Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки

Виконав: ст. 2-го курсу, групи УБ-21м
спеціальності 125 – Кібербезпека
Освітня програма – Управління інформаційною безпекою
(шифр і назва напряму підготовки, спеціальності)

_____ Скирда А.В.
(прізвище та ініціали)

Керівник: д.т.н., професор каф. МБІС
_____ Яремчук Ю.Є.
(прізвище та ініціали)
«15» грудня 2022 р.

Опонент: к.т.н., доцент, доцент каф. ОТ
_____ Войцеховська О.В.
(прізвище та ініціали)
«15» грудня 2022 р.

Допущено до захисту
Голова секції УБ кафедри МБІС

_____ Юрій ЯРЕМЧУК
«15» грудня 2022 р.

Вінниця ВНТУ - 2022 рік

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітньо-професійна програма - Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Голова секції УБ, кафедра МБІС

_____ **Юрій ЯРЕМЧУК**
«15» вересня 2022 року

ЗАВДАННЯ
на магістерську кваліфікаційну роботу студенту

Скирда Антону Вячеславовичу
(прізвище, ім`я, по-батькові)

1. Тема роботи: «Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки»

Керівник роботи: Яремчук Юрій Євгенович, д.т.н., професор
(прізвище, ім`я, по-батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від 14.09.2022 року № 203.

2. Строк подання студентом роботи: до 10 грудня 2022 року

3. Вихідні дані до роботи: матеріали попередніх наукових досліджень студента; матеріали участі в студентських наукових конференціях та конкурсах студентських наукових робіт; матеріали та напрацювання, здійснені під час переддипломної практики, вимоги законодавства в сфері захисту інформації, технічне завдання 08-72.МКР.009.00.000.ТЗ

4. Зміст текстової частини: вступ, основна частина (розділ 1: проблеми сучасного стану кіберзахисту, розділ 2: вдосконалення моделей автентифікації, доступу та політики безпеки з нульовою довірою, практична реалізація розроблених моделей або експеримент), економічна частина, висновки, список використаних джерел, додатки.

5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень): рисунки, таблиці, презентаційний матеріал у вигляді слайдів

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основна частина	Яремчук Ю.Є., директор Центру інформаційних технологій і захисту інформації ВНТУ	15.09.22	15.09.2022
Економічна частина	Лесько О.Й., завідувач кафедри економіки підприємства і виробничого менеджменту ФМІБ ВНТУ		15.11.2022

7.Дата видачі завдання: 15 вересня 2022 року

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Отримання завдання	15.09.2022	
2.	Пошук та аналіз науково-технічної літератури, наукових публікацій, інших достовірних джерел інформації	15-20.09.2022	
3.	Збір та підготовка матеріалів під час переддипломної практики на підприємстві, ознайомлення із спеціальною та технічною документацію, експериментальні дослідження, практична реалізація обраних рішень	01-30.09.2022	
4.	Готовність основної частини	до 24.11.2022	
5.	Попередній захист на кафедрі	24-25.11.2022	
6.	Перевірка магістерської кваліфікаційної роботи на наявність ознак академічного плагіату	28-30.11.2022	
7.	Подача роботи опоненту, отримання відгуку	05-09.12.2022	
8.	Перевірка керівником, отримання відгуку	05-09.12.2022	
9.	Фінальна перевірка	до 10.12.2022	
10.	Захист	19, 21.12.2022	

Студент (підпис) **А.В.Скирда**

Керівник роботи (підпис) **Ю.Є.Яремчук**

АНОТАЦІЯ

Скирда А.В. Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки. Магістерська кваліфікаційна робота зі спеціальності 125 «Кібербезпека», освітня програма «Управління інформаційною безпекою». Вінниця: ВНТУ, 2022. 152 с.

Укр. мовою. Бібліогр.: 115 назв; рис. 34; табл.: 11.

У магістерській кваліфікаційній роботі проведено дослідження практичних та концептуальних підходів підвищення кіберзахисту сучасних інформаційно-комунікаційних систем (різної конфігурації, структури, функціонального призначення) від складних та комплексних кібератак шляхом впровадження концепції архітектури нульової довіри на основі вдосконалених моделей доступу, автентифікації, політики безпеки, що здатні забезпечити практичну реалізацію цієї концепції з урахуванням вимог чинного законодавства в сферах кіберзахисту та захисту інформації.

Ключові слова: кіберзахист, кібератака, архітектура нульової довіри, автентифікація, рольова модель доступу, політика безпеки.

