УДК 001.51/.99 + 001.895 + 004.946 + 681.5

***Ігор Миколайович Козубцов*** *(канд. техн. наук, с.н.с)*
***Володимир Вікторович Куцаєв***
***Володимир Олександрович Ткач***
***Леся Михайлівна Козубцова***

***Військовий інститут телекомунікацій та інформатизації, Київ, Україна***

# КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ПОБУДОВИ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ СТАЦІОНАРНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ВУЗЛІВ УКРАЇНИ НА ПРИНЦИПАХ МАСШТАБУВАННЯ ТА ДОПОВНЕННЯ

*Авторами на основі існуючих ідей обґрунтовано концептуальний підхід до побудови системи кібернетичної безпеки стаціонарних інформаційно-телекомунікаційних вузлів України на принципах масштабування та доповнення. Це дає змогу динамічно розширювати функціональні можливості системи кібернетичної безпеки без розробки додаткової конструкторської документації та втрат часу на її узгодження. Обраний блочно-модульний підхід до формування та комплектації вузлів системи кібернетичної безпеки забезпечує швидке налаштування та ремонт обладнання (відновлення працездатності системи та відповідності новим кібернетичним загрозам). Запропоновано адекватний шлях реалізації концепції побудови системи кібернетичної безпеки стаціонарних інформаційно-телекомунікаційних вузлів України.*

***Ключові слова:*** *концептуальний підхід; побудова; системи кібернетичної безпеки; стаціонарний; інформаційно-телекомунікаційний вузол; принцип; масштабування; доповнення.*

## Вступ

**Концептуальна стадія. Визначення проблеми, розв'язання якої спрямоване в концепції.** Однією з ключових проблем, які в умовах глобалізації інформаційного обміну і широкого впровадження інформаційних технологій в усіх сферах життєдіяльності суспільства в тому числі військовій, постали перед усіма державами світу. Проблема захисту інформації, що передається і обробляється в інформаційно-телекомунікаційних системах, не захищена від відомих впливів та загроз у кібернетичному просторі.

Інформаційно-телекомунікаційна система стає вразливим місцем у функціонуванні всієї систем зв'язку і об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності і конфіденційності інформації та нанесення шкоди інформаційним ресурсам і телекомунікаційним системам. При цьому особливу занепокоєність викликає можливість застосування інформаційних технологій у кібернетичному просторі в інтересах здійснення військово-політичного та силового протиборства, тероризму та проведення хакерських атак.

Тому у чисельних нормативних документів з питань оборони та безпеки України чільне місце відводиться проблемі протидії кібернетичним загрозам (КЗ). Зокрема у [1, 2] КЗ віднесено до актуальних загроз національній безпеці держави, а створення системи кібернетичної безпеки (КБ) та захист від кібернетичних атак визначено нагальними завданнями.

**Аналіз причин виникнення проблеми та обґрунтування необхідності її розв'язання концептуальним методом.** Такими причинами є:

наявність негативно налаштованих групувань які бажають реалізації протиправних дій у кібернетичному просторі шляхом порушення цілісності, доступності і конфіденційності інформації та нанесення шкоди інформаційним ресурсам і телекомунікаційним системам;

угрупування програмістів типу хакер набагато швидше створює шкідливе програмне забезпечення а ніж оновлюється антивірусне (програмне забезпечення);

застосування інформаційних технологій та шкідливого програмного забезпечення у кібернетичному просторі в інтересах здійснення військово-політичного та силового протиборства, інформаційної/кібернетичної операції, тероризму та проведення хакерських атак.

Саме в час створення та налаштування системи зв'язку відбувається стрімкий розвиток кібернетичних загроз.

Сучасні засоби кібернетичного захисту інформації приймаються на озброєння з певними труднощами, у зв'язку з відсутністю достатнього фінансування.

Аналіз причин виникнення проблеми дозволив нам виявити низку прогалин.

По-перше, суттєвою причиною є не

адаптованість нормативно-правових актів України, та інших відомств сучасним реаліям парадигми швидкого реагування на виклики кібернетичної загрози. Це проявляється в тому, що основні норми детермінують статичний режим і гальмують процес швидкої адаптації системи.

По-друге, тривалий час відсутня єдина фундаментальна термінологічна основа понять зі сфери кібернетичної безпеки.

По-третє, спроба трансформувати поняття "Хакер" на військовий манер.

По-четверте, спроба динамічний процес замінити статичним шляхом написання керівництв.

По-п'яте, відсутня єдина концепція побудови системи кібернетичної безпеки (СКБ) стаціонарних ІТВ на принципах масштабування та доповнення.

По-шосте, негативна практика закупівель програмно-апаратного забезпечення по принципу залишкових коштів та мінімального підходу.

По-сьоме, відсутністю єдиного погляду на функціональне призначення структурних підсистем СКБ, надання їм не притаманних функцій.

По-восьме, відсутністю мінімально необхідного укомплектованого аналітичного відділу СКБ компетентними фахівцями, ентузіастами, особами, що подобається даний вид професійної діяльності.

