КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.11.166182
УДК 004.056.53

Гнатюк Сергій Олександрович
д.т.н., доцент, заступник декана факультету кібербезпеки, комп'ютерної та програмної інженерії
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua

Юдін Олексій Юрійович
к.т.н., заступник начальника
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ, Україна
ORCID ID: 0000-0002-4730-1463
alex@ukrdeftech.com.ua

Сидоренко Вікторія Миколаївна
к.т.н., доцент кафедри безпеки інформаційних технологій
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Євченко Ярослав Петрович
аспірант
Інститут спеціального зв'язку та захисту інформації
НТУ України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID ID: 0000-0002-2385-2658
evchenkoyaroslav29@gmail.com

МЕТОД ФОРМУВАННЯ ФУНКЦІОНАЛЬНОГО ПРОФІЛЮ ЗАХИЩЕНОСТІ ГАЛУЗЕВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Анотація. Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту інформаційно-телекомунікаційних систем, зокрема, галузевих, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення інформаційної складової національної безпеки. З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми захисту критичної інфраструктури, на загальнодержавному рівні, створення системи захисту такої інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України. Таким чином, виникає необхідність розробки методів та моделей віднесення інформаційно-телекомунікаційних систем до критичної інфраструктури для забезпечення національної безпеки України. У роботі запропоновано структурно-функціональний метод визначення функціонального профілю захищеності підсистеми галузевої інформаційно-телекомунікаційної системи, що дозволяє за рахунок визначення галузевих вимог до конфіденційності , цілісності, доступності та спостереженості здійснити коригування базового функціонального профілю захищеності галузевої інформаційно-телекомунікаційної системи та більш повно сформулювати критерії оцінки захищеності інформації, що циркулює в критичних інформаційно-телекомунікаційних системах. Продовженням дослідження стало проведення експериментального дослідження на прикладі ІТС Національної системи конфіденційного зв'язку, за допомогою якого перевірено адекватність реагування методу на зміну вхідних даних.

Ключові слова: інформаційно-телекомунікаційні системи, критична інфраструктура, об'єкт критичної інфраструктури, кібербезпека, оцінка захищеності, функціональний профіль захищеності.

ВСТУП

Світові тенденції до збільшення кількості та підвищення складності кібератак зумовили актуалізацію питання захисту галузевих інформаційно-телекомунікаційних систем (ІТС), зокрема, галузевих, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення інформаційної складової національної безпеки.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми захисту критичної інфраструктури, на загальнодержавному рівні, створення системи захисту такої інфраструктури є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

При цьому, основними проблемами, які потребують розв'язання, є:

–відсутність єдиних критеріїв та методології віднесення ІТС об'єктів інфраструктури до критичної інфраструктури;

–відсутність єдиної методології оцінювання загроз безпеці ІТС об'єктів критичної інфраструктури.

Постановка проблеми. Необхідно зазначити, що Законом України «Про основні засади забезпечення кібербезпеки України» [1] визначено необхідність формування переліку об'єктів критичної інформаційної інфраструктури та необхідність розробки критеріїв і порядку віднесення об'єктів до об'єктів критичної інфраструктури, а Указом Президента України №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [2] передбачено, що кіберзахист критичної інфраструктури має полягати, насамперед, у визначенні критеріїв віднесення інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури.

Таким чином, нормативно-правовими актами України задекларовано необхідність розробки єдиних критеріїв і методології віднесення ІТС об'єктів інфраструктури до критичної інфраструктури. При цьому доцільно зазначити, що використання якісних оцінок пов'язане зі складністю їх порівнювання та відтворювання. Насамперед, це обумовлено складністю підбору експертів і специфікою обробки експертних даних. Ці обмеження в меншій мірі характерні для методів розрахунку кількісних оцінок критичності.

Зазначені обмеження свідчать про наявність важливого наукового завдання щодо визначення критеріїв віднесення ІТС до критичної інформаційної інфраструктури.

Аналіз останніх досліджень і публікацій. Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [3] та Закону України «Про захист персональних даних» [4] обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом. З метою забезпечення захисту інформації в ІТС повинна бути побудована комплексна система захисту інформації (КСЗІ). Також необхідно зазначити, що постановою Кабінету Міністрів України «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [5] встановлено норму щодо впровадження на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації.

В той же час, можливо констатувати, що НД ТЗІ України, які описують порядок створення КСЗІ [6] та критерії оцінки захищеності інформації [7] вже морально застарілі та не відповідають вимогам сьогодення [8; 9]. Так наприклад, критерії визначені НД ТЗІ [7] не поновлювались з 1999 року, а вимоги щодо порядку створення

КСЗІ – з 2005 року. Натомість, міжнародні нормативні документи переглядаються та уточнюються майже щороку [10].

Таким чином виникає протиріччя в необхідності створення КСЗІ та застарілості норм, за якими ця КСЗІ створюється.

В більшості країн світу інформаційно-телекомунікаційна галузь займає одне з перших місць за критичністю після енергетики та транспорту [8]. З урахуванням цього експериментальна перевірка розроблених у роботі положень була здійснена на прикладі ІТС Національної системи конфіденційного зв'язку (НСКЗ).

Відповідно до Закону України «Про Національну систему конфіденційного зв'язку» [11] НСКЗ є сукупністю спеціальних телекомунікаційних систем подвійного призначення, які за допомогою криптографічних та технічних засобів забезпечують обмін інформацією з обмеженим доступом, в інтересах органів державної влади та органів місцевого самоврядування.

Основними функціями НСКЗ, згідно Постанови Кабінету Міністрів України «Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку» [12] є:

- забезпечення обміну відкритою, службовою та конфіденційною інформацією між суб'єктами та/або абонентами систем НСКЗ і її захисту;
- створення технологічного підґрунтя для інтеграції розподілених інформаційних ресурсів в ІТС, у яких циркулює відкрита та службова інформація органів державної влади та органів місцевого самоврядування, військових формувань, державних органів, державних підприємств, установ та організацій;
- забезпечення взаємодії між ІТС органів державної влади та органів місцевого самоврядування, військових формувань, державних органів, державних підприємств, установ та організацій;
- надання ресурсу спеціальної транспортної мережі НСКЗ для забезпечення функціонування спеціальних ІТС суб'єктів НСКЗ;
- забезпечення захищеного доступу державних органів до Інтернету.

Враховуючи зазначені функції, можна припустити, що НСКЗ, або її підсистеми, відноситься до категорії критичних. Також, при віднесенні ІТС до категорії критичних, необхідно враховувати не задекларовані функції, а реальні, які система реалізує на теперішній час.

