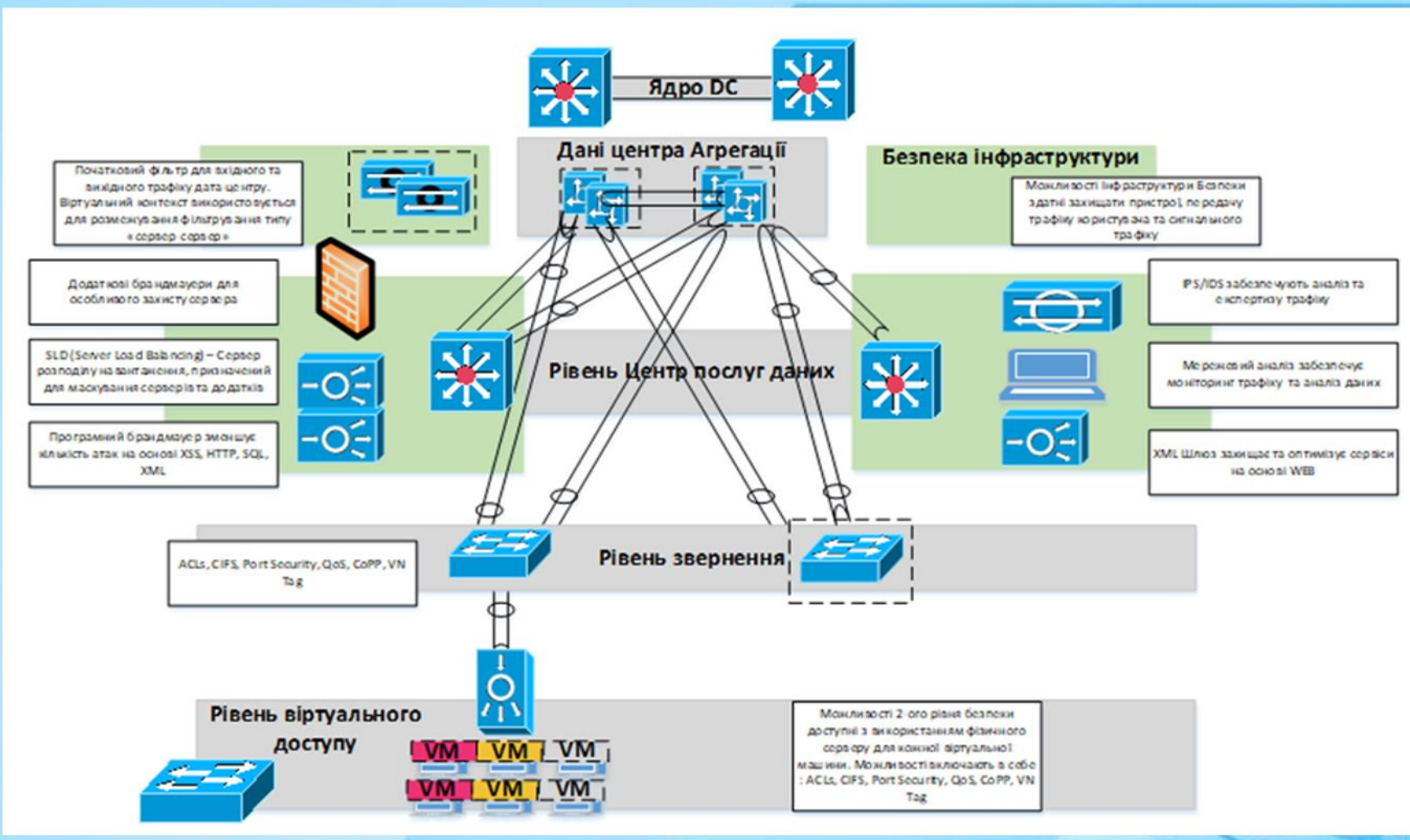


Рисунок 2.2. – Типова схема розгортання КБ в ІТС ПВЗ тактичної ланки управління ЗС України

Однією з основних задач міжмережевих екранів в ІТС ПВЗ (Рисунок – 2.3.) для будь-якої ЛУ є захист мережевих сегментів або окремих хостів від НСД, зокрема через вразливості в протоколах мережевої моделі OSI або ПЗ на ПК. Міжмережеві екрани аналізують трафік, порівнюючи його характеристики з попередньо визначеними шаблонами, що дозволяє пропускати або блокувати дані в залежності від встановлених правил.

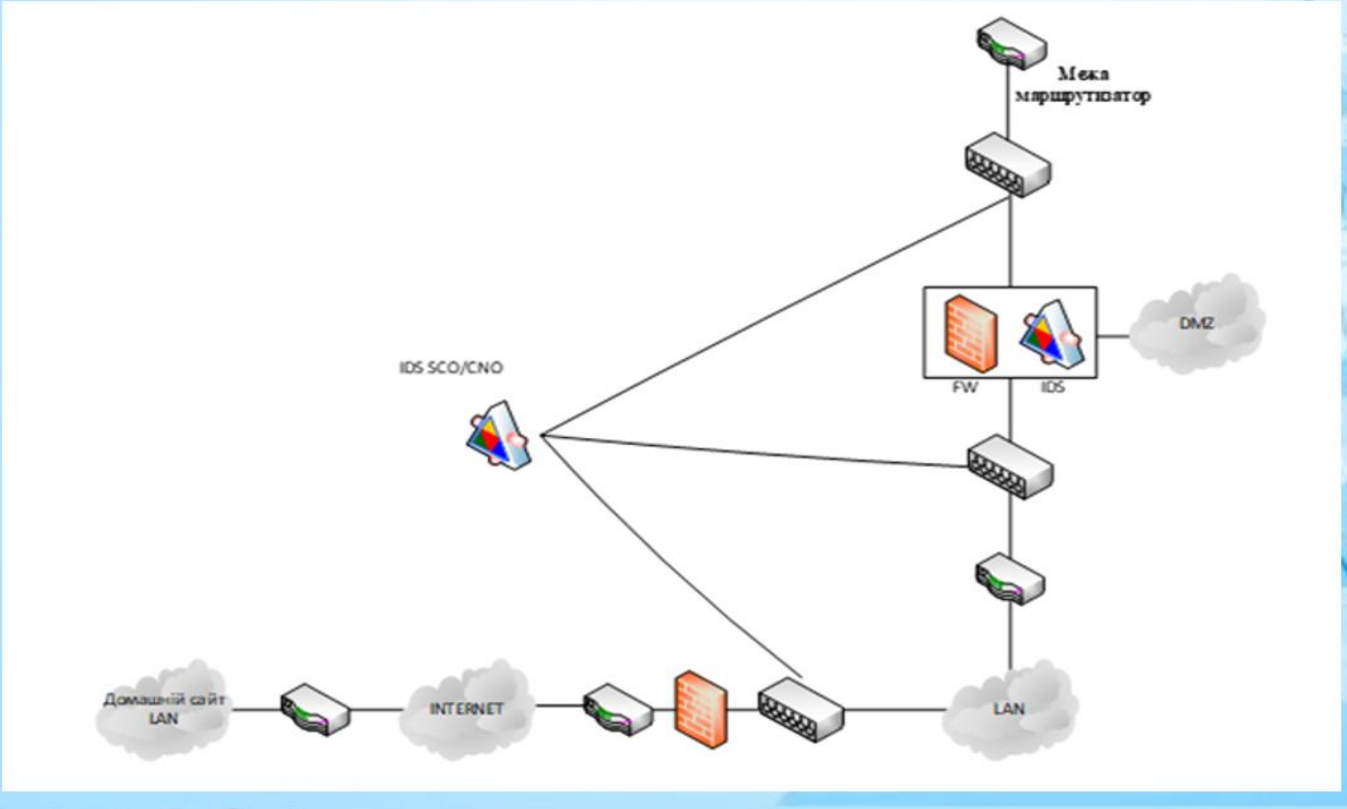


Рисунок 2.3. – Міжмережеві екрани в ІТС ПВЗ РУ

Принцип роботи віртуальних приватних мереж полягає в тунелюванні трафіку через телекомунікаційні мережі, такі як мережа ЗС України або Інтернет. Реалізація технології здійснюється за допомогою спеціальних пристроїв – кріптошлюзів. Ці пристрої не лише забезпечують захист локальної мережі від зовнішніх загроз, але й здійснюють маршрутизацію трафіку. VPN відрізняється від традиційних рішень на основі виділених каналів завдяки своїй гнучкості, масштабованості та нижчій вартості, а також високому рівню ЗІ.