По-дев'яте, спроби побудови СКБ здійснювалось не на основі принципів масштабування та доповнення.

**Аналіз останніх досліджень і публікацій**

Фундаментальним на наш погляд є роботи [3] у яких автори розглядають актуальні проблеми забезпечення міжнародної та національної кібербезпеки, а також пропонують підходи до створення адекватної сучасним загрозам системи забезпечення кібербезпеки автоматизованих систем органів військового та державного управління [4]. Частково на їх наступних та функціональних компонентах будемо проектувати СКБ.

**Отже не вирішеним питанням** є розробка концептуального підходу до побудови системи кібернетичної безпеки стаціонарних ІТВ України на принципах масштабування та доповнення.

**Формулювання мети статті.**

Обґрунтувати концептуального підходу до побудови системи кібернетичної безпеки стаціонарних ІТВ України на принципах масштабування та доповнення.

**Мета концепції** полягає в науковому обґрунтуванні напрямку, шляху та способу забезпечення побудови системи кібернетичної безпеки стаціонарних ІТВ на принципах масштабування та доповнення.

## Виклад основного матеріалу дослідження.

**Визначення оптимального напрямку розв'язання проблеми на основі порівняльного аналізу концепцій**

***Першим варіантом*** розвитку є побудова підсистеми кібернетичної безпеки в побудованій принципово новій основі цифрової інформаційно-телекомунікаційної системи ЗС України за хмарною технологією.

Перевагою даного варіанту є можливість варіації в широкому діапазоні вибору шляхів реалізації.

Крім того, цей варіант дозволяє відносно легко реалізувати підсистему кібернетичної безпеки в частині кібератак. Зміст її полягає в наступному.

При інтенсивному надходженні DDoS атак маршрутизатор рахує кількість інтенсивних запитів, що надходять від віртуальної БОТ-мережі. При перевищенні гранично допустимого значення відбувається вирізання IP адресу. В результаті віртуальна БОТ-мережа стає недоступна до потенційного об'єкту атаки.

***Другим варіантом*** розвитку є побудова підсистеми кібернетичної безпеки в цифровій інформаційно-телекомунікаційній системі імплиментовану в існуючій хмарній технології.

Перевагою другого варіанту відсутність у потребі проектувати власну інформаційно-телекомунікаційну мережу.

**Шляхи і способи розв'язання проблеми у концепції.** Розглянемо та обґрунтуємо можливі шляхи розв'язання проблеми, від яких залежить строк реалізації виконання концепції побудови СКБ стаціонарних ІТВ на принципах масштабування та доповнення і ефективність її функціонування.

Узагальнений перелік шляхів націлених на побудову СКБ стаціонарних ІТВ наведено на рис. 1.

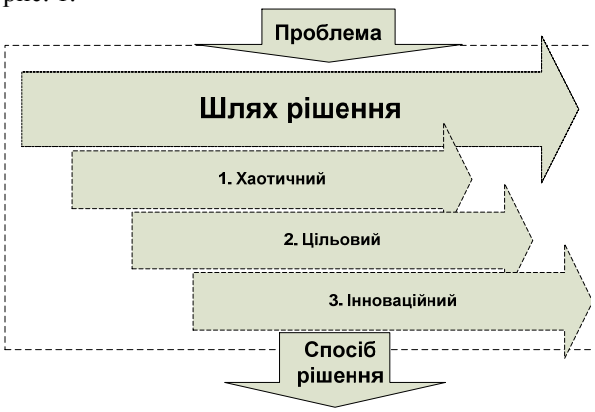


**Рис. 1. Перелік шляхів націлених на побудову СКБ стаціонарних ІТВ**

**Першим шляхом** розв'язання проблеми є хаотичний підхід. Ключовим недоліком якої є відсутність цілісного бачення на концепцію побудови СКБ стаціонарних ІТВ на принципах масштабування та доповнення.

Шлях є очевидним і логічним як адекватна реакція на сучасні виклики кібернетичних загроз.

***Спосіб реалізації першого шляху*** зводиться до побудови тих фрагментів підсистем СКБ стаціонарних ІТВ за наявними матеріально-технічними можливостями або принципово

важливими на даний час.

Спосіб носить хаотичний та епізодичний характер, що ґрунтується на мінімальному підході закупівельної вартості обладнання. Мінімальний підхід не завжди адекватний функціональній спроможності обладнання та технічній надійності. З появою нових напрямків кібернетичної безпеки виникає необхідність обґрунтовувати організаційно-штатну структуру системи кібернетичної безпеки, управління та функціональне призначення структурних підсистем. Іншими словами процес масштабування СКБ тривалий.

**Другий шлях. Цільовий.** Власно за рахунок цільового підходу до побудови СКБ стаціонарних ІТВ без ґрунтування на принципах масштабування та доповнення пояснюється відсутністю розуміння функціонального призначення структурних складових підсистеми кібернетичної безпеки.

Такий шлях залишається на заваді при побудові цілісної працездатної СКБ стаціонарних ІТВ і є тупиковим.

***Спосіб реалізації другого шляху*** передбачає стандартизацію (уніфікацію) структури СКБ на принципі чіткої системної лінії.