Додатково, при визначенні критичності ІТС, необхідно враховувати, що згідно з Указом Президента України від 18.04.2005 №663 «Про забезпечення урядовим зв'язком посадових осіб» [13] система урядового зв'язку забезпечується ресурсами телекомунікаційних мереж на всій території України і для забезпечення функціонування системи урядового зв'язку можуть використовуватись засоби і ресурси телекомунікаційних мереж операторів телекомунікацій. Відповідно до «Інструкції з організації технічної експлуатації мереж і комплексів державної системи урядового зв'язку України» [14] одним з основних елементів станції урядового зв'язку є цифровий лінійно-апаратний зал транспортної мережі спеціального призначення НСКЗ.

Мета статті. Метою даної статті є розробка та експериментальне дослідження структурно-функціонального методу формування функціонального профілю захищеності (ФПЗ) галузевої ІТС

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Структурно-логічна модель формування функціонального профілю захищеності галузевої ІТС

З урахуванням того, що, нормативний документ системи технічного захисту інформації України [7] результатом оцінки визначає рейтинг, який є упорядкованим рядом (переліченням) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій, необхідно реалізувати метод формування ФПЗ, який буде враховувати вимоги цього документу, що в свою чергу дозволить використовувати результати методу при побудові комплексних систем захисту інформації.

Запропонована структурно-логічна модель визначення ФПЗ галузевої ІТС (рис. 1) ґрунтується на використанні базового (початкового) ФПЗ. Базовий ФПЗ обирається з урахуванням вимог [7].

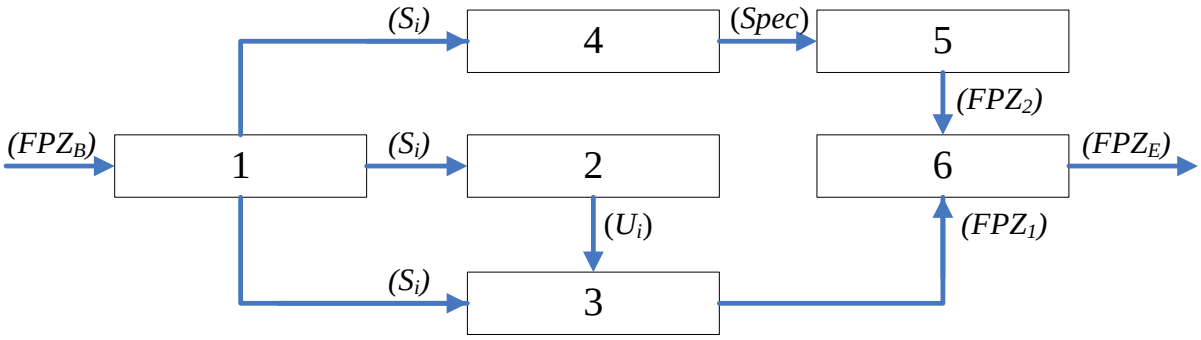

Рисунок 1. Структурно-логічна модель визначення ФПЗ галузевої ІТС

В блоці 1 здійснюється визначення множини основних систем галузевої ІТС (Si).

В блоці 2 визначаються інформаційні потоки (інтерфейсів) взаємодії основних систем галузевої ІТС між собою (Ui).

В блоці 3 визначаються специфічні (галузеві), по відношенню до базових, вимоги, щодо КЦДС, до (Si) і формується ФПЗ – FPZ1.

В блоці 4 аналізуються нормативні документи та кращі практики (ISO/IEC, NIST, NERC CIP, ISACA, CERT, SANS, PCI DSS, COBIT, HIPAA, CSA, ITAF) щодо наявності додаткових або деталізованих вимог (Spec).

В блоці 5 здійснюється зіставлення деталізованих (додаткових) вимог до семантики НД ТЗІ 2.5-004-99 та формування вимог FPZ2. В блоці 6 відбувається коригування базового ФПЗ, або розробка ФПЗ для нової основної системи галузевої ІТС FPZE.

Зазначена модель дозволяє використовувати окрім рекомендованого інші профілі захищеності, які може запропонувати експерт. Запропонована модель дозволяє формалізувати реалізовані послуги безпеки та їх рівні з урахуванням додаткових вимог, які базуються на кращих світових практиках, щодо захищеності галузевих ІТС.

Структурно-функціональний метод формування функціонального профілю захищеності галузевої ІТС

Структурно функціональний метод формування ФПЗ галузевої ІТС складається з наступних етапів:

Етап 1. Визначення множини основних систем (елементів) галузевої ІТС (Si) та інформаційних потоків (інтерфейсів) взаємодії цих систем галузевої ІТС (Ui);

Етап 2. Формування специфічних (галузевих), по відношенню до базових, вимог щодо КЦДС до (Si) – FPZ1;

Етап 3. Визначення нормативних документів та кращих практик щодо наявності додаткових або деталізованих вимог (Spec);

Етап 4. Формування деталізованих (додаткових) вимог у вигляді семантики НД ТЗІ та формування вимог FPZ2;

Етап 5. Коригування базового ФПЗ, або розробка ФПЗ для нової системи галузевої ІТС FPZE.

Запропонований структурно-функціональний метод визначення ФПЗ галузевої ІТС враховує сучасний досвід і кращі світові практики та дозволяє, більш детально та об'єктивно, в порівнянні з діючим НД ТЗІ 2.5-004-99, сформулювати критерії оцінки захищеності інформації, яка циркулює в критичних ІТС.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Експериментальне дослідження структурно-функціонального методу формування функціонального профілю захищеності галузевої ІТС

Застосування методу було розглянуто на прикладі ІТС НСКЗ.

Етап 1. Визначення множини основних систем (елементів) галузевої ІТС (Si) та інформаційних потоків (інтерфейсів) взаємодії цих систем галузевої ІТС (Ui).

Відповідно до [12] НСКЗ складається з таких відокремлених ІТС спеціального зв'язку (далі – системи НСКЗ):

1) спеціальна транспортна мережа НСКЗ – телекомунікаційна мережа, призначена для транзиту трафіку між системами НСКЗ;

2) спеціальні ІТС суб'єктів НСКЗ, призначені для обміну відкритою, службовою та конфіденційною інформацією в інтересах органів державної влади, юридичних та фізичних осіб, які замовляють та/або отримують послуги НСКЗ;

3) спеціальна мережа мобільного зв'язку НСКЗ, призначена для обміну службовою і конфіденційною інформацією в інтересах суб'єктів НСКЗ під час перебування у стаціонарних і позастаціонарних умовах за допомогою мобільних абонентських терміналів, захист якої забезпечується шляхом застосування криптографічних та технічних методів і засобів. У складі спеціальної мережі мобільного зв'язку НСКЗ функціонує спеціальна мережа стільникового зв'язку;

4) спеціальна ІТС захищеного відеоконференцзв'язку НСКЗ, призначена для проведення в режимі реального часу службових нарад керівниками органів державної влади та органів місцевого самоврядування;

5) система захищеного електронного документообігу НСКЗ, призначена для забезпечення оперативного обміну електронними документами, що містять службову та конфіденційну інформацію, між органами державної влади, органами місцевого самоврядування, а також здійснення аналізу та контролю за виконанням рішень

Президента України і Кабінету Міністрів України. У складі системи захищеного електронного документообігу функціонує акредитований центр сертифікації ключів, призначений для надання органам державної влади та органам місцевого самоврядування послуг електронного цифрового підпису в зазначеній системі;

6) система захищеного доступу державних органів до Інтернету НСКЗ, призначена для захисту державних інформаційних ресурсів державних органів, що обробляються в інформаційно-телекомунікаційних системах і доступ до яких здійснюється через Інтернет.