ANNOTATION

Skyrda A.V. Increasing cyber defense against sophisticated and complex cyber attacks using a zero-trust architecture and based on improved access models, authentication and security policies. Master's thesis on the specialty 125 "Cyber security", educational program "Information security management". Vinnytsia: VNTU, 2022. 152 p.

Ukraine language. Bibliography: 115 titles; fig. 34; tabl.: 11.

In the master's qualification work, a study of practical and conceptual approaches to improving the cyber protection of modern information and communication systems (of various configurations, structures, functional purposes) against complex and target cyber attacks was carried out by implementing the concept of a zero-trust architecture based on improved access models, authentication, security policies, which are capable ensure the practical implementation of this concept, taking into account the requirements of current legislation in the areas of cyber protection and information protection.

Keywords: cyber defense, cyber attack, zero trust architecture, authentication, role model of access, security policy.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Технічний прогрес, стрімкий розвиток інформаційних технологій, цифрова трансформація мають й негативну складову: зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти та механізми кібератак. Зростає тенденція використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою, впливу на виборчі процеси, порушення нормального функціонування (а в деяких випадках навіть руйнування) об'єктів критичної інфраструктури. Поширення кіберзагроз на всі сфери життєдіяльності суспільства та держави в цілому, вдосконалення інструментарію реалізації кіберзагроз зумовлює необхідність перегляду стратегії та тактики протидії ним, пошук шляхів підвищення ефективності кіберзахисту від складних, комплексних та цільових кібератак. Що, в свою чергу, відповідає пріоритетам забезпечення кібербезпеки нашої держави та стратегічним цілям, визначеним Стратегією кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 № 447/2021.

Мета роботи полягає в дослідженні практичних та концептуальних підходів підвищення кіберзахисту сучасних інформаційно-комунікаційних систем (різної конфігурації, структури, функціонального призначення) від складних та комплексних кібератак шляхом впровадження концепції архітектури нульової довіри на основі вдосконалених моделей доступу, автентифікації, політики безпеки, що здатні забезпечити практичну реалізацію цієї концепції з урахуванням вимог чинного законодавства в сферах кіберзахисту та захисту інформації.

Для досягнення цієї мети в ході роботи вирішено наступні **завдання:**

- проведено пошук, збір, систематизацію та аналіз інформації для вивчення сучасного стану кіберзахисту, виявлено тенденції його розвитку, основні проблеми, виокремлено причини та фактори проблем, запропоновано можливий концептуальний варіант підвищення ефективності кіберзахисту від складних та комплексних кібератак;

- проаналізовано еволюцію шкідливого програмного забезпечення та кібератак, сценарії реалізації складних та комплексних кібератак;

- систематизовано вимоги законодавства України з кіберзахисту, виокремлено вимоги, необхідні для врахування при опрацюванні окремих завдань дослідження;

- висвітлено іноземний досвід впровадження концепції архітектури нульової довіри, виокремлено основні принципи, аспекти, складності застосування, інновації в підході до процедур автентифікації та доступу, наведено приклад достовірної практичної реалізації, оцінено можливість подібної реалізації із використанням апаратних, програмних засобів вітчизняного виробництва та з урахуванням вимог чинного законодавства;

- побудовано формалізовані моделі обраного рішення організації процедур автентифікації, доступу та політики безпеки доступу користувачів до ресурсів, реалізованих на принципах нульової довіри, здійснено їх аналіз, запропоновано варіант вдосконалення;

- проведено пошук програмних та апаратних засобів вітчизняного виробництва для практичної реалізації процедур автентифікації, доступу та політики безпеки доступу;

- здійснено практичне впровадження вдосконалених моделей автентифікації, доступу та політики безпеки доступу в реальній інфраструктурі (інформаційно-комунікаційній системах), проаналізовано отримані результати;

- проведено економічний розрахунок запропонованих рішень, проведено порівняння конкурентних варіантів, оцінено економічну ефективність.

Об’єктом дослідження є кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Предметом дослідження є підвищення кіберзахисту з використанням архітектури нульової довіри на основі вдосконалених моделей доступу, автентифікації та політики безпеки.