Даний спосіб також не практичний у разі необхідності розширення структури за напрямками кібернетичної безпеки. Знову ж виникає необхідність в обґрунтовувати організаційно-штатної структуру системи кібернетичної безпеки, управління та функціональне призначення структурних підсистем. Процес масштабування СКБ взагалі не передбачає. На різних ланках управлінні вирішуються різні тактичні завдання втому числі і на кібернетичному полі. В мирний час проведення кібернетичних операцій, що пов'язані з кібернетичним впливом на систему ймовірного противника передує складний механізм прийняття рішень. Тому наприклад не на всіх рівнях слід розгортати підсистему кібернетичного впливу, але ґрунтуючись на принципі доповнення необхідно закладати в проектну функціональну можливість приймати участь в таких діях.

**Третій шлях. Інноваційний.** Він передбачає за мету обґрунтування якісно нової концепції побудови СКБ стаціонарних ІТВ саме на основах принципів масштабування та доповнення.

Зважаючи на це для України є актуальним обрання даного шляху з розробки комплексу науково-обґрунтованих заходів по гармонізації всіх підсистем СКБ стаціонарних ІТВ на принципах масштабування та доповнення.

Цей шлях побудований на принципах масштабування та доповнення є перспективним, і визначатиме вектор подальшого розвитку СКБ в світовому просторі з урахування динаміки. В такому разі структура системи не є стандартизованою і може бути змінена своєчасно без проведення організаційно-штатних заходів.

***Спосіб реалізації третього шляху.*** Третій спосіб націлений на реалізацію заходів щодо побудови структуру СКБ на принципах масштабування та доповнення.

Пропонується реалізовувати побудову СКБ на модульному (блоковому) принципу з централізованою системою управління складатиметься:

модуля Головного ІТС України (МЗІКБ);

модуль Запасного Головного ІТС України (він же виконує резервну функцію та архівування ключових важливих даних);

модуль регіонального ІТС України (МРІТС);

модуль периферійного ІТС України (МПІТС);

модуль територіального ІТС України (МТІТС)

модуль мобільного комплексу кібернетичного захисту;

модуль навчально-тренувального та кібернетичного полігону.

В свою чергу кожен модуль побудований за реконфігурованим та масштабованим принципом, який залежності від функціонального навантаження становлять завершені системно-цілісні блоки:

блок антивірусного модуля захисту;

блок модуля міжмережевого захисту типу FireWall;

блок модуля захисту від "відмови в доступі" (DoS та DdoS) з виходом на зовнішні маршрутизатори (по окремим каналам);

блок модуля захисту Web додатків;

блок модуля захисту E-mail;

блок модуля захисту сервісів;

блок модуля побудови і застосування VPN каналів.

Виходячи з цього із загальної функціональної схема СКБ побудови на основах блочно-модульного принципу матиме вид представлений на рис. 2. Необхідність розгляду цього способу обумовлено тим, що цей шлях пропонує перехід від теоретичної частини дослідження до практичної частини.

Прикладний результат зазвичай є інноваційним, оскільки передбачає застосування частини відомих технологій, що удосконалюють відомі рішення, оскільки поняття і сутність СКБ вже відома.

Реалізація цього шляху націлена на впровадженні науково-обґрунтованих результатів в практику побудови систем. Весь шлях можна уявити як цілісну систему, що складається зі способу та конкретних заходів. Конкретні заходи

способу є складовими системи. Відмова від реалізація перелічених заходів або порушення цілісності призведе до порушення функціонування цілісності всієї системи.