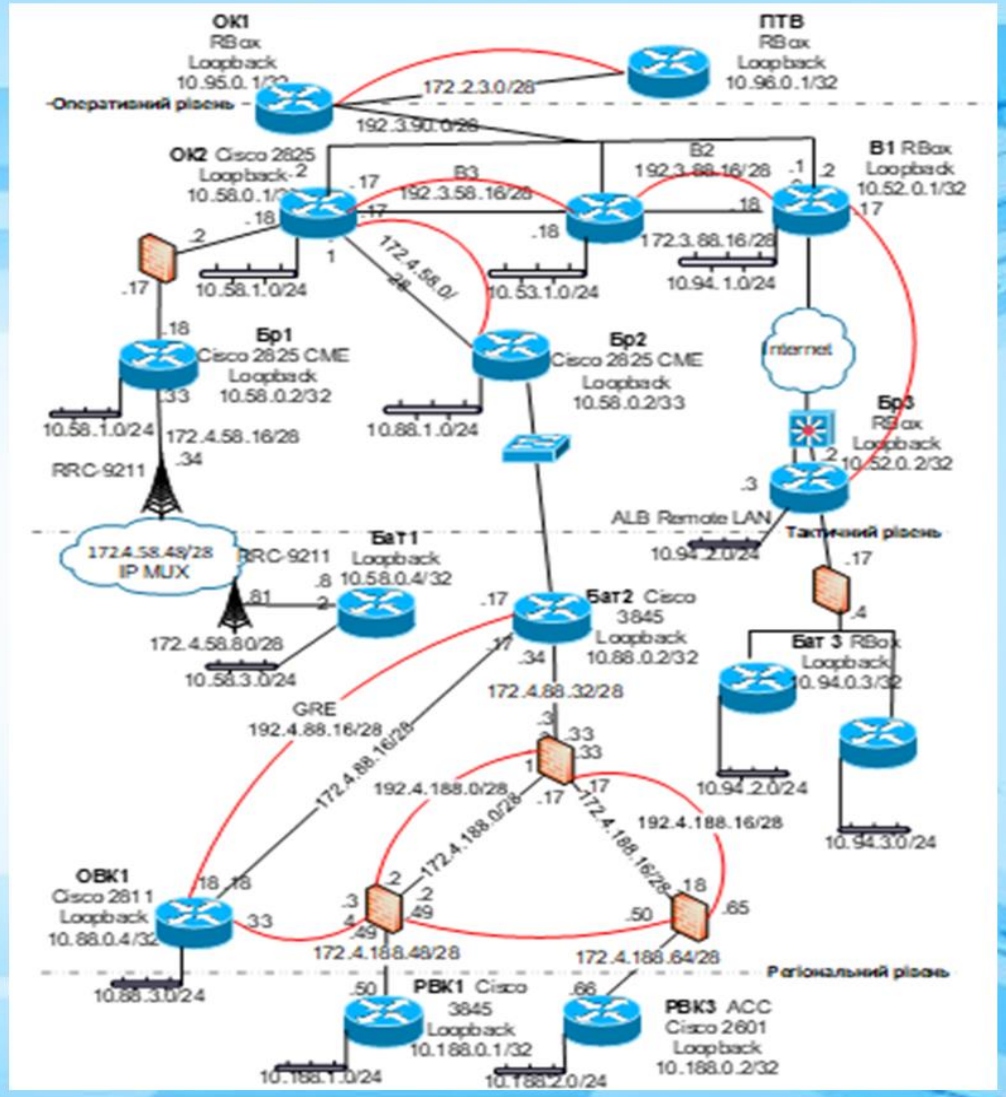


Рисунок 2.4. – Реалізація КБ в ІТС ПВЗ ПУ через VPN

Інфраструктура відкритих ключів (PKI) (Рисунок – 2.5.) являє собою комплекс засобів – технічних, матеріальних та людських — а також розподілених служб і компонентів, які використовуються для забезпечення криптографічних задач на основі закритих і відкритих ключів. Ця система підтримує безпечний обмін інформацією, аутентифікацію користувачів та забезпечує цілісність даних.

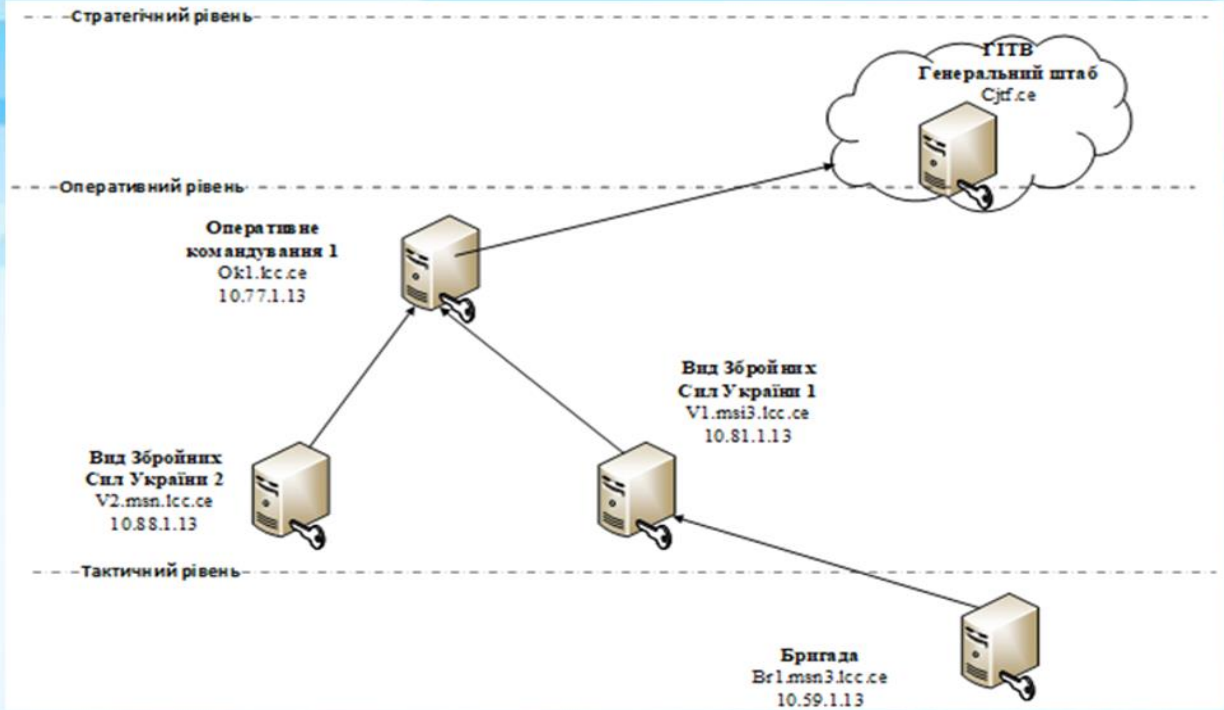


Рисунок 2.5. – Інфраструктура відкритих ключів системи КБ в ІТС ПВЗ ПУ різних ЛУ

У ТРЕТЬОМУ РОЗДІЛІ РОБОТИ БУЛИ РОЗРОБЛЕНІ МОЖЛИВІ ВАРІАНТИ СХЕМ РОЗГОРТАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ РІЗНИХ ЛАНОК УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ. ТАКОЖ ЗАПРОПОНОВАНО ПЕРЕЛІК НЕОБХІДНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЕФЕКТИВНОГО РОЗГОРТАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ПОЛЬОВИХ ВУЗЛІВ ЗВ'ЯЗКУ НА ТАКТИЧНОМУ, ОПЕРАТИВНОМУ ТА СТРАТЕГІЧНОМУ РІВНЯХ УПРАВЛІННЯ.

Склад СКБ в ІТС ПВЗ ПУ стратегічної ЛУ ЗС України стратегічної, оперативної та тактичної ЛУ ЗС України [23]:

- підсистема КЗ периметру Додаток 1 (Таблиця 1);
- підсистема відображення обстановки та керування інфраструктурою КБ в ІТС СКБ в ІТС ПВЗ ПУ стратегічної, оперативної та тактичної ЛУ ЗС України з підтримкою віртуалізації Додаток 2 (Таблиця 2);
- сервер КЗ Додаток 3 (Таблиця 3);
- підсистема комутації Додаток 4 (Таблиця 4);
- джерело безперебійного живлення UPS 220V, 50Hz, 1000VA, 19" вбудовуємий Додаток 5 (Таблиця 5);
- монтажний кейс на 19", 6U Додаток 6 (Таблиця 6).