Найбільш критичними, з точки зору витоку інформації з обмеженим доступом (ІзОД), є спеціальна транспортна мережа, спеціальна ІТС захищеного відеоконференцзв'язку та система захищеного електронного документообігу (далі - ЕДО).

За функціональним призначенням виділені системи можна скомпонувати наступним чином:

–спеціальна транспортна мережа – транспортна система, система захисту інформації, система управління;

–ІТС відеоконференцзвязку та захищеного ЕДО – сервісні системи (надання послуг абоненту).

Таблиця 1

Декомпозиція систем НСКЗ

№	Об'єкт	Опис
Транспортна мережа		
1	Система офісу (St1)	Забезпечення підключення абонентського обладнання на фізичному рівні
1.1	Система абонентського обладнання (St11)	Прикінцеве обладнання (телефони, кабель, з'єднувачі, засоби захисту інформації)
1.2	Система доступу до мережі (St12)	Обладнання, що забезпечує доступ до мережі (комутатор, маршрутизатор, кабельна структура)
1.3	Допоміжні системи захисту (St13)	Допоміжне обладнання (засоби резервного живлення, датчики сигналізації, лінії сигналізації)
2	Система телекомунікаційного оператору (St2)	Забезпечення підключення операторського обладнання на фізичному рівні
2.1	Система фізичного рівня (St21)	Кабель, з'єднувачі, підсилювачі (повторювачі) сигналу, комутаційні панелі, конвертери сигналу, мережеві адаптери
2.2	Система канального рівня (St22)	Комутатори доступу, вузлові комутатори, сервісні комутатори
2.3	Система транспортного та мережевого рівня (St23)	Магістральні комутатори, мультисервісні маршрутизатори, комутатори операторського класу
2.4	Прикладні системи (St24)	Сервери системи управління фізичного рівня, сервери управління канального рівня, сервери управління транспортного та мережевого рівня
3	Система оператору зв'язку (St3)	Забезпечення підключення операторського обладнання на логічному рівні
3.1	Система фізичного рівня (St31)	Структурована кабельна система, мережеві адаптери, перетворювачі сигналів
3.2	Система канального рівня (St32)	Комутатори доступу
3.3	Система транспортного та мережевого рівня (St33)	Комутатори, маршрутизатори
3.4	Прикладні системи (St34)	Сервери контролю та управління транспортного та мережевого рівня
Сервісні системи (надання послуг)		
4	Система офісу (Ss1)	

4.1	Прикладні системи абонентського обладнання (Ss11)	Прикінцеве обладнання (термінал зв'язку, термінал відеозв'язку, АРМ передачі даних
5	Система оператору зв’язку (Ss2)	Забезпечення надання послуг споживачам
5.1	Прикладні системи оператору зв’язку (Ss21)	Сервери електронної пошти, центр сертифікації ключів, сервери реєстрів та довідників, сервер CUCM, сервер контролеру домену, сервер відеозв'язку, сервер контактцентру
5.2	Система управління та резервування (Ss22)	Сервери резервного зберігання даних, Prime Collaboration Assurance, Prime Collaboration Provisioning, АРМ управління (черговий)
Система захисту інформації		
6	Система офісу (Sd1)	Захист прикінцевого обладнання та приміщень
6.1	Система захисту абонентського обладнання (Sd11)	КЗЗ телефону, блок підключення телефону
6.2	Система захисту доступу до мережі (Sd12)	КЗЗ комутатору, КЗЗ маршрутизатору, засіб криптографічного захисту інформації
6.3	Допоміжні системи захисту (Sd13)	Датчики сигналізації, датчики протипожежної сигналізації, пульт сигналізації
7	Система телекомунікаційного оператору (Sd2)	Захист каналів зв’язку та обладнання оператору
7.1	Система захисту фізичного рівня (Sd21)	Прилади виявлення пошкодження кабелю, прилади контролю підсилювачів (повторювачів) сигналу, мультиплексор
8	Система оператору зв’язку (Sd3)	Захист операторського обладнання
8.1	Система моніторингу та захисту канального рівня (Sd22)	КЗЗ комутатору доступу, КЗЗ вузлового та сервісного комутатору
8.2	Система моніторингу та захисту транспортного і мережевого рівня (Sd23)	КЗЗ маршрутизатору, КЗЗ комутатору, КЗЗ системи моніторингу, КЗЗ системи управління, КЗЗ АРМу управління
8.3	Допоміжні системи захисту (Sd24)	КЗЗ системи захисту фізичних ліній зв'язку, КЗЗ системи сигналізації
9	Система оператору зв’язку (Sd3)	Здійснення управління системами оператору зв’язку
9.1	Система захисту фізичного рівня (Sd31)	Прилади виявлення пошкодження кабелю, прилади контролю підсилювачів (повторювачів) сигналу, мультиплексор
9.2	Система моніторингу та захисту канального рівня (Sd32)	КЗЗ комутатору доступу, КЗЗ вузлового та сервісного комутатору, DDoS Protector
9.3	Система моніторингу та захисту транспортного і мережевого рівня (Sd33)	КЗЗ маршрутизатору, КЗЗ комутатору, КЗЗ системи моніторингу, КЗЗ системи управління, КЗЗ АРМу управління, DDoS Protector
9.4	Система захисту прикладного рівня (Sd34)	Міжмережевий екран Next Generation Threat Prevention, міжмережевий екран, захист операційних систем, захист баз даних
9.5	Система криптографічного захисту (Sd35)	Засоби криптографічного захисту інформації
9.6	Допоміжні системи захисту (Sd36)	Засоби резервного живлення, датчики сигналізації, лінії сигналізації, пульт сигналізації, пристрої (системи) охолодження
Система управління		
10	Система офісу (Sm1)	Здійснення управління та контролю прикінцевим обладнанням
10.1	Система сенсорів абонентів (Sm11)	Датчики розкриття монтажної коробки, сенсори підключення абонентського обладнання, сенсори доступу до засобу КЗІ
10.2	Система управління доступом до мережі (Sm12)	АРМ налаштування комутатору та маршрутизатору, ПЗ комутатору та маршрутизатору, ПЗ засобів резервного