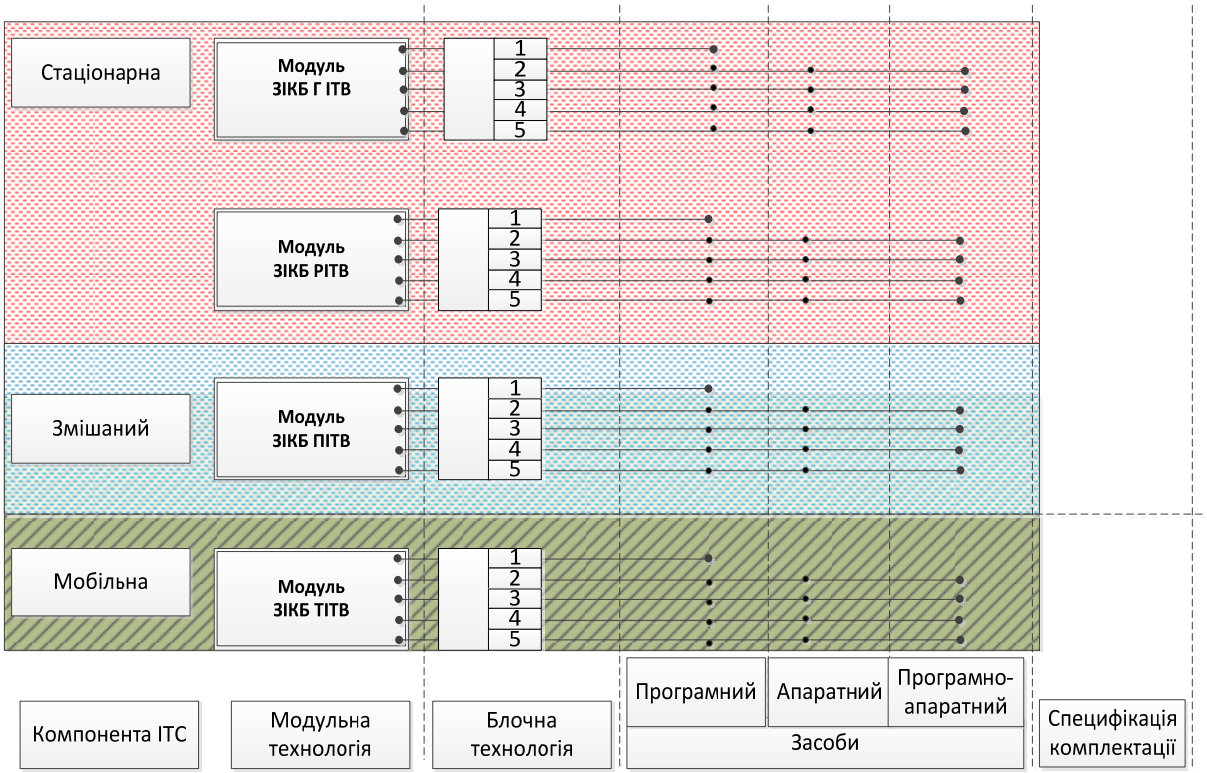


**Рис. 2. Фрагмент функціональної схеми системи кібернетичної захисту як складова в системі зв'язку України**

**Технологічна стадія реалізації концепції. Завдання які необхідно виконати щодо реалізації концепції.** Відповідно до мети концепції спосіб розв'язання полягає саме через шлях закладеного в сутності реалізації основних завдань дослідження, що полягають на фундаментальній основі:

спланувати розробку структурної, функціональної та принципової схем побудови СКБ в системі зв'язку ІТС;

розробити та проаналізувати можливих варіантів схем розгортання СКБ;

розробити та обґрунтувати технічні вимоги до розподілених підсистем СКБ стаціонарних ІТВ;

розробити вимоги до СКБ в ІТС стаціонарних ІТВ;

розробити перспективні схеми розгортання СКБ;

розробити перелік необхідного програмного забезпечення для розгортання СКБ в ІТС стаціонарних ІТВ;

розробити практичні рекомендації з технології статичного та динамічного аналізу вразливості програмного забезпечення

розробити та обґрунтувати перелік програмного забезпечення розподілених підсистем СКБ в інтересах забезпечення заходів з кіберрозвідки, кіберзахисту та кібердій (кібероперацій)

провести оцінку впливу СКБ на характеристики системи зв'язку.

**Заходи реалізації концепції**

Принцип (повноти і оптимальності). Запропонований набір заходів повинен забезпечувати досягнення поставлених цілей (вимог повноти) оптимальним (і/або допустимим) способом. Ефективна реалізація концепції на практиці потребує реалізації системи органічно-єдиних заходів.

Заходи із забезпечення кібернетичної безпеки жодним чином не можуть суперечити принципу гарантування прав та свобод громадян України, в тому числі права на недоторканність приватного життя та свободи спілкування.

**Принципи.** Підчас реалізації концепції необхідно додержуватися наступних принципів:

1. Принцип високої доступності інформації. Це означає реалізацію видаленого санкціонованого доступу до інформаційних ресурсів територіальних органів державної статистики, включаючи існуючі операційні бази даних і сховища даних.

2. Принцип централізації розповсюдження офіційної статистичної інформації.

3. Принцип масштабованості При реалізації заходів щодо розвитку СКБ необхідно передбачати етап апробації проектного вирішення перспективних завдань і етап тиражування проектного рішення. Заходи щодо розвитку СКБ повинні бути реалізовані так, щоб обмежуватися мінімальним набором апаратного і програмного забезпеченню на початковому етапі використання. Проте використовувані проектні рішення повинні

допускати збільшення продуктивності з погляду кількості обслуговуваних користувачів, об'ємів даних і нарощування обчислювальних ресурсів, а також розширюваності новими функціями.

Додавання нових функціональних можливостей не повинне супроводжуватися змінами в раніше розробленій і експлуатованій частині. Взаємодія між інформаційними підсистемами СКБ повинна будуватися на використанні загальноприйнятих стандартів. Таким чином, принцип масштабованості накладає на рішення по організації СКБ наступні концептуальні вимоги:

використання технічних засобів і рішень, архітектура яких допускає розширення функціонала і збільшення продуктивності без перебудови системи.

використання програмних рішень, що дозволяють налагодити інформаційний обмін з використанням стандартної функціональності.

4. Принцип використання Єдиної системи метаданих. Для підвищення якості формованих інформаційних ресурсів і їх інтеграції, необхідне централізоване ведення Єдиної системи метаданих, що включає Каталог статистичних показників, єдині довідники і класифікатори і обов'язковість їх використання на всіх етапах проектування і розробки програмно-технологічних засобів, а також на всіх етапах обробки інформації.