В цілому склад СКБ в ІТС ПВЗ ПУ різних ЛУ ЗС України розроблений за функціональними завданнями, як самостійно, так і у складі кожної ЛУ.

- ПЗ, основні характеристики складових ПЗ та порядок продовження сервісної підтримки для існуючих міжмережевих екранів в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України Додаток 7 (Таблиця – 7);
- ПЗ, основні характеристики складових ПЗ моніторингу, аналізу мережевої поведінки та виявлення аномалій в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ЛУ ЗС України Додаток 8 (Таблиця – 8).

ВИСНОВОК

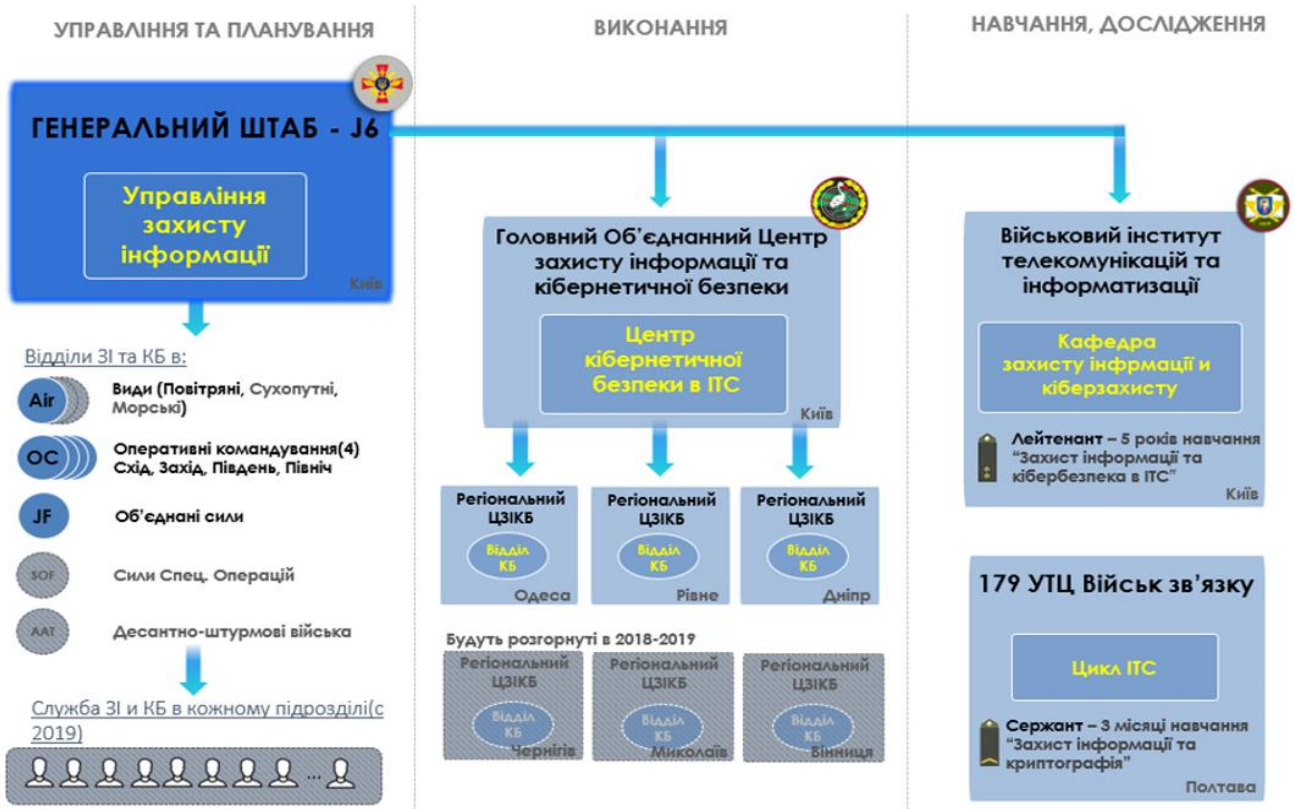
У ДАНІЙ РОБОТІ РОЗГЛЯНУТО КЛЮЧОВІ ВИМОГИ ДО СТВОРЕННЯ ТА РОЗГОРТАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ІТС ПУ ЗС УКРАЇНИ. ОСНОВНОЮ ВИМОГОЮ СТАЛА ЕВОЛЮЦІЙНІСТЬ СИСТЕМИ, ЯКА ПОВИННА АДАПТУВАТИСЯ ДО ЗМІН У КІБЕРСЕРЕДОВИЩІ ПРОТЯГОМ УСЬОГО ЖИТТЄВОГО ЦИКЛУ. ПІДКРЕСЛЕНО, ЩО ДЛЯ ЕФЕКТИВНОГО ЗАХИСТУ НЕОБХІДНИЙ КОМПЛЕКСНИЙ ПІДХІД, ЩО ВКЛЮЧАЄ ТЕХНІЧНІ, ОРГАНІЗАЦІЙНІ ТА НОРМАТИВНІ ЗАХОДИ.

ТАКОЖ АКЦЕНТОВАНО НА ВАЖЛИВОСТІ ІНТЕГРАЦІЇ РІЗНОМАНІТНОГО ОБЛАДНАННЯ ВІД РІЗНИХ ВИРОБНИКІВ, ЩО ЗАБЕЗПЕЧИТЬ ГНУЧКІСТЬ І МОЖЛИВІСТЬ МОДЕРНІЗАЦІЇ СИСТЕМИ. НЕОБХІДНО ТАКОЖ ОБМЕЖИТИ КОЛО ОСІБ, ДОПУЩЕНИХ ДО НАЛАШТУВАННЯ СИСТЕМИ, ТА ВИКОРИСТОВУВАТИ АВТОМАТИЗОВАНІ РІШЕННЯ ДЛЯ ЗНИЖЕННЯ РИЗИКІВ, ПОВ’ЯЗАНИХ З ЛЮДСЬКИМ ФАКТОРОМ. ЗАГАЛОМ, ПІДКРЕСЛЮЄТЬСЯ ВАЖЛИВІСТЬ КОМПЛЕКСНОГО І АДАПТИВНОГО ПІДХОДУ ДО КІБЕРБЕЗПЕКИ В УМОВАХ СУЧАСНИХ ЗАГРОЗ.

ВИСНОВОК

ДОДАТОК Ї

Структура Головного Об'єднаного Центру захисту інформації та кібернетичної безпеки