		живлення
10.3	Система протоколювання роботи (Sm13)	ПЗ комутатору та маршрутизатору, ПЗ засобів резервного живлення, ПЗ абонентського обладнання
11	Система оператору зв'язку (Sm2)	Здійснення управління системами оператору зв'язку
11.1	Система управління обладнанням вузлів (Sm21)	ПЗ управління роботою мультиплексорів, ПЗ управління роботою комутаторів та маршрутизаторів, ПЗ управління роботою апаратного забезпечення серверів, ПЗ управління міжмережевими екранами та DDoS протекторами
11.2	Система управління засобами криптографічного захисту (Sm22)	ПЗ управління засобами КЗІ, ПЗ управління центром сертифікації ключів
11.3	Система управління прикладним ПЗ (Sm23)	ПЗ управління прикладним ПЗ серверів
11.4	Система управління АО (Sm24)	ПЗ віддаленого конфігурування абонентського обладнання

Етап 2. Формування специфічних (галузевих), по відношенню до базових, вимог щодо КЦДС до (Si) – FPZ1.

На теперішній час ядро НСКЗ включає в себе наступні основні компоненти [15]:

CUCM – Cisco Unified Communications Manager. Центральний компонент комунікаційної платформи Cisco через яку взаємодіють і до якої підключаються інші сервіси Cisco, такі як IM&Presence, Contact Center Express, Pagginig, Media Sence, Webex, зовнішні допоміжні сервіси і інформаційні системи, такі як Microsoft Active Directory (LDAP), DNS, Aurus Directory і інші. CUCM є кластером з двох віртуальних машин. Основний сервер, який обробляє виклики і обслуговує абонентів в штатному режимі називається Publisher, другий сервер, який так само є активним але не обслуговує абонентів в штатному режимі, називається Subscriber.

Сервіс Cisco IM&Presence – є віртуальною машиною, або кластером з двох віртуальних машин. Сервіс дозволяє збирати і публікувати інформацію про статус користувача і розширює його комунікаційні можливості. Доступність користувача визначає чи можна встановити з ним комунікації, а також інформацію про можливі способи комунікації, наприклад аудіо-зв'язок, e-mail, інтерактивний обмін повідомленнями. Сукупна інформація відображається в клієнтському додатку Jabber, який підвищує швидкість і ефективність взаємодії з колегами, за допомогою вибору найбільш ефективного способу комунікації. Центральний внутрішній компонент називається Extensible Communications Platform (XCP). XCP використовує протоколи SIP / SIMPLE and Extensible Messaging і Presence Protocol (XMPP). Основний сервер, який обробляє повідомлення і обслуговує абонентів в штатному режимі називається Publisher, другий сервер, який так само є активним але не обслуговує абонентів в штатному режимі, називається Subscriber.

Сервіс MediaSence – дозволяє записувати розмови абонентів, потім переглядати, прослуховувати і завантажувати їх через веб-інтерфейс.

Сервіс Cisco Webex Server – система для онлайн конференцій, нарад, відео конференцій, вебмінаров. Клієнти завантажуються в web-бразуер як плагіни, потім підключаються до сервера. Cisco Webex Server складається з декількох віртуальних машин. Віртуальна машина адміністратора, віртуальна машина зворотного проксі для доступу з Інтернету, віртуальна машина конференцій Webex і віртуальна машина для обробки медіа даних. Залежно від кількості одночасних сесій і можливості доступу з Інтернету, число віртуальних машин змінюється.

R-PC – Prime Collaboration Software. Забезпечує єдиний інтерфейс для управління абонентами і всіх комунікаційних сервісів, і швидке налаштування обладнання та інтеграції з мережею передачі даних.

Функції: наскрізний моніторинг; перегляд всіх сесій – планованих, виконаних, поточних; швидкий пошук місця проблеми – мережа або термінал; контроль затримок, втрат пакетів – оперативна діагностика; перегляд маршруту відео та голосової сесії в мережі; перегляд статистики по CPU, пам'яті і інтерфейсів обладнання Cisco; перегляд джиттера, втрат пакетів, даних DSCP для обладнання Cisco.

CTI-CMS – Cisco Meeting Server 1000 Bundle. Програмна платформа для конференцзв'язку надає наступні можливості.

Підключення будь-якого учасника за допомогою: відеотерміналів Cisco або сторонніх виробників; клієнта Cisco Jabber; Cisco Meeting App (клієнтську програму або через сумісний з WebRTC браузер); Skype for Business.

Розгортання рішень на платформах Cisco CMS, з підтримкою до 96 портів відео високої чіткості в одному стійко-місці (1RU).

Необмежене збільшення числа учасників завдяки простій масштабованості і уніфікованого користувальницького середовища, що не залежить від платформи.

Контроль витрат завдяки оптимізації використання смуги пропускання між центрами обробки даних.

ASA5516-FPWR – ASA 5516-X with FirePOWER services. Багатофункціональний міжмережевий екран, призначений для розширеного захисту від новітніх загроз і шкідливих програм. Брандмауер Cisco ASA з сервісами FirePOWER забезпечує інтегрований захист від загроз протягом усього процесу атаки – перед її початком, під час атаки і після її завершення – шляхом об'єднання в одному пристрої можливостей брандмауера Cisco ASA і кращих в галузі функцій захисту від загроз і шкідливих програм Sourcefire.

Cisco ASA з сервісами FirePOWER пропонує повний набір функцій, а саме:

–функції віддаленого доступу до мереж VPN і розширеною кластеризацією, що забезпечує швидкий і безпечний доступ і високу надійність систем;

–функція детального моніторингу і контролю додатків (AVC) підтримує більш 3000 елементів управління на рівні додатків, які в разі ризику можуть активувати встановлені політики виявлення загроз в системі захисту від вторгнень (IPS), що дозволяє значно підвищити ефективність захисту;

–система запобігання вторгнень нового покоління FirePOWER (NGIPS) значно підвищує ефективність захисту від загроз і надає повну контекстуальну інформацію про користувачів, інфраструктуру, додатків та їх вмісту, що дозволяє вчасно виявляти багатовекторні загрози і автоматизувати процес захисту.

–фільтрація URL-адрес по репутації і категоріям забезпечує комплексне оповіщення і контроль над підозрілим веб-трафіком, а також застосування політик для сотень мільйонів URL-адрес в більш ніж 80 категоріях;

–удосконалена система захисту від шкідливого ПО забезпечує високу ефективність виявлення вторгнень, низьку вартість володіння і оптимальний рівень захисту, дозволяючи швидко виявляти, аналізувати і намагатися запобігти розповсюдженню шкідливого ПО та виникаючих загроз, які можуть бути пропущені на інших рівнях захисту.