5. Принцип інформаційної безпеки. Питання рівня інформаційної безпеки СКБ вважається одним з найважливіших питань, оскільки у складі інформаційних ресурсів СКБ велика частина інформації є конфіденційною, а за об'ємом інформації представляє одну з наймасштабніших державних інформаційно-обчислювальних систем.

Рівень інформаційної безпеки при впровадженні і експлуатації інформаційних технологій в СКБ визначається вимогами нормативно-правової бази України і нормативними документами в області захисту інформації.

6. Принцип централізації планування, контролю і управління процесами. Принцип централізації планування, контролю і управління процесами означає створення системи кібернетичної безпеки, що реалізовує узгоджену роботу всіх підсистем і модулів системи кібернетичної безпеки.

7. Принцип компетентності – створення умов для підбору обслуговуючого штату, що компетентний в даній галузі.

8. Принцип творчості – створення умов для розвитку індивідуально-особистісної творчості.

9. Принцип проблемності передбачає орієнтацію майбутнього фахівця на вирішення реальних проблем.

10. Принцип реалізму передбачає орієнтованість випускника аспірантури на досягнення реальних професійних цілей, оволодіння необхідними для цього засобами і методами.

11. Принцип технологічної єдності процесу навчання та практики на кібернетичному полігоні.

12. Принцип (регламентації управлінської діяльності). Управлінська діяльність повинна бути регламентована. Відповідно до даного принципу всі функції управління повинні бути регламентовані і узгоджені між всіма рівнями ОС. Отже, для апробації моделей управління необхідні, зокрема:

1. Розробка відповідного нормативно-правового забезпечення (створення нових положень про органи управління освітою, їх діяльність, посадових інструкцій і так далі);

2. Розробка критеріїв оцінки ефективності змін (результатів реалізації проектів) і ефективності діяльності органів управління;

3. Розробка відповідного науково-методичного і інформаційного забезпечення;

4. Перепідготовка управлінських кадрів.

**Рефлексивна стадія концепції.** Завершальною фазою проекту концепції є рефлексивна фаза. Метою якої є порівняти результат з метою та оцінити похибку відхилення. За необхідності відкоригувати концепцію.

**Термін виконання концепції. Термін виконання** концепції з побудови СКБ стаціонарних ІТВ включає час затрачений на реалізацію теоретичної та практичної фази концепції.

До визначеного терміну потрібно приплюсувати необхідний час підготовки всіх учасників експерименту.

Таким чином, загальний прогнозований термін реалізації концепції побудови СКБ стаціонарних ІТВ на принципах масштабування та доповнення наведено в табл. 1.

Отже, очікуваний ефект почнемо отримувати в залежності від того якомога раніше розпочнемо реалізовувати концепцію побудови СКБ стаціонарних ІТВ на принципах масштабування та доповнення.

*Таблиця 1*

**Загальний прогнозований термін реалізації концепції**

| № п/п | Найменування робіт | Норма | Термін (роки) |
|---|---|---|---|
| 1 | Теоретична фаза (написання НДР) | 0.1.2015 – 31.12.2015 | 1 |
| 2 | Практична фаза | 2016 – 2019 роки | 4 |
| 2.1 | Закупівля програмно-апаратного забезпечення | 2016 – 2018 роки | 3 |
| 2.2 | Розгортання системи кібернетичної безпеки | 2016 – 2019 роки | 4 |
| Загальний термін реалізації проекту | | 2015 – 2019 роки | 5 |

Хід реалізації завдань та заходів запланованих

на період 2015-2019 років раціонально розподілити на три етапи. Перелік етапів представлено на рис. 3. Зазначимо, що на схемі представлено чотири етапи, перший з яких реалізовано в 2013 році передбачений Планом наукової та науково-технічної діяльності Військового інституту телекомунікацій та інформатизації НТУУ "КПІ" особовим складом підрозділу Наукового центру зв'язку та інформатизації. Результат реалізації етапу представляє собою заключні звіти про науково-дослідні роботи (НДР) "Атака" та "Хвиля".

**Перший етап** реалізації концепції (01.2015 – 12.2015 р.) планування та проектування. На першому етапі реалізації Програми (01.2015 – 12.2015 р.)

**Другий етапі** реалізації Програми (01.2016 – 12.2016 р.) закупівлі та монтажу.

Закупівля обладнання планується за обґрунтованим переліком програмно-апаратного обладнання отриманого в НДР "Атака" та "Хвиля" та під кореговано з урахуванням швидкозмінних тенденцій появи нових кібернетичних загроз та морального старіння програмно-апаратного обладнання.