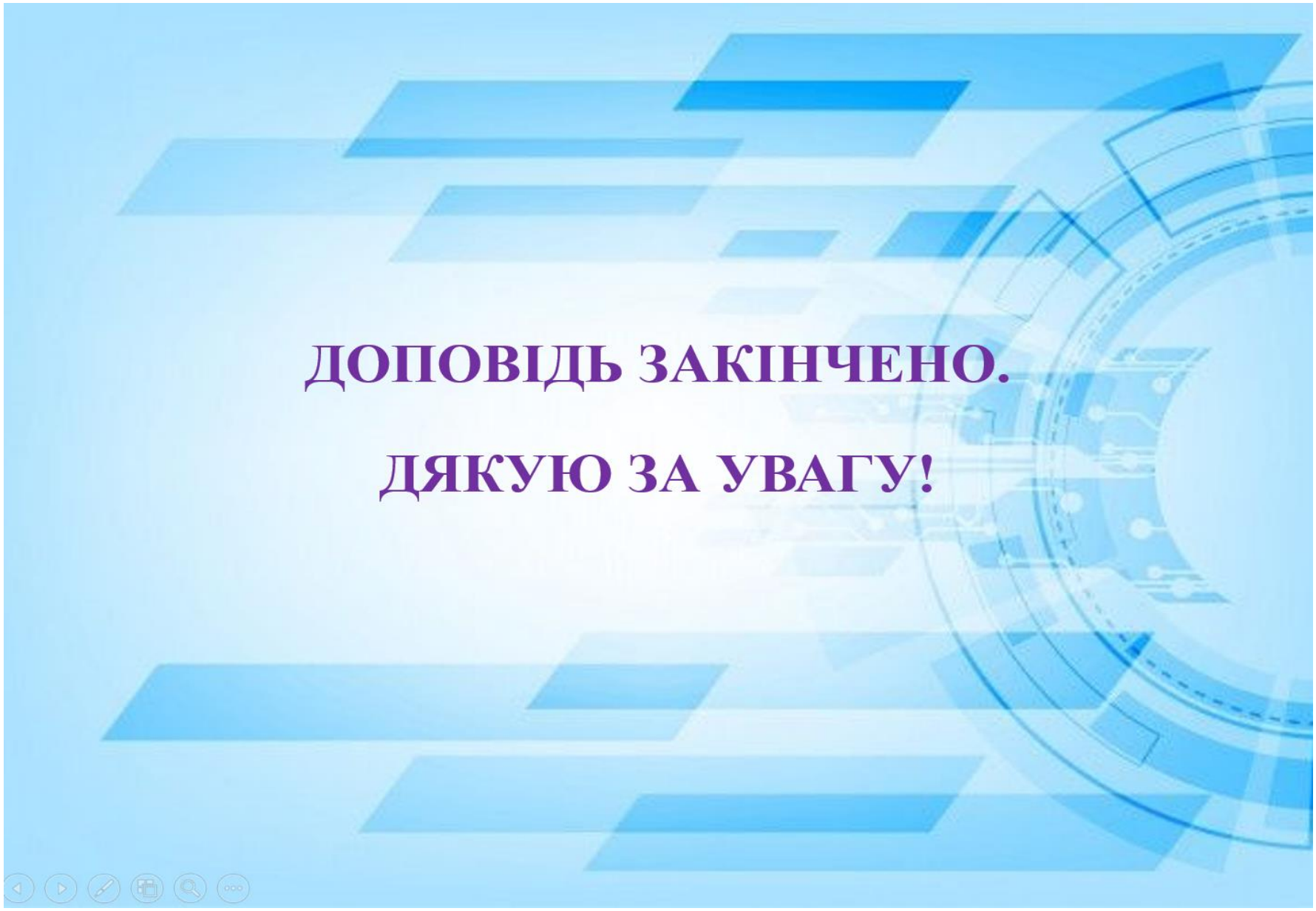
ВИСНОВОК

ДОДАТОК Й

Завдання Головного Об'єднаного Центру захисту інформації та кібернетичної безпеки

ВИСНОВОК

ДЛЯ ДОСЯГНЕННЯ ЦІЄЇ МЕТИ ВАЖЛИВО ВИКОРИСТОВУВАТИ ОБЛАДНАННЯ ВІД РІЗНИХ ВИРОБНИКІВ, ТАКИХ ЯК CISCO, MICROTIC, HP, IBM, JUNIPER ТОЩО. ЦЕ ДОЗВОЛИТЬ ОРГАНІЗУВАТИ ВЗАЄМОКОНТРОЛЬ МІЖ РІЗНИМИ КОМПОНЕНТАМИ ТА СПРИЯТИ ОБМІНУ ІДЕЯМИ ТА НАПРАЦЮВАННЯМИ, ЩО ПІДВИЩИТЬ ЗАГАЛЬНУ ЕФЕКТИВНІСТЬ СИСТЕМИ. В УМОВАХ ІНТЕНСИВНОГО РОЗВИТКУ РИНКУ АПАРАТНО-ПРОГРАМНИХ КОМПЛЕКСІВ КІБЕРБЕЗПЕКИ НЕОБХІДНО ПРИДІЛЯТИ УВАГУ ОСНОВНИМ ХАРАКТЕРИСТИКАМ ПРОДУКТІВ, ТАКИМ ЯК ПРОДУКТИВНІСТЬ, АЛГОРИТМИ ШИФРУВАННЯ, КЛЮЧОВІ СХЕМИ ТОЩО. ЦІ АСПЕКТИ БЕЗПОСЕРЕДНЬО ВПЛИВАЮТЬ НА ЕФЕКТИВНІСТЬ ЗАХИСТУ СИСТЕМИ.


ДОПОВІДЬ ЗАКІНЧЕНО.
ДЯКУЮ ЗА УВАГУ!

ДОДАТОК Г

(Перелік умовних позначень, скорочень і термінів)

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АРМ	–	Автоматизоване робоче місце
АСУ	–	Автоматизована система управління
АУВ	–	Автоматизоване управління військами
БД	–	Бойові дії
БЗ	–	Бойове застосування
ГОЦЗІ та КБ	–	Головний об’єднаний центр захисту інформації та кібернетичної безпеки
ГШ ЗСУ	–	Генеральний штаб Збройних Сил України
ЗІ	–	Захист інформації
ІВФ	–	Інші військові формування
ІМ	–	Інформаційні мережі
ІР	–	Інформаційні ресурси
ІС	–	Інформаційні системи
ІТ	–	Інформаційні технології
ІТехС	–	Інформаційно-технічна система
ІТС	–	Інформаційно-телекомунікаційна система
КА	–	Кібератака
КБ	–	Кібербезпека
КВ	–	Кібервплив
КД	–	Кібердії
КЗ	–	Кіберзахист
КЗаг	–	Кіберзагроза
КО	–	Кібероперація
КОб	–	Кібероборона
КП	–	Кіберпростір
КР	–	Кіберрозвідка
КС	–	Кіберсередовище
ЛУ	–	Ланка управління
НАТО	–	Організація Північноатлантичного договору
НСД	–	Несанкціонований доступ
ОВУ	–	Органи військового управління
ОДВ		Органи державної влади
ОМ	–	Обчислювана машина
ОС	–	Об’єднані сили
ОС	–	Операційна система
ОУ	–	Органи управління
ПВЗ	–	Польовий вузол зв’язку
ПЗ	–	Програмне забезпечення
ПрО	–	Правоохоронні органи
РЕБ	–	Радіоелектронна боротьба
РП	–	Розподілені підсистеми

СКБ	–	Система кібербезпеки
СУ	–	Система управління
УВ	–	Управління військами
ЦОРІ КБ	–	Центр оперативного реагування на інциденти кібербезпеки
ALG	–	Application Layer Gateway SIP
AVC	–	Application Visibility and Control
BGP	–	Border Gateway Protocol
CAPEC	–	Common Attack Pattern Enumeration and Classification Загальний набір шаблонів атак та їх класифікація
CISCO	–	Американська транснаціональна компанія
DSCP	–	Differentiated Services Code Point
MITRE	–	Massachusetts Institute of Technology Roberta Everetta Масачутський Інститут Технологій ім. Roberta Everetta
NGIPS	–	Threat Defense
NSF	–	Non Stop Forwarding
OWASP	–	Open Web Application Security Project Відкритий проект безпеки веб-додатків
RTBH	–	Remotely Triggered Black Hole
US-CERT	–	Команда реагування на кібернетичні інциденти США
WASC	–	Web Application Security Consortium Консорціум безпеки з веб-додатків
Wi-Fi	–	Wireless Fidelity Бездротова передача цифрових потоків даних по радіоканалах

ДОДАТОКИ Ґ

(Призначення та основні характеристики складових підсистеми кібернетичного захисту периметру)

Додаток Ґ.

Назва параметру складової підсистеми	Певні особливі вимоги
Міжмережевий екран з IPS (для ПВЗ ПУ стратегічної ЛУ до 1 Гбіт/с) у складі: **Кріплення** для встановлення в шафу; **Блок живлення** не менш ніж 250W (або вбудований) – 1шт.; **Ліцензовані опції** на використання функціоналу Application Visibility and Control (AVC), Threat Defense (NGIPS), Malware Protection (AMP) та URL Filtering (URL) у режимі NGFW або еквівалент – строком не менш ніж на 3 роки.	
Архітектура	Зразок у складі пристрою обробки трафіку, ПЗ, відповідних ліцензій та засобів взаємодії з ПЗ керування та моніторингу пристроями КБ, збору журнальної інформації та формування звітності безпеки.
Фізичні характеристики	Наявність пристрою обробки трафіку з характеристиками, не гірше: форм-фактор пристрою обробки трафіку не вище ніж 1 монтажна одиниця (1 rackunit); не менше одного блока живлення 250W від промислової мережі 220В/50Гц; зовнішній порт USB – не менше ніж 1 (v2.0); накопичувачі – не менше ніж один твердотільний накопичувач (SSD) ємністю не менш ніж 100 ГБ; кількість портів LAN/WAN: не менш ніж 12 портів 10/100/1000G RJ-45 та 4 порта 1G SFP для встановлення відповідних трансіверів; порт керування – окремий, не менше ніж 1 порт 10/100/1000 Мбіт/с, Ethernet;
Сервіси мережевого захисту	Класичний міжмережевий екран – stateful firewall. Режим роботи в мережі: L3 firewall, L2 firewall, virtual firewall context, підтримка одночасної робота віртуальних контекстів в L2 та L3 на одному пристрої: Не менше ніж 2 віртуальних міжмережевих екранів з контролем ресурсів, що виділяються та власним керуванням; Підтримка не менше ніж 25 таких віртуальних міжмережевих екранів. Відмовостійкість: Active/Active, обов'язково з синхронізацією станів сесій. Active/Standby. Міжмережевий екран з функціями ідентифікації: автентифікація користувачів в активному каталозі (MS AD агент); можливість формування та виконання політики доступу по групам користувачів з різних каталогів (MS AD, multiforest AD чи LDAP); можливість формування та виконання політики доступу по групам пристроїв. Інспекція на прикладному рівні: Application Layer Gateway SIP (ALG) в тому числі через TLS-proxy; Інспекція корректності роботи (Ipv4 опції; DNS over UDP, HTTP FTP, H.323/H.225);