З урахуванням наведених компонент ядра НСКЗ, а також декомпозиції системи (табл. 1) викладемо вимоги щодо безпеки відносно кожного з об’єктів (систем). Зазначені вимоги викладені в табл. 2, при цьому зазначимо, що викладені вимоги з безпеки вже реалізовані в НСКЗ.

Таблиця 2

Функціональний профіль захищеності об'єктів НСКЗ

№	Об'єкт	Опис
Транспортна мережа		
1	Система офісу (St1)	
1.1	Система абонентського обладнання (St11)	КА-2, КВ-3, ЦА-2, ЦВ-2, НК-1, НВ-1, НР-2, НТ-2, НИ-2, НА-1, НП-1
1.2	Система доступу до мережі (St12)	КА-1, КА-2, КВ-3,ЦА-1, ЦА-2, ЦВ-2, ДР-1, ДС-1, ДВ-1, НР-1, НР-2, НТ-2, НИ-1, НИ-2, НА-1, НК-1, НО-2, НЦ-1, НЦ-2, НВ-1, НП-1
1.3	Допоміжні системи захисту (St13)	ДС-1, ДВ-1, НТ-2, НР-1
2	Система телекомунікаційного оператору (St2)	
2.1	Система фізичного рівня (St21)	КА-2, ЦА-1, ДС-1, ДЗ-1,ДВ-1, НР-1, НР-2, НИ-2, НО-2, НК-1, НТ-2
2.2	Система канального рівня (St22)	КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1, ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1
2.3	Система транспортного та мережевого рівня (St23)	КА-1, КА-2, ЦА-1, ЦА-2, ЦО-2, ДР-1, ДС-1, ДЗ-1, ДЗ-2, ДВ-1, НР-1, НИ-1, НИ-2, НК-1, НО-2, НТ-2, НВ-1
2.4	Прикладні системи (St24)	КА-2, КД-2. КО-1, КВ-2, ЦА-1, ЦВ-1, ЦД-1, ЦО-1, ДС-2, ДЗ-2, ДВ-2, ДР-2, НР-2, НИ-2, НО-1, НК-1, НТ-2, НВ-1
3	Система оператору зв'язку (St3)	
3.1	Система фізичного рівня (St31)	КА-2, ЦА-1, ДС-1, ДЗ-1,ДВ-1, НР-1, НР-2, НИ-2, НО-2, НК-1, НТ-2
3.2	Система канального рівня (St32)	КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1, ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НВ-1
3.3	Система транспортного та мережевого рівня (St33)	КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1, ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НВ-1
3.4	Прикладні системи (St34)	КА-2, КД-2. КО-1, КВ-2, ЦА-1, ЦВ-1, ЦД-1, ЦО-1, ДС-2, ДЗ-2, ДВ-2, ДР-2, НР-2, НИ-2, НО-1, НК-1, НТ-2, НВ-1
Сервісні системи (надання послуг)		
4	Система офісу (Ss1)	
4.1	Прикладні системи абонентського обладнання (Ss11)	КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НТ-2, НВ-1
5	Система оператору зв'язку (Ss2)	
5.1	Прикладні системи оператору зв'язку (Ss21)	КД-2, КА-1, КА-2, КО-1, КВ-1, ЦД-1, ЦА-1, ЦА-2, ЦО-1, ЦВ 1, ДР-1, ДС-1, ДЗ-2, ДВ-2, НР-2, НИ-1, НИ-2, НК-1, НО-1, НО-3, НТ-2, НВ-1
5.2	Система управління та резервування (Ss22)	КА-1, КА-2, КД-2, КО-1, КВ-2, ЦА-1, ЦВ-1, ЦД-1, ЦО-1, ЦО-2, ДС-2, ДЗ-2, ДВ-2, ДР-2, НР-2, НИ-2, НО-1, НО-2, НК-1, НТ-2, НВ-1
Система захисту інформації		
6	Система офісу (Sd1)	
6.1	Система захисту абонентського обладнання (Sd11)	ЦО-1, ДС-1, ДВ-1, НР-1, НР-2, НЦ-1, НВ-1, НТ-2
6.2	Система захисту доступу до мережі (Sd12)	КА-1, КА-2, КВ-2, ЦА-1, ЦА-2, ЦВ-2, ДР-1, ДС-1, ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НТ-2, НЦ-1, НЦ-2, НВ-1, НА-1, НП-1
6.3	Допоміжні системи захисту (Sd13)	ДС-1, ДВ-1, НТ-2, НР-1, НТ-2
7	Система телекомунікаційного оператору (Sd2)	

7.1	Система захисту фізичного рівня (Sd21)	КА-2, ЦА-1, ДС-1, ДЗ-1,ДВ-1, НР-2, НИ-2, НО-2, НК-1, НЦ-1, НТ-2
7.2	Система моніторингу та захисту канального рівня (Sd22)	КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1, ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1
7.3	Система моніторингу та захисту транспортного і мережевого рівня (Sd23)	КА-2, КД-2, КО-1, КВ-2, ЦА-1, ЦА-2, ЦВ-1, ЦД-1, ЦО-1, ДР-1, ДС-2, ДЗ-2, ДВ-2, ДР-2, НР-2, НИ-2, НО-1, НО-3, НК-1, НЦ-1, НТ-2, НВ-1
7.4	Допоміжні системи захисту (Sd24)	ДС-1, ДВ-1, НТ-2, НР-1
8	Система оператору зв'язку (Sd3)	
8.1	Система захисту фізичного рівня (Sd31)	КА-2, ЦА-1, ДС-1, ДЗ-1,ДВ-1, НР-2, НИ-2, НО-2, НК-1, НЦ-1, НТ-2
8.2	Система моніторингу та захисту канального рівня (Sd32)	КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1, НТ-2
8.3	Система моніторингу та захисту транспортного і мережевого рівня (Sd33)	КА-2, КД-2, КО-1, КВ-2, ЦА-1, ЦВ-1, ЦД-1, ЦО-1, ДС-2, ДЗ-2, ДВ-2, ДР-2, НР-2, НИ-2, НО-1, НО-3, НК-1, НЦ-1, НЦ-2, НТ-2, НВ-1
8.4	Система захисту прикладного рівня (Sd34)	КД-2, КА-1, КА-2, КО-1, КВ-1, ЦД-1, ЦА-1, ЦА-2, ЦО-1, ЦО-2, ЦВ-1, ДР-1, ДС-1, ДЗ-2, ДВ-2, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-1, НЦ-2, НТ-2, НВ-1
8.5	Система криптографічного захисту (Sd35)	КА-2, КВ-3, ЦА-2, ЦВ-2, НК-1, НВ-1, НР-2, НТ-2, НЦ-2, НИ-2, НА-1, НП-1
8.6	Допоміжні системи захисту (Sd36)	ДС-1, ДВ-1, НТ-2, НР-1
Система управління		
9	Система офісу (Sm1)	
9.1	Система сенсорів абонентів (Sm11)	ДС-1, ДВ-1
9.2	Система управління доступом до мережі (Sm12)	КА-1, КА-2, КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦА-2, ЦВ-1, ЦО-1, ДР-1, ДС-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1
9.3	Система протоколювання роботи (Sm13)	КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1, ДВ-1, НТ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1
10	Система оператору зв'язку (Sm2)	
10.1	Система управління обладнанням вузлів (Sm21)	КА-1, КА-2, ЦА-1, ЦА-2, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-2, НЦ-1, НВ-1, НТ-2
10.2	Система управління засобами криптографічного захисту (Sm22)	КД-2, КА-1, КА-2, КО-1, КВ-1, КВ-2, ЦД-1, ЦА-1, ЦА-2, ЦО-1, ЦВ-1, ЦВ-2, ДР-1, ДС-1, ДЗ-2, ДВ-2, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-1, НЦ-2, НТ-2, НВ-1, НА-1, НП-1
10.3	Система управління прикладним ПЗ (Sm23)	КД-2, КА-1, КА-2, КО-1, КВ-1, ЦД-1, ЦА 1, ЦА 2, ЦО-1, ЦВ 1, ДР-1, ДС 1, ДЗ-2, ДВ-2, НР-2, НИ-1, НИ 2, НК 1, НО-3, НЦ-1, НЦ-2, НТ-2, НВ-1
10.4	Система управління АО (Sm24)	КД-2, КА-1, КА-2, КО-1, КВ-1, ЦД-1, ЦА 1, ЦА 2, ЦО-1, ЦВ 1, ДР-1, ДС 1, ДЗ-2, ДВ-2, НР-2, НИ-1, НИ 2, НК 1, НО-3, НЦ-1, НЦ-2, НТ-2, НВ-1