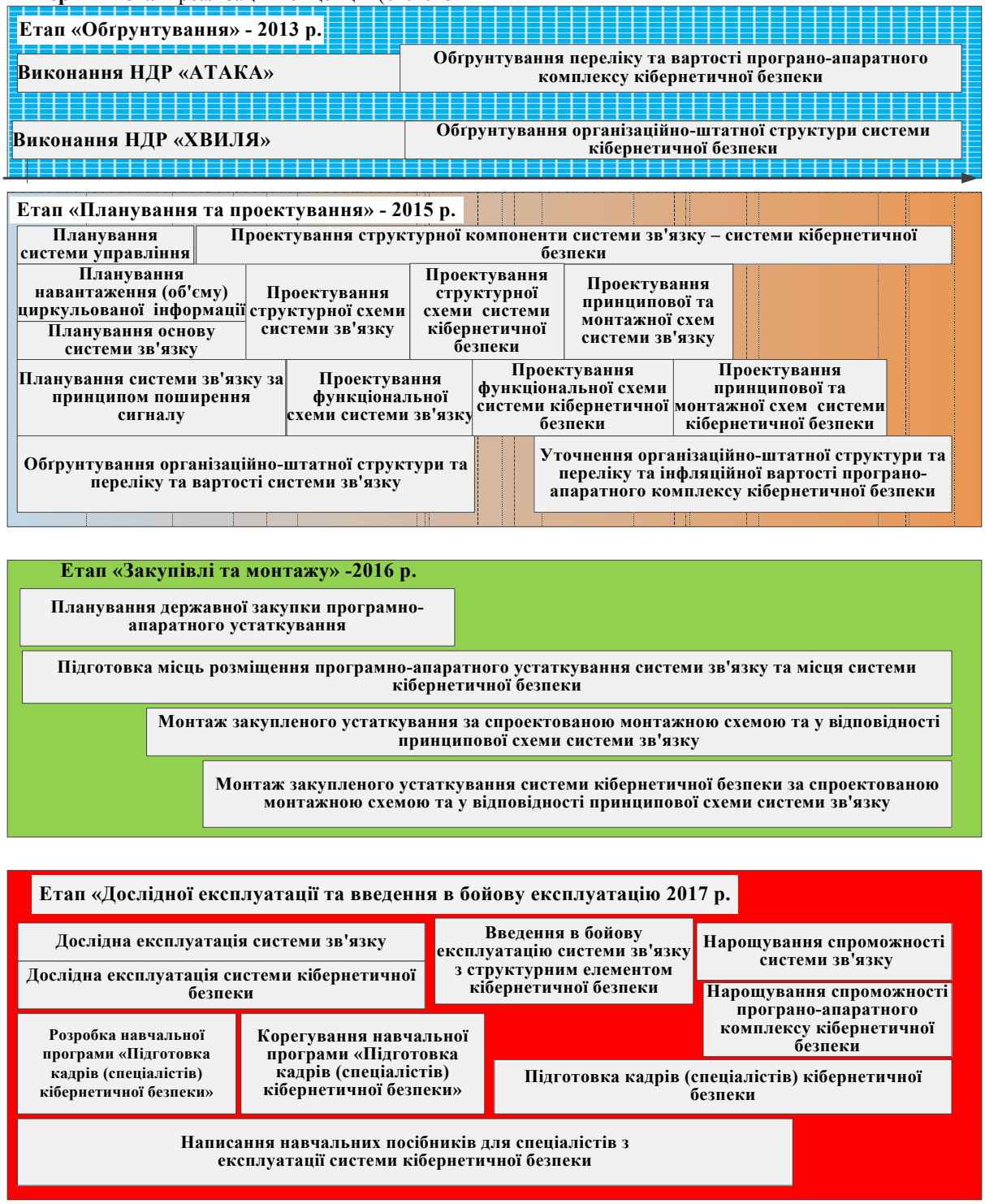


**Рис. 3. Поетапність реалізації концепції**

Паралельно необхідно вести ремонтно-відновлювальні роботи запланованих місць розгортання стаціонарної компоненти.

Для мобільної компоненти – відповідно пошук автомобільної бази високої прохідності. Науковим обґрунтуванням служитиме результат НДР "Левада".

**Третій етапі** реалізації Програми (01.2017 – 12.2017 р.). Етап дослідної експлуатаційний та введення техніки в бойову експлуатацію. Метою етапу є налаштування програмно-апаратного обладнання системи зв'язку узгодження її зі складовою – системою інформаційної та кібернетичної безпеки.

В процесі дослідної експлуатаційний головним завданням:

залученого науково-педагогічного складу профільного інституту для написання методичних рекомендацій, навчальних посібників, складання навчальної програми підготовки спеціалістів забезпечення обслуговування системи кібернетичної безпеки;

наукового складу – написання дисертацій, монографій.

Облаштування навчально-тренувального (кібернетичного полігону).

За результатами дослідної експлуатації та акту виявлених з проблем науково-педагогічному складу інституту – внести корекцію до навчальної програми підготовки спеціалістів забезпечення обслуговування системи кібернетичної безпеки; розробити відповідні рекомендації, інструкції.

**Очікувані результати виконання концепції, визначення її ефективності.** Розглянемо очікувані результати та визначимо ефективність від реалізації концепції побудови СКБ стаціонарних ІТВ на принципах масштабування та доповнення.