Назва параметру складової підсистеми	Певні особливі вимоги
	інспекція GTP при додаванні відповідної ліцензії. Функції захисту від DdoS атак. Виявлення та класифікація мережевого трафіку додатків прикладного рівня (Application firewall). Розпізнавання не менше 4 000 додатків. Захист від мережевих атак з наступним функціоналом: statefull DPI на рівнях 3–7 моделі OSI; виявлення спроб НСД в режимі реального часу; попередження спроб НСД в режимі реального часу шляхом блокування або завершення небажаних мережевих сесій; вбудовані сигнатури IPS довічної дії; протидія технікам обходу захисту; підписка на оновлення сигнатур (IPS) та отримання динамічного автоматичного сповіщення про джерела глобальних атак (SIO). Забезпечення URL-фільтрації: не менш ніж 80 категорій; Категоризація не менш ніж 280 млн URL; Можливість перенаправити http(s) трафік до зовнішнього сервісу багаторівневої фільтрації з автоматичним балансуванням навантаження; Забезпечення захисту від злоякісного ПЗ: з можливістю ретроспективного аналізу, пошуку та відображення шляхів розповсюдження. Продуктивність: ідеальні умови, однотипний трафік: не менше ніж **2 Гбіт/с** для сервісу міжмережевого екрану; мультипротокольний трафік (обов'язково включаючи наступні: HTTP, SMTP, FTP, IMAPv4, BitTorrent and DNS): не менше ніж **1,0 Гбіт/с** для сервісу міжмережевого екрану; режим без втрат, для типового HTTP-трафіку, середній розмір пакетів 1024 байт: не менше **0,6 Гбіт/с** (для сервісу захисту від мережевих атак з глибоким аналізом контенту пакетів (IPS) та сервісу аналізу та контролю додатків (AVC)); Не менше ніж **0,3 Гбіт/с** продуктивність сервісу IPSec VPN та максимальною кількістю **750** VPN підключень. Не менше ніж **500 000** одночасних з'єднань та **20 000** нових сессій/сек для сервісу міжмережевого екрану (TCP), збільшення цього значення при формуванні кластеру; Не менше ніж **750**VLAN. Функціональні принципи побудови архітектури захисту пристроїв обробки трафіку: архітектура повинна передбачати відсутність на апаратних платформах пристроїв обробки трафіку сервісів, що можуть вплинути на роботу основного функціоналу, використовуючи ресурси на обчислювально-обтяжливі процеси, зокрема: анти-спам (Antispam); система запобігання витокам інформації (DLP) з обмеженнями до вільного розповсюдження; сервіси оптимізації WAN трафіку.

Назва параметру складової підсистеми	Певні особливі вимоги
	Маршрутизація: протокол маршрутизації OSPF, EIGRP, BGP; Remotely Triggered Black Hole (RTBH) для безпеки Border Gateway Protocol (BGP); Non Stop Forwarding (NSF) в режимі відмовостійкості (HA) при виході одного з пристроїв пари з ладу. Сервіси – Ipv4, Ipv6 та Ethernet: статична трансляція мережевих адрес (Static NAT); динамічна трансляція мережевих адрес (Dynamic NAT); трансляція адрес портів (PAT); протокол перенаправлення трафіку у реальному часі на пристрої кешування (CacheEngines); Layer 2 TunnelingProtocol (L2TP). Багатоадресні розсилки: IGMP, PIM-SM, Bidirectional PIM. Система повинна мати можливість штатної інтеграції з зовнішніми сканерами пошуку вразливостей – щонайменше Qualys, Nessus; Система повинна мати вбудовану можливість створювати та налаштовувати правила за допомоги мови SNORT; Система повинна мати підтримку обміну інформацією про мітки безпеки (Security-Group Tags) з сумісними системами; Моніторинг та керування: підтримка протоколів RADIUS, TACACS або TACACS+, LDAP, Kerberos, систем One-TimePassword; підтримка цифрових сертифікатів; автентифікація та авторизація користувачів по протоколам HTTP, HTTPS, FTP, SSH v2; протокол SNMP версії 1, 2, 3; забезпечення різних рівнів доступу до пристрою; протокол збору агрегованої інформації про IP-потоки (source та destination IP-адреси, порти TCP/UDP) (NetFlow, NSEL); керування за допомогою CLI, HTTP, HTTPS.
Технічна підтримка та гарантії	Підтримка від виробника типу 8x5xNBD, що включає заміну обладнання не пізніше наступного робочого дня, з моменту підтвердження несправності, а також право на оновлення програмного забезпечення обладнання у період гарантійного обслуговування або еквівалент на кожну одиницю обладнання не менше ніж на 3 роки. Усі складові повинні бути від оригінального Виробника обладнання. Все обладнання повинно бути новим, в оригінальній упаковці Виробника.

ДОДАТОК Д

(Призначення та основні характеристики складових підсистеми відображення обстановки та керування інфраструктурою КБ в ІТС ПВЗ ПУ з підтримкою віртуалізації)

ДОДАТОК Д

Таблиця – 2 Призначення та основні характеристики складових підсистеми відображення обстановки та керування інфраструктурою КБ в ІТС ПВЗ ПУ з підтримкою віртуалізації

Назва параметру складової підсистеми	Певні особливі вимоги
Функціональне призначення	Відображення узагальнених даних про стан КБ в підконтрольній ІТС ПВЗ ПУ, деталізованої інформації про інциденти КБ, а також іншої інформації (за рішенням адміністратора безпеки), яка надходить із підсистем програмно-апаратного комплексу керування інфраструктурою КБ на базі відмовостійкої платформи з підтримкою віртуалізації; керування програмними та апаратними складовими комплексу (створення та налаштування політик безпеки, реагування на інциденти КБ, пошук та нейтралізація вразливостей елементів ІТС тощо) з використанням термінальних сесій віддаленого керування, через єдине віртуалізоване середовище чи шляхом безпосереднього фізичного підключення до апаратних складових комплексу.
Засоби відображення обстановки	До складу підсистеми повинно входити: а) не менше ніж 2 фізично відокремлені засоби відображення текстової та графічної інформації, що надходить від підсистем програмно-апаратного комплексу керування інфраструктурою КБ на базі відмовостійкої платформи з підтримкою віртуалізації. Кожен термінал повинен являти собою дисплей з характеристиками не гірше ніж: Діагональ екрану: не менш 42"; Формат зображення: 16:9; Роздільна здатність: не гірше 1920x1080 точок; Інтерфейси: HDMI; Живлення: блок живлення від промислової мережі 220В/50Гц. Силовий кабель: не менш 2 м; Інформаційний кабель: типу HDMI-HDMI довжиною не менш 10 м. Колір: чорний або сірий. Вага: не більше 25 кг. б) відеокомутатор Інтерфейс – HDMI; Живлення: блок живлення від промислової мережі 220В/50Гц. Силовий кабель: не менш 2 м.
Термінали керування	До складу підсистеми повинно входити не менш ніж 6 (шість) фізично відокремлених терміналів керування підсистемами комплексу. Кожен термінал повинен являти собою обчислювальну машину (далі – ОМ) із ОС та ПЗ, що дозволяє здійснювати сесії віддаленого керування апаратними та програмними складовими комплексу з використанням протоколів SSH, telnet, http, https. Кожен термінал повинен мати апаратні складові не гірше ніж: Процесор: Intel; ОЗП: 4 ГБ; НЖМД: 500 Гб; Відеоадаптер: вбудований з підтримкою VGA, HDMI;

Назва параметру складової підсистеми	Певні особливі вимоги
	Оптичний привід: DVD-RW; Маніпулятор типу “миша”; Клавіатура з алфавітно-цифровими клавішами; Інтерфейси: RJ-45, VGA, USB– не менш 2 шт.; Дисплей: діагональ не менш 15.6” з роздільною здатністю не гірше 1366x768 точок; Живлення: блок живлення від промислової мережі 220В/50Гц та додаткове джерело живлення, що здатне підтримувати безперебійну роботу терміналу протягом не менше 1,5 годин у разі раптового зникнення живлення від промислової мережі 220В/50Гц.
Гарантійне обслуговування	Надання однорічної гарантії на заміну окремих технічних складових обладнання.