Формування галузевих вимог щодо КЦДС до підсистем НСКЗ – FPZ1 здійснюється з урахуванням стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу [16, 24] та з урахуванням значень табл. 2.

ФПЗ транспортної системи - КА-2, КВ-3, КД-2, КО-1, ЦА-2, ЦВ-2, ЦД-1, ЦО-2, ДС-2, ДЗ-2, ДВ-2, ДР-2, НА-1, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НР-2, НВ-1, НП-1;

ФПЗ сервісної системи - КА-2, КВ-2, КД-2, КО-1, ЦА-2, ЦВ-1, ЦД-1, ЦО-1, ДС-2, ДЗ-2, ДВ-2, ДР-2, НИ-2, НК-1, НО-3, НЦ-1, НТ-2, НР-2, НВ-2;

ФПЗ системи захисту - КА-2, КВ-3, КД-2, КО-1, ЦА-2, ЦВ-2, ЦД-1, ЦО-2, ДС-2, ДЗ-2, ДВ-2, ДР-2, НА-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НР-2, НВ-1, НП-1;

ФПЗ системи управління - КА-2, КВ-2, КД-2, КО-1, ЦА-2, ЦВ-2, ЦД-1, ЦО-2, ДС-1, ДЗ-2, ДВ-2, ДР-1, НА-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НР-2, НВ-1, НП-1.

Підсумковий ФПЗ НСКЗ можна сформулювати як поєднання ФПЗ складових систем, а саме - КА-2, КВ-3, КД-2, КО-1, ЦА-2, ЦВ-2, ЦД-1, ЦО-2, ДС-2, ДЗ-2, ДВ-2, ДР-2, НА-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НР-2, НВ-2, НП-1.

Етап 3. Визначення нормативних документів та кращих практик щодо наявності додаткових або деталізованих вимог (Spec).

Нормативними документами, що описують вимоги безпеки до систем класу НСКЗ, є:

–NIST SP 800-53A. Guide for Assessing the Security Controls in Federal Information Systems and Organizations [17];

–NIST SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations [18];

–ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки [19];

–ISO/IEC 15408-1:2009 Evaluation criteria for IT security [20].

Етап 4. Формування деталізованих (додаткових) вимог у вигляді семантики НД ТЗІ та формування вимог FPZ2.

При формуванні додаткових вимог у вигляді семантики НД ТЗІ доцільно використовувати відповідні нормативні документи [16; 21-24].

З урахуванням вимог безпеки до федеральних інформаційних систем [18] сформуємо додаткові вимоги до ФПЗ НСКЗ (табл. 3), де, в загальному випадку, під позначенням ACO_VUL розуміється розширені послуги аналізу вразливостей композицій, AVA_VAN – посилений методичний аналіз вразливостей, ADV_ARC – додатковий матеріал щодо архітектури безпеки (самозахист, розподіл доменів, неможливість обходу), ADV_INT – внутрішня структура.

Таблиця 3

Додаткові вимоги до ФПЗ НСКЗ

№ з/п	Назва послуги безпеки	NIST SP800-53	ISO/IEC 15408-1
1	Risk Assessment (Оцінка ризику)	RA-3	AVA_VAN.1 AVA_VAN.2 AVA_VAN.3 AVA_VAN.4 AVA_VAN.5 ACO_VUL.1 ACO_VUL.2 ACO_VUL.3
2	Vulnerability Scanning (Сканування вразливостей)	RA-5	
3	Security Function Isolation (Ізоляція функцій безпеки)	SC-3	ADV_ARC.1 ADV_INT.1 ADV_INT.2 ADV_INT.3

З урахуванням даних наведених в табл. 3 можна здійснити формування деталізованих (додаткових) вимог у вигляді семантики НД ТЗІ та формування вимог FPZ2 (табл. 4).

Таблиця 4

Додаткові вимоги безпеки

№ сист.	Додаткові функціональні критерії NIST	НД ТЗІ (FPZ_2)
1	RA-3	НР-3, НР-4, НР-5, НТ-3
2	RA-5	КК-2, НТ-3
3	SC-3	ЦА-4, ДВ-3, НТ-3

Також, при формуванні додаткових вимог безпеки необхідно враховувати стандартні вимоги [16, 24] викладені в табл. 5:

Таблиця 5

Стандартні ФПЗ АС класу 3

№ сист.	Стандартний ФПЗ
1	3.ЦД.3 = {КО-1, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}
2	3.КД.3 = {КД-3, КА-3, КО-1, КК-1, КВ-4, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2}
3	3.КД.3 = {КД-3, КА-3, КО-1, КК-1, КВ-4, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2}
4	3.ЦД.3 = {КО-1, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2, НА-1, НП-1}

Етап 5. Коригування базового ФПЗ, або розробка ФПЗ для нової системи галузевої ІТС FPZE.