Ефективність процесу реалізації концепції побудови СКБ стаціонарних ІТВ на принципах масштабування та доповнення залежатиме від повноти реалізації усіх компонентів та заходів концепції.

Критеріями досягнення результату є: функціонування побудованої СКБ стаціонарних ІТВ та можливість масштабувати її та доповнювати.

При оцінці ефективності реалізації проекту концепції враховувались наступні особливості.

По-перше, труднощі оцінки ефективності більшості проектів пов'язані з тим, що вони не мають найчастіше аналогів.

По-друге, реалізація проекту концепції може не дати миттєвого позитивного результату, результати можуть проявлятися згодом.

Основними методами оцінки ефективності реалізації проекту будемо використовувати формальні моделі оцінки (див. [5]) є:

Самооцінка – у разі колективного проекту – (колективна самооцінка, одержувана в результаті обговорень, дискусій);

експертиза із залученням незалежних експертів – фахівців з боку, в тому числі науковців, представників сторонніх організацій і т.д.

Очікувані результати (табл. 2):

отримання системи захисту інформації та кібернетичної безпеки в ІТС;

набуття бойових спроможностей системою захисту інформації та кібернетичної безпеки в ІТС.

*Таблиця 2.*

**Очікувані результати**

| Найменування завдання | Найменування показників виконання завдання | Одиниця виміру | Значення показників | | | | |
|---|---|---|---|---|---|---|---|
| | | | усього | у тому числі за роками | | | |
| | | | | 2015 | 2016 | 2017 | 2018 |
| Проектування системи захисту інформації та кібернетичної безпеки в ІТС | Документація на впровадження системи захисту інформації та кібернетичної безпеки | комплект | + | + | | | |
| | Програмно-апаратний комплекс забезпечення захисту інформації та кібернетичної безпеки | комплекс | + | + | + | + | |
| | Мобільна апаратна КБ | апаратна | + | | | + | + |
| | Спеціальне програмне забезпечення КБ | комплект | + | + | + | + | |

Перевагами запропонованого підходу до побудови СКБ як складової в системі зв'язку України є:

можливість системно і незалежно нарощувати спроможність модулів (блоків);

можливість оновлювати якісний склад модулів (блоків) з урахуванням сучасних викликів кібернетичної безпеки суспільства;

спрощена процедура "гарячого" резервування модулів (блоків);

модульно-блочний підхід дозволяє масштабування за єдиним принципом, оскільки передбачається дзеркальна уніфікація і використання однотипного обладнання, що дозволяє застосовувати при ремонті (відновленні) метод блочної заміни блоків (модулів).

**Оцінка фінансових, матеріально-технічних, трудових ресурсів, необхідних для реалізації концепції.**

Фінансування розробки теоретичної фази концепції побудови СКБ стаціонарних ІТВ здійснюватиметься за рахунок грошового утримання виконавців.

Фінансування практичної фази реалізації

концепції здійснюватиметься за рахунок коштів державного бюджету в рамках джерел, що не заборонені законодавством України.

Побудова СКБ як складової в системі зв'язку потребує фінансування за ключовими напрямами:

закупівлю програмного, програмно-апаратного, апаратного обладнання та з'єднувального (такелажного обладнання) згідно номенклатури закупівлі;

фінансування за статтею заробітна платня персоналу залученого комерційних (державних) фірм по встаткуванню та налагодженню складової в системі зв'язку;

резервний фонд на випадок масштабування (збільшення) числа модулів, блоків у визначених Законами і підзаконними актами у випадках стихійного лиха, антитерористичної операції, війни, без зворотної втрати в ході експлуатації (фізичної втрати в бою), тощо.

У загальному вигляді науковий проект можна класифікувати таким чином – див. табл. 3.

*Таблиця 3*

**Загальна класифікація наукового проекту**

| Параметр | Рівень | Очікування |
|---|---|---|
| Рівень організації | міжнародний | |
| | державний | + |
| | відомчий | + |
| | освітня установа | + |
| Форма організації | програма | |
| | тема | |
| | НДР | + |
| | дисертація | + |

У загальному вигляді оцінка трудового ресурс необхідних для реалізації теоретичної частини концепції представлено в табл. 4.

*Таблиця 4*

**Оцінка трудових ресурсів**

| Параметр | Рівень | Очікування |
|---|---|---|
| Склад учасників | наукові співробітники | + |
| | викладачі | –/+ |
| | докторанти/аспіранти | –/+ |

## Висновки й перспективи подальших досліджень

На нашу думку є раціональним вибір інноваційного шляху обґрунтований у концепції побудови системи кібернетичної безпеки. Ця раціональність ґрунтується на застосуванні блочно-модульного підходу до побудови системи, що спрощує процедуру просторового масштабування та функціонального доповнення.

**Елемент наукової новизни.**

Авторами запропоновано застосування підходів масштабування та доповнення при проектуванні СКБ ІТВ, що дозволить динамічно розширювати функціональну можливість СКБ і відійти від стаціонарного підходу рішення.

**Перспективи подальших досліджень у даному напрямку** доцільно зосередити:

на дослідженні поняття довірливого програмно-апаратного забезпечення;

з'ясуванні коректності застосування довірливого програмно-апаратного забезпечення в даній концепції.