ДОДАТОК Е

Таблиця 3 Призначення та основні характеристики серверів кібернетичного захисту

Назва параметру складової сервера	Певні особливі вимоги
Сервер КБ розгортається на базі ОМ	Конструкція ОМ повинна забезпечувати її встановлення в телекомунікаційну стійку 19” розміром (ШхГ) 600ммх1000мм.
Вимоги до ОМ:	
Корпус	Не вищий ніж1 монтажні одиниці (1U rackmount).
Процесор	Типу Intel Xeon Processor (частота не нижче 2,40 GHz, об’єм кешу 3 рівня не менше 15 MB, кількість ядер не менш 6, потужність, що споживається – не більше 85W.
Кількість процесорів	Не менше 1.
Чипсет	Типу Intel C610 або аналогічний.
Об’єм пам’яті (максимально)	встановлено не менше ніж 4 модулі пам’яті 16ГБ PC4-2400 RDIMM DDR4 1,2V. Можливість підтримки роботи встановлених модулів пам’яті у чотирьох канальному режимі на частоті не менше ніж 2133 MHz при використанні двох модулів DIMM на канал (2 DPC) та процесорів які працюють з пам’яттю на частоті 2133 MHz.
Слоти для пам’яті	Не менше 24.
Жорсткий диск	Не менше 4x1,2TB SAS Hot Plug зі швидкістю обертання шпинделя 10к обертів на хвилину та фром-фактором 3,5 дюйма.
Контролер жорсткого диску	RAID контролер дискової підсистеми з підтримкою RAID 0, 1, 10 та забезпеченням функції “гарячої заміни” дисків та диску “гарячого резерву” (Hot Spare).
Флеш-модуль	об’ємом не менше 32 GB.
Графічна карта	Розширення, що підтримується – не нижче 1920x1200x16M (Integrated 2D graphics core with hardware acceleration).
Зовнішні порти вводу-виводу	Послідовний – не менше 1 (RJ-45); графічний порт VGA– не менше 1; KVM connector не менше 1; USB – не менше 2 + 1 внутрішній (усі USB 3.0); порт керування – не менше 1; можливість встановлення в сервер вбудованого модуля безпеки > 1; Наявність не менш двох слотів PCIex16 Gen 3;
Мережевий інтерфейс	Сумарно не менше шести 10/100/1000 GbE мережевих адаптерів (портів). Можливість встановлення в flex слот-не займаючи PCIe слоти не менше однієї мережевої плати 1, 10 (Ethernet and iSCSI, Fiber Channel Over Ethernet (FcoE)). Опціонально плати, які не займають PCIe слот, повинні мати можливість ділення 10 GbE (Fiber Channel Over Ethernet (FcoE)) на 256 віртуальних адаптера (апаратна віртуалізація). Опціонально повинна бути можливість встановлення плати, що має роз’єм 10GbE (Fiber Channel Over Ethernet (FcoE)) RJ-45 cat 6e.
Додатково	Наявність в корпусі не менш 6-ти вентиляторів Hot Plug.
Додаткове	Наявність у комплекті телескопічних рейок для встановлення ОМ у

Назва параметру складової сервера	Певні особливі вимоги
обладнання	серверну шафу.
Живлення	2 блока живлення Hot Spare потужністю не менш 770 Вт та ККД не менше 90% (або аналогійні) та два електричних кабелі 10А.
Управління	Наявність активного, відокремленого від мережевих адаптерів, порту віддаленого керування зі швидкістю не менше 1 Gb/s. Підтримка інтегрованим контролером управління з веб-інтерфейсу користувача, призначеного для управління ОМ. Можливість віддалено підключати клавіатуру, дисплей та маніпулятор типу “миша” (KVM), CD і DVD дисководи, які визначаються ОМ як локальні. Підтримка керування на основі XML API для інтеграції з єдиною системою керування ресурсами.
Операційна система	Microsoft WinSvr 2016 (або аналогічне програмне забезпечення з функціоналом не гірше ніж у зазначеного).
Цільове призначення (сервіси КБ)	Для оцінки ефективності захищеності елементів комп’ютерних мереж (серверне та мережеве обладнання, ПЕОМ, веб-сайтів, веб-додатків тощо) від КА, сервер КБ повинен забезпечувати: емуляцію основних видів Кзаг; тестування ефективності систем виявлення/попередження вторгнень (IDS/IPS); тестування ефективності політик безпеки між мережевих екранів; тестування комп’ютерних мереж, побудованих на основі ОС сімейств Windows, Linux, на наявність вразливостей; тестування веб-сайтів та веб-додатків на наявність вразливостей; тестування стійкості паролів облікових записів користувачів; автоматизоване виявлення елементів комп’ютерних мереж, автоматизація процедур виявлення та експлуатації їх вразливостей; оцінка можливості отримання доступу через скомпроментовані вузли до інших вузлів; створення програмних модулів за напрямом тестування комп’ютерних мереж, веб-сайтів та веб-додатків на наявність вразливостей; створення програмних модулів за напрямом соціальної інженерії; можливість під’єднання до єдиної корпоративної системи КБ.
Гарантійне обслуговування	Підтримка від виробника типу 8x5xNBD, що включає заміну обладнання не пізніше наступного робочого дня, з моменту підтвердження несправності, а також право на оновлення програмного забезпечення обладнання у період гарантійного обслуговування або еквівалент на кожну одиницю обладнання не менше ніж на 3 роки. Усі складові повинні бути від оригінального Виробника обладнання. Все обладнання повинно бути новим, в оригінальній упаковці Виробника.

ДОДАТОК Є

Таблиця 4 Призначення та основні характеристики складових підсистеми комутації

Назва параметру складової підсистеми	Певні особливі вимоги
Інтерфейси	не менше 24 портів 10/100/1000 BASE-T Ethernet RJ-45; не менше 4 портів 1GbE SFP; У складі повинні бути наявні 2 оптичних трансіверів з наступними характеристиками: Швидкість підключення: 1 Гбіт/с, 1000BASE-LX/LH; Оптичні характеристики: Повинен працювати у вікні прозорості (1310 нм); Відстань: не менше 10 км за умові використання кабелю SM (G.652). не менше 550 метрів за умові використання кабелю OM3/OM4, MM. У складі повинні бути наявні 2 оптичних трансіверів з наступними характеристиками: Швидкість підключення: 1 Гбіт/с, 1000BASE-SX; Оптичні характеристики: Повинен працювати у вікні прозорості (850 нм); Відстань: не менше 550 метрів за умові використання кабелю OM2, MM. не менше 1000 метрів за умові використання кабелю OM3, MM.
Архітектура	Фіксована; Системна пам’ять: не менш ніж 512Мб DRAM; не менш ніж 128Мб FLASH; Підтримка можливості стекування не менше ніж 8 комутаторів на швидкості до 80 Гбіт/с. Наявний модуль з 2 портами для стикування.
Продуктивність комутаційної шини	Підтримка 100%-ого навантаження на всі порти; Не менше 200 Гбіт/с (full duplex); Продуктивність не менше 70 Мп/с;
Розмір таблиць (в залежності від режиму використання)	Не менш ніж 2 000 IPv4 записів Не менш ніж 1 000 мультикаст маршрутів Не менше ніж 16 000 MAC-адрес. Не менше ніж 1 023 VLAN. Підтримка Jumbo frame, розмір пакету 9216 байт.
Підтримка мережевих протоколів та стандартів	Підтримка протоколів комутації (L2): IEEE 802.1Q тегування VLAN для транкових з’єднань; IEEE 802.1D специфікація STP (Spanning-Tree Protocol); IEEE 802.1s специфікація MSTP (Multiple STP); IEEE 802.1w специфікація RSTP (Rapid Spanning Tree Protocol); IEEE 802.3ad Можливість об'єднання кількох фізичних з'єднань в одне логічне з'єднання Per-VLAN Rapid Spanning Tree (PVRST+). Trunking, private VLAN (PVLAN); підтримка протоколів забезпечення якості обслуговування QoS: Підтримка IEEE 802.1p CoS (class-of-service) та Differentiated Services Code Point (DSCP).