Коригування базового ФПЗ для систем НСКЗ FPZE здійснюється з урахуванням даних викладених в табл. 4-5.

Таблиця 6

Коригування базового ФПЗ

№ сист.	Базовий ФПЗ	Додаткові функціональні критерії	Відкоригований ФПЗ
1	КД-2, КА-2, КО-1, КВ-3, ЦД-1, ЦА-2, ЦО-2, ЦВ-2, ДР-2, ДС-2, ДВ-2, ДЗ-2, НА-1, НР-2, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1, НП-1	КО-1, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НР-4, НР-5, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НТ-3, НВ-2, НА-1, НП-1	КД-2, КА-2, КО-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НА-1, НР-3, НР-4, НР-5, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НТ-3, НВ-2, НП-1
2	КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-1, ДР-2, ДС-2, ДВ-2, ДЗ-2, НР-2, НИ-2, НК-1, НО-3, НЦ-1, НТ-2, НВ-2	КД-3, КА-3, КО-1, КК-1, КК-2, КВ-4, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НТ-3, НВ-2	КД-3, КА-3, КО-1, КК-1, КК-2, КВ-4, ЦА-2, ЦВ-1, ЦД-1, ЦО-1, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НТ-3, НВ-2
3	КД-2, КА-2, КО-1, КВ-3, ЦД-1, ЦА-2, ЦО-2, ЦВ-2, ДР-2, ДС-2, ДВ-2, ДЗ-2, НА-1, НР-2, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1, НП-1	КД-3, КА-3, КО-1, КК-1, КВ-4, ДР-3, ДС-2, ДЗ-2, ДВ-2, ДВ-3, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НТ-3, НВ-2, ЦА-4	КД-3, КА-3, КО-1, КК-1, КВ-4, ЦА-4, ЦВ-2, ЦД-1, ЦО-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, ДВ-3, НА-1, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НТ-3, НВ-2, НП-1
4	КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-2, ЦВ-2, ДР-1, ДС-1, ДВ-2, ДЗ-2, НА-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НР-2, НВ-1, НП-1	КО-1, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2, НА-1, НП-1	КА-2, КВ-2, КД-2, КО-1, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1

Підсумковий відкоригований базовий ФПЗ НСКЗ можна представити у вигляді ФПЗ складових систем: КД-3, КА-3, КО-1, КК-2, КВ-4, ЦД-1, ЦА-4, ЦО-2, ЦВ-2, ДР-3, ДС-2, ДЗ-2, ДВ-3, НА-1, НР-5, НИ-2, НК-1, НО-3, НЦ-3, НТ-3, НВ-2, НП-1.

ВИСНОВКИ

Таким чином, в роботі було проаналізовано існуюче нормативно-правове забезпечення, яке використовуються для оцінки ефективності захисту систем інформаційної інфраструктури ОКІ. Встановлено, що міжнародні та регіональні нормативні документи пропонують здійснювати оцінку ефективності захисту через оцінку ризиків (чим нижчий ризик, тим вище ефективність захисту). В той же час, нормативний документ системи технічного захисту інформації України (НД ТЗІ) № 2.5-004-99 результатом оцінки визначає рейтинг, який є упорядкованим рядом (переліченням) буквено-числових комбінацій, що позначають рівні реалізованих послуг, в поєднанні з рівнем гарантій. Таким чином виникає протиріччя між підходами до оцінки ефективності захисту та обґрунтовується вибір напрямку дослідження.

Також в роботі розроблено структурно-функціональний метод формування функціонального профілю захищеності галузевої ІТС який складається з п’яти етапів. Запропонований структурно-функціональний метод визначення ФПЗ галузевої ІТС враховує сучасний світовий досвід в галузі захисту інформації та дозволяє, більш детально і об’єктивно, в порівнянні з діючим НД ТЗІ 2.5-004-99, сформулювати критерії оцінки захищеності інформації, яка циркулює в критичних ІТС. Впровадження запропонованого методу дозволяє, за рахунок визначення галузевих вимог щодо конфіденційності, цілісності, доступності та спостереженості, здійснити коригування базового функціонального профілю захищеності галузевої ІТС.

Крім того, з використанням структурно-функціонального методу формування ФПЗ галузевої ІТС було проведено експериментальне дослідження запропонованого методу. Виконано декомпозиція НСКЗ на складові системи, підсистеми та компоненти, сформульовані галузеві вимоги щодо захисту інформації, визначені додаткові вимоги у вигляді семантики НД ТЗІ, здійснено коригування базового функціонального профілю захищеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2020) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19
2 Про Стратегію кібербезпеки України, Рішення Ради національної безпеки і оборони України (2016) (Україна). https://zakon.rada.gov.ua/laws/show/n0003525-16
3 Про захист інформації в інформаційно-телекомунікаційних системах, Закон України № 80/94-ВР (2020) (Україна). https://zakon.rada.gov.ua/laws/show/80/94-вр
4 Про захист персональних даних, Закон України № 2297-VI (2020) (Україна). https://zakon.rada.gov.ua/laws/show/2297-17
5 Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України № 518 (2019) (Україна). https://zakon.rada.gov.ua/laws/show/518-2019-п
6 НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі // ДСТСЗІ СБ України. – 2005.
7 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу // ДСТСЗІ СБ України. – 1999.
8 Звіт про НДР «Дослідження та аналіз проблем захисту інформації на об’єктах критичної інфраструктури», шифр «Інфрастуктура» (д.р. № 0114U000038д).
9 Гончар, С., Леоненко, Г., & Юдін, О. (2013). Анализ угроз и уязвимостей индустриальных автоматизированных систем управлении. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, *2*(26), 9-14.
10 Леоненко, Г., & Юдин, А. (2013). Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины. (с. 44–49).