## *Література*

**1. Про рішення** Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Воєнної доктрини України": Указ Президента України № 390/2012 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/390/2012. **2. Про Доктрину** інформаційної безпеки України: Указ Президента України №514/2009 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/514/2009. **3. Бородакий Ю. В.** Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) / Ю. В. Бородакий, А. Ю. Добродеев, И. В. Бутусов // Вопросы кибербезопасности. 2013. – №1(1). – С. 2–9. **4. Бородакий Ю. В.** Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) / Ю. В. Бородакий, А. Ю. Добродеев, И. В. Бутусов // Вопросы кибербезопасности. 2014. – №1(2). – С. 5–12. **5. Мазур И. И.** Управление проектами: справочное пособие / И. И. Мазур, В. Д. Шапиро. – М.: Высш. шк., 2001. – 875 с.

## КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМЫ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ СТАЦИОНАРНЫХ ИНФОРМАЦИОННО ТЕЛЕКОММУНИКАЦИОННЫХ УЗЛОВ УКРАИНЫ НА ПРИНЦИПАХ МАСШТАБИРОВАНИЯ И ДОПОЛНЕНИЯ

***Игорь Николаевич Козубцов (канд. техн. наук, с.н.с)***
***Владимир Викторович Куцаев***
***Владимир Александрович Ткач***
***Леся Михайловна Козубцова***

***Военный институт телекоммуникаций и информатизации, Киев, Украина***

*Авторами на основе существующих идей обоснованно концептуальный подход к построению системы кибернетической безопасности стационарных информационно телекоммуникационных узлов Украины на принципах масштабирования и дополнения. Это дает возможность динамически расширять функциональные возможности системы кибернетической безопасности без разработки дополнительной конструкторской документации и потерь времени на ее согласование. Избран блочно модульный подход до формирования и комплектации узлов системы кибернетической безопасности обеспечивает быструю настройку и ремонт оборудования (возобновление работоспособности системы*

*и соответствия новым кибернетическим угрозам). Предложен адекватный путь реализации концепции построения системы кибернетической безопасности стационарных информационно телекоммуникационных узлов Украины.*

***Ключевые слова:*** *концептуальный подход; построение; системы кибернетической безопасности; стационарный; информационно телекоммуникационный узел; принцип; масштабирование; дополнение.*

## THE CONCEPTUAL APPROACH TO CONSTRUCTION OF THE UKRAINE INFORMATION TELECOMMUNICATION NODES CYBER SECURITY SYSTEM BASED ON SCALING AND COMPLEMENTATION PRINCIPLES

***Igor M. Kozubtsov*** *(Candidate of Technical Sciences, Senior Research Fellow)*
***Volodymyr V. Kutsaiev***
***Volodymyr O. Tkach***
***Lesja M. Kozubtsova***

***Military Institute of Telecommunications and Informatization, Kyiv, Ukraine***

*By authors on the basis of existent ideas grounded conceptual going near the construction of the cybernetic safety system of stationary informatively telecommunication knots of Ukraine on principles of down-scaling and addition. It enables dynamically to extend functional possibilities of cybernetic safety system without development of additional designer document and losses time on its concordance. Block module approach is select to forming and acquisition knots of cybernetic safety system provides the rapid tuning and repair of equipment (proceeding in the capacity of the system and accordance to the new cybernetic threats). The adequate way for realization the conception of construction of cybernetic safety system of stationary informatively telecommunication knots of Ukraine is offered.*

***Keywords:*** *conceptual approach; construction; systems of cybernetic security; stationary; informatively telecommunication knot, principle; down-scaling; addition.*

## *References*

**1. Pro rishennia** Rady natsionalnoi bezpeky i oborony Ukrainy vid 8 chervnia 2012 roku "Pro novu redaktsiiu Voiennoi doktryny Ukrainy": Ukaz Prezydenta Ukrainy №390/2012 [Elektronnyi resurs], Rezhym dostupu: http://zakon3.rada.gov.ua/laws/show/390/2012. **2. Pro** Doktrynu informatsiinoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy №514/2009 [Elektronnyi resurs], Rezhym dostupu: http://zakon2.rada.gov.ua/laws/show/514/2009.

**3. Borodakiy Yu.V.** (2013) Cyber Security as a major factor of national and international security XXI century (Part 1). [*Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti HHI veka (Chast 1)*], Dobrodeev A.Yu., Butusov I.V., Voprosyi kiberbezopasnosti, No 1(1), pp. 2–9. **4. Borodakiy Yu.V.,** (2014) Cyber Security as a major factor of national and international security XXI century (Part 2). [*Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti HHI veka (Chast 2)*], Dobrodeev A.Yu., Butusov I.V., Voprosyi kiberbezopasnosti, No 1(2), pp. 5–12. **5. Mazur I.I.** (2001) Project Management: handbook. [*Upravlenie proektami: spravochnoe posobie*], Shapiro V.D., Moscow, Vyissh.shk, 875 p.

Отримано: 27.10.2015 р.