Назва параметру складової підсистеми	Певні особливі вимоги
	Підтримка автоматичної настойки QoS. Підтримка не менше 8 черг на порт. Підтримка протоколів відмовостійкості шлюзу. Протоколи відмовостійкості повинні працювати у режимах active/active або active/standby; 802.1x L2 Basic NAC автентифікація для портів.
Керування	SSH, telnet , SNMPv1/v2c/v3, RMON I/II. Підтримка протоколу для розповсюдження інформації другого рівня про VLAN. Підтримка протоколу збору інформації другого рівня про сусіднє мережеве обладнання. Підтримка можливості копіювання трафіку з одного порту на другий порт для моніторингу у межах комутатора або на інший комутатор: Switched Port Analyzer (SPAN), Remote SPAN (RSPAN); Підтримка технології Flexible NetFlow (FNF) або аналог з можливістю підтримки не менш ніж 8 000 flows Обладнання повинно мати можливість керування, централізованою системою керування того ж Виробника;
Фізичні специфікації	Встановлення у стандартні 19” монтажні шафи; Висота не більш, ніж 1U. Споживча потужність не вище ніж 35 Вт; Підтверджене напрацювання на відмову (Mean Time Between Failures, MTBF) не нижче ніж 500 000 годин; Робочій діапазон температур невужче, ніж: -5…45 °C;
Гарантійне обслуговування та сервісна підтримка	Підтримка від виробника типу 8x5xNBD, що включає заміну обладнання не пізніше наступного робочого дня, з моменту підтвердження несправності, а також право на оновлення програмного забезпечення обладнання у період гарантійного обслуговування або еквівалент на кожну одиницю обладнання не менше ніж на 3 роки. Усі складові повинні бути від оригінального Виробника обладнання. Все обладнання повинно бути новим, в оригінальній упаковці Виробника.

ДОДАТОК Ж

Таблиця 5 Призначення та основні характеристики джерела безперебійного живлення

Назва складової	Певні особливі вимоги
Джерело безперебійного живлення	Максимальна вихідна потужність – 1000 ВА UPS 220V, 50Hz, 19” Форма вихідної напруги - Синусоїдальний сигнал Технологія – лінійно-інтерактивний Вихідні розетки IEC-320-C13 – 8 шт. Вхідні розетки IEC-320-C20 – 1 шт.

ДОДАТОК З

Таблиця 6 Призначення та основні характеристики монтажного кейсу

Назва складової	Певні особливі вимоги
Монтажний кейс	Виготовлений зі спеціалізованого полімерного матеріалу, який дозволяє проводити роботи по монтажу, експлуатації та технічному обслуговуванню розміщеного в ньому обладнання в будь-яких кліматичних умовах при температурі від -54°С до +85°С. Монтажний кейс повинен бути розрахований не менше, ніж на 6 юніта в стандартні стійки розміром 19 дюймів. Кейс повинен мати складні підпружинені ручки, які покриті гумою.
Розмір	Висота – 42U Габаритна ширина - 600 мм. Установочна ширина - 19" Внутрішня глибина - 1000 мм. Система вентиляції - 6 вентиляторів Полиця - 3 шт.

ДОДАТОК И

Таблиця 7 Програмне забезпечення, основні характеристики складових ПЗ та порядок продовження сервісної підтримки для існуючих міжмережевих екранів в інтересах забезпечення заходів з КР, КЗ, ведення КД (КО) та КОб в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ланок управління ЗС України

№	Назва параметру складової програмного забезпечення	Певні особливі вимоги
1	**Ліцензовані опції** на використання функціоналу Application Visibility and Control (AVC), Threat Defense (NGIPS), Malware Protection (AMP) та URL Filtering (URL) у режимі **NGFW** або еквівалент – строком не менш ніж на 3 роки.	
2	**Обладнання до якого застосовується програмне забезпечення**	Програмно-апаратний комплекс Cisco ASA 5525 **(2 шт.)**: S/N: FGL193270ZS S/N: FGL193270ZT Програмно-апаратний комплекс Cisco ASA 5508 **(4 шт.)**: S/N: JMX2023YO4R S/N: JMX2023YOMO S/N: JMX2023YOLT S/N: JMX2023YOM4
3	**Ліцензовані опції** на використання функціоналу Application Visibility and Control (AVC) та Threat Defense (NGIPS) у режимі **NGFW** або еквівалент – строком не менш ніж на 1 рік.	
4	**Обладнання до якого застосовується програмне забезпечення**	Програмно-апаратний комплекс Cisco ASA 5515**(3 шт.)**: S/N: FGL1932711B S/N: FGL1932711C S/N: FGL1932711A

№	Назва параметру складової програмного забезпечення	Певні особливі вимоги
5	**Ліцензовані опції** на використання функціоналу Application Visibility and Control (AVC) та Threat Defense (NGIPS) у режимі **NGFW** або еквівалент – строком не менш ніж на 3 роки.	
6	**Обладнання до якого застосовується програмне забезпечення**	Програмно-апаратний комплекс Cisco ASA 5506 **(27 шт.)**: S/N: JMX1932Z0ZE S/N: JMX1932Z124 S/N: JMX1932Z10B S/N: JMX1932Z0ZJ S/N: JMX1932Z0ZH S/N: JMX193241BX S/N: JMX193241C6 S/N: JMX193241CB S/N: JMX1932Z0ZF S/N: JMX193241CL S/N: JMX193241CK S/N: JMX193241CD S/N: JMX193241CM S/N: JMX193241ED S/N: JMX193241BY S/N: JMX1932Z0ZG S/N: JMX1932Z0ZN S/N: JMX193241CX S/N: JMX1932Z126 S/N: JMX193241CC S/N: JMX1932Z125 S/N: JMX1932Z0ZC S/N: JMX1932Z122 S/N: JMX1932Z0ZD S/N: JMX193241C8 S/N: JMX2018841Q4 S/N: JMX201841Q3
7	**Технічна підтримка та гарантії**	Підтримка від виробника типу 8x5xNBD, що включає заміну обладнання не пізніше наступного робочого дня, з моменту підтвердження несправності, а також право на оновлення програмного забезпечення обладнання у період гарантійного обслуговування або еквівалент на кожну одиницю обладнання не менше ніж на 3 роки (окрім пп. 3-4).

ДОДАТОК І

Таблиця 8 Програмне забезпечення, основні характеристики складових ПЗ моніторингу, аналізу мережевої поведінки та виявлення аномалій в ІТС ПВЗ ПУ тактичної, оперативної та стратегічної ланок управління ЗС України