11 Про Національну систему конфіденційного зв'язку, Закон України № 2919-III (2014) (Україна). https://zakon.rada.gov.ua/laws/show/2919-14
12 Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку, Постанова Кабінету Міністрів України № 303 (2015) (Україна). https://zakon.rada.gov.ua/laws/show/303-2015-п
13 Указ Президента України від 18.04.2005 №663 «Про забезпечення урядовим зв'язком посадових осіб».
14 Наказ Адміністрації Держспецзв'язку від 18.05.2015 №07 «Про затвердження інструкції з організації технічної експлуатації мереж і комплексів державної системи урядового зв'язку України».
15 Звіт про НДР «Визначення шляхів створення спеціальної системи уніфікованих комунікацій в інтересах абонентів державних органів, установ і організацій», шифр «Платформа» (д.р. № 0116U000072T)
16 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу // ДСТСЗІ СБ України. – 1999.
17 National Institute of Standards and Technology Special Publication 800-53A. Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans. June 2010.
18 National Institute of Standards and Technology Special Publication SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations. April 2013.
19 ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
20 ISO/IEC 15408-1:2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model // The International Organization for Standardization and The International Electrotechnical Commission. – 2009.
21 НД ТЗІ 2.6-002-2015 Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 // Держспецзв'язку . – 2015.
22 НД ТЗІ 2.6-003-2015 Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99 // Держспецзв'язку . – 2015.
23 НД ТЗІ 2.7-013-2016 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99 // Держспецзв'язку . – 2016.
24 Юдин, А. (2018). Структурно-логічна та функціональна моделі визначення функціонального профілю захищеності підсистем інформаційно-телекомунікаційних систем. (с. 50-51).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023

Sergiy O. Gnatyuk
DSc, Associate Professor, Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0003-4992-0564
s.gnatyuk@nau.edu.ua,

Oleksiy Yu. Yudin
PhD, Vice-Chair of the Institute
State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine
ORCID ID: 0000-0002-4730-1463
alex@ukrdeftech.com.ua

Viktoriia M. Sydorenko
PhD, Associate Professor of IT-Security Academic Department
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

Yaroslav P. Yevchenko
PhD Student
Institute of Special Communication and Information Protection
NTU of Ukraine "Igor Sikorsky Kyiv Polytechnic University", Kyiv, Ukraine
ORCID ID: 0000-0002-2385-2658
evchenkoyaroslav29@gmail.com

METHOD FOR FORMING THE FUNCTIONAL SECURITY PROFILES OF SECTORAL INFORMATION AND TELECOMMUNICATION SYSTEMS

Abstract. Global trends to increase and improve the quality of cyber attacks have led to the actualization of the protection of information and telecommunications systems (ITS), in particular, sectoral, which are critical for the functioning of society, socio-economic development and ensuring the information component of national security. Taking into account the needs of national security and the need to introduce a systematic approach to solving problems of critical infrastructure protection, at the national level, the creation of protection systems for such infrastructure is one of the priorities in reforming the defense and security sector of Ukraine. Thus, there is a need to develop methods and models for classifying ITS as critical infrastructure to ensure the national security of Ukraine. The paper proposes a structural-functional method for determining the functional security profile of the subsystem of the sectoral ITS, which allows to determine the basic functional security profile of the sectoral ITS by determining the sectoral requirements for confidentiality, integrity, accessibility and observability and more fully formulate criteria for assessing the security of information circulating in critical ITS. The study was followed by an experimental study on the example of ITS of the National System of Confidential Communication, which tested the adequacy of the method's response to changes in input data.

Keywords: information and telecommunication systems, critical infrastructure, critical infrastructure object, cybersecurity, security assessment, functional security profile.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 On the main ambush of the cybersecurity of Ukraine, Law of Ukraine No. 2163-VIII (2020) (Ukraine). https://zakon.rada.gov.ua/laws/show/2163-19
2 About the Strategy of the Cybersecurity of Ukraine, Decision for the sake of the National Security and Defense of Ukraine (2016) (Ukraine). https://zakon.rada.gov.ua/laws/show/n0003525-16
3 On the seizure of information in information and telecommunication systems, Law of Ukraine No. 80/94-VR (2020) (Ukraine). https://zakon.rada.gov.ua/laws/show/80/94-vr

4 On the seizure of personal tributes, Law of Ukraine No. 2297-VI (2020) (Ukraine). https://zakon.rada.gov.ua/laws/show/2297-17
5 About the consolidation of Zagalnyh vimog to the cyber defense of critical infrastructure, Resolution of the Cabinet of the Ministry of Ukraine No. 518 (2019) (Ukraine). https://zakon.rada.gov.ua/laws/show/518-2019-п
6 ND TZI 3.7-003-05 The procedure for carrying out work from the establishment of a complex system and retrieval of information in the information and telecommunication systems // DSTSZI SB of Ukraine. - 2005.
7 ND TZI 2.5-004-99 Criteria for assessing the seizure of information in computer systems due to unauthorized access // DSTSZI SB of Ukraine. - 1999.
8 Sounds about NDR “Pre-Session and Analysis of Problems to Obtain Information on Critical Infrastructure Objects”, code “Infrastructure” (file number 0114U000038d).
9 Gonchar, S., Leonenko, G., & Yudin, O. (2013). Analysis of threats and vulnerabilities of industrial automated control systems. Legal, normative and metrological safety of the system and the source of information in Ukraine, 2 (26), 9-14.
10 Leonenko, G., & Yudin, A. (2013). Problems of ensuring information security of systems of critical information infrastructure of Ukraine. (pp. 44–49).
11 On the National Confidentiality System, Law of Ukraine No. 2919-III (2014) (Ukraine). https://zakon.rada.gov.ua/laws/show/2919-14
12 Nutritional arrangements for the organization of information exchange in the National Confidential System, Resolution of the Cabinet of Ministries of Ukraine No. 303 (2015) (Ukraine). https://zakon.rada.gov.ua/laws/show/303-2015-п
13 Decree of the President of Ukraine dated 04/18/2005 No. 663 "On the safety of the poor communication of the townspeople".
14 Order of the Administrative Department of State Specialized Communications dated 05/18/2015 No. 07 "On the consolidated instructions for organizing technical exploitation of the net and complexes of the state system and the level of security of Ukraine."
15 Sounds about the PDR "Designation of paths of special systems and unified communications in the interests of subscribers of state bodies, installation and organization", code "Platform"
16 ND TZI 2.5-005-99 Classification of automated systems and standard functional profiles of seized information from unauthorized access // DSTSZI SB of Ukraine. - 1999.
17 National Institute of Standards and Technology Special Publication 800-53A. Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans. June 2010.
18 National Institute of Standards and Technology Special Publication SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations. April 2013.
19 DSTU ISO / IEC 27002: 2015 Information technology. I will get it. Star of practice for entering information security.
20 ISO / IEC 15408-1: 2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model // The International Organization for Standardization and The International Electrotechnical Commission. - 2009.
21 ND TZI 2.6-002-2015 The procedure for introducing functional components without baking, in accordance with ISO / IEC 15408, with vimogs ND TZI 2.5-004-99 // Derzhspetszvyazku. - 2015.
22 ND TZI 2.6-003-2015 The order of insertion of components until they are safe, according to ISO / IEC 15408, with the help of ND TZI 2.5-004-99 // Derzhspetsvyazku - 2015.
23 ND TZI 2.7-013-2016 Methodical instructions for reporting the results of assessments to the information officer regarding unauthorized access to the statement of information to ISO / IEC 15408 statements in accordance with 2.54- TZI - 2016.
24 Yudin, A. (2018). Structurally logical and functional model of assigning the functional profile of the security of the information and telecommunication systems. (p. 50-51).