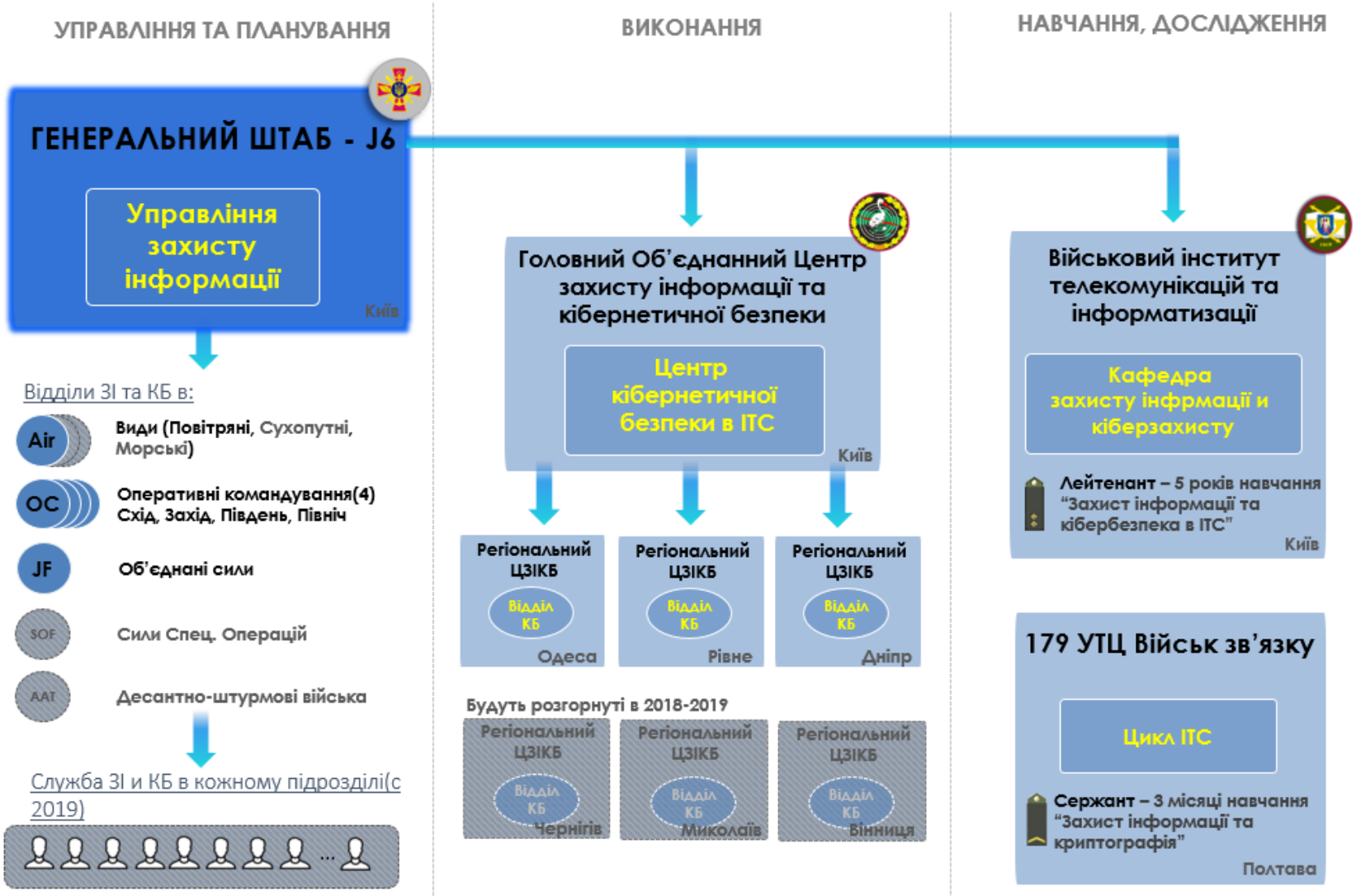
№	Назва параметру основних складових програмного забезпечення	Певні основні вимоги
1	**Програмне забезпечення підсистеми моніторингу, аналізу мережевої поведінки та виявлення аномалій** у складі: **Програмна продукція** консолі керування для встановлення в віртуальному середовищі або еквівалент – 2 шт.; **Програмна продукція** модулів сбору телеметрії (колектор) для встановлення в віртуальному середовищі або еквівалент – 2 шт.; **Ліцензована опція** для обробки системою не менш ніж **1 000** одночасних потоків (flows) строком на 3 роки – 1 шт.;	
2	**Архітектура**	Модульна. Система повинна мати поділ щонайменше між модулями управління та збору даних з мережевих пристроїв та бути реалізована як окремі віртуальні пристрої. Повинна бути можливість збільшення кількості модулів для масштабування. Програмна реалізація (у вигляді віртуальних пристроїв під управлінням гіпервізора).
3	**Кількість пристроїв, з яких збираються дані**	Не менш ніж 2000 мережевих пристроїв на один модуль збору даних. Можливість розширення кількості пристроїв і хостів за рахунок збільшення кількості модулів системи.
4	**Швидкість обробки подій (flow)**	Підтримка обробки не менш ніж 2 000 мережевих потоків (flow) в секунду. Ліцензійна розширюваність для підтримки не менше 30000 мережевих потоків (flow) в секунду.
5	**Апаратна платформа**	Програмно-апаратна або програмна реалізація (в рамках єдиного віртуалізованого середовища комплексу).
6	**Підтримка джерел інформації**	Повинні підтримуватися наступні типи джерел інформації: Маршрутизатор; Комутатори; Міжмережеві екрани; Контролери WiFi; Сервера; Системи віртуалізації (VMware vSphere 5.x, 6.x, HyperV) Повинні підтримуватися наступні набори протоколів: NetFlow (зокрема RFC 3954); NSEL; IPFIX (RFC 3917, RFC 7011- 7015, RFC 5103.) HSL, sFlow, NetStream, cFlow, jFlow, AppFlow, preIPFIXv9, Packeteer-2 Повинна підтримуватися обробка асиметричних потоків і дедуплікації потоків з різних мережевих пристроїв.
7	**Функції виявлення**	Забезпечення виявлення загроз шляхом профілювання

№	Назва параметру основних складових програмного забезпечення	Певні основні вимоги
	та запобігання загрозам	хостів, мережевого трафіку / активності та оповіщення на наявність аномалій в залежності від нормального трафіку, профілів послуг, політики безпеки або перевищення хостом заявлених поведінкових порогів; Забезпечення виявлення поліморфних, шифрованих, модифікованих і Zeroday (невідомих) атак; Забезпечення виявлення атак типу відмова в обслуговуванні (DDoS); Забезпечення можливості інтеграції з мережевими пристроями захисту (наприклад, маршрутизатор, міжмережевий екран і т.д.) з метою подальшого конфігурації для протидії виявленим атакам; Забезпечення протидії загрозам за рахунок таких видів дій, як Block Source, Block Destination, Block Port, Block Service, Custom; Наявність власного репутаційного сервісу та можливості інтеграції з зовнішніми (від третьої виробника).
8	**Функції моніторингу мережевої інфраструктури**	Забезпечення можливості виявлення несправних або невірно налаштованих мережевих пристроїв (маршрутизаторів, серверів, робочих станцій і т.п.); Забезпечення моніторингу утилізації мережевих каналів, інтерфейсів, сервісів і додатків; Наявність можливості ідентифікації додатків власними механізмами і за рахунок інтеграції з зовнішніми системами (наприклад, по протоколу NBAR). Забезпечення підтримки функції flow deduplication (ідентифікація та видалення повторюваних потоків з різних джерел); Забезпечення можливості об'єднання flow-записів в один для надання єдиного виду потоку комунікації від клієнта до сервера; Забезпечення можливості моніторингу як IPv4, так і IPv6 мереж; можливість забезпечувати моніторинг віртуальної інфраструктури: віртуальних серверів, їх переміщення і т.д. (за умови додаткового ліцензування). Забезпечення можливості аналізу наступних показників (за умови додаткового ліцензування): Network round-trip-time (RTT); Server Response Time (SRT); Re-transmission rates.

№	Назва параметру основних складових програмного забезпечення	Певні основні вимоги
9	**Створення та застосування політик**	Наявність консолі управління з графічним інтерфейсом (GUI); підтримка рольової моделі доступу з можливістю призначення повноважень для кожної ролі; можливість налаштування зовнішнього вигляду і наповнення консолі індивідуально для кожного користувача; Забезпечення можливості інтеграції з системами управління інцидентами і подіями (SIM / SIEM), активними каталогами, а також мати API для інтеграції з іншими зовнішніми додатками і системами; можливість інтеграції з системами контролю доступу для отримання розширеної інформації про хости / користувачів і блокування доступу аномальних хостів в мережі; Забезпечення можливості збереження інформації про всі дані, які збираються тривалістю не менше 30 календарних днів; можливість створення як системних звітів, так і тих, які створюються користувачами за певними критеріями, експорт звітів в різні формати даних, налаштування відправки звітів в різних форматах в зовнішні системи для подальшого аналізу.
10	**Гарантійне обслуговування**	Підтримка від виробника типу 8x5xNBD, що включає право на оновлення програмного забезпечення у період гарантійного обслуговування або еквівалент на кожну одиницю не менше ніж на 3 роки.

ДОДАТОК Ї

Структура Головного Об'єднаного Центру захисту інформації та кібернетичної безпеки



ДОДАТОК Й

Завдання Головного Об’єднаного Центру захисту інформації та кібернетичної безпеки