Методи дослідження. Для реалізації визначеної мети та вирішення поставлених завдань використано комплекс взаємодоповнюючих загальнонаукових та спеціальних методів дослідження та аналізу, зокрема: системний аналіз та синтез (у всіх розділах роботи), методи інформаційно-аналітичного дослідження (розділ 1), моделювання (підрозділи 2.2-2.4), методи вивчення аналога (прототипу) та метод еталонного оцінювання (підрозділи 2.1, 3.1), експеримент (підрозділ 3.3), метод аналізу ієрархій та метод побудови рольового дерева розмежування доступу, методика теоретико-графового представлення (підрозділ 2.4), методи визначення та оцінки економічної ефективності (розділ 4).

Новизна одержаних результатів полягає в тому, що:

- вперше запропоновано, досліджено та доведено можливість застосування концепції архітектури нульової довіри для підвищення ефективності кіберзахисту об’єктів критичної інфраструктури, захисту державних інформаційних ресурсів та інформаційно-комунікаційних систем, з урахуванням вимог та обмежень, регламентованих законодавчими та нормативно-правовими актами в цих сферах;

- вперше здійснено технічний переклад NIST 1800-35B (дата публікації: липень 2022 року) та його аналіз, на основі якого висвітлено невідомі до цього достовірні приклади практичної реалізації інновацій архітектури нульової довіри, що дозволяє: 1) більш глибоке розуміння концепції архітектури нульової довіри, абстрактний опис принципів якої зазначений в NIST 800-207 (дата публікації: серпень 2020 року); 2) стимулює подальші дослідження парадигми архітектури нульової довіри, як найбільш перспективного варіанту вирішення проблем кіберзахисту; 3) надає можливість практичного використання: як наведених в NIST 1800-35B програмних продуктів для реалізації архітектури нульової довіри, так й вітчизняних аналогів, що в свою чергу: 4) дозволяє знизити капітальні витрати на придбання та утримання засобів кіберзахисту;

- вперше використано положення стандарту IAS 38 «Нематеріальні активи» для демонстрації економічної ефективності впровадження конкурентних між собою програмних засобів захисту, що надає можливість оптимальних витрат бюджетних коштів та уникнення проблем з фінансуванням щорічного утримання програмних продуктів.

- дістало подальшого розвитку використання напрацювань та запропонованих раніше методик в процесах створення та дослідження формалізованих моделей;

- дістала подальшого розвитку раніше запропонована ідея поєднання двох відомих методів (аналізу ієрархій та побудови рольового дерева розмежування доступу) при моделюванні на основі теоретико-графового представлення ієрархії ролей, що розширює можливості вдосконалення практичних рольових моделей доступу.

Практичне значення одержаних результатів, ступінь їх готовності до практичної реалізації, полягають в тому, що:

- продемонстровано можливість застосування програмних та апаратних засобів вітчизняного виробництва, які відповідають обов’язковим вимогам законодавства та нормативно-правових актів в сфері технічного та криптографічного захисту інформації, для практичного впровадження концепції архітектури нульової довіри.

- доведено, що реалізовані рішення здатні підвищити ефективність захисту реальних інформаційних та кіберфізичних систем різного призначення та архітектури від складних, цільових та комплексних кібератак, описаних в підрозділі 1.2 даної роботи, та, відповідно, вирішувати проблеми сучасного стану кіберзахисту.

Результати дослідження, висновки та практичні рекомендації використано:

- департаментом інформаційних технологій Вінницької міської ради практичною реалізацією вдосконалених моделей на кількох реальних інформаційно-комунікаційних системах, об’єднаних ERP-системою «IT-Enterprise» та в реальній локалізованій системі SAP R/3, шляхом відповідних

налаштувань програмного комплексу захисту «ІІТ Захист SAP-системи» (довідка від 01.11.2022 № 13/00/019/163804);

- комунальним підприємством «Вінницькартсервіс» в автоматизованій системі обліку оплати проїзду в громадському транспорті та системі автоматичного визначення місцезнаходження транспорту (довідка від 26.10.2022 № 105/1);

- комунальним підприємством «Вінницький інформаційний центр» в системі відеоспостереження «Безпечне місто» (довідка від 27.10.2022 № 194/2/15).

Довідки про впровадження приведені в додатку А даної роботи.

Особистий внесок здобувача: основні результати, наведені у магістерській кваліфікаційній роботі, отримані самостійно. Практична реалізація вдосконалених моделей проведена за допомогою та під наглядом спеціалістів департаменту інформаційних технологій Вінницької міської ради.

Апробація результатів роботи: окремі результати досліджень [24, 103], використані в роботі, оприлюднені на Всеукраїнській науково-практичній інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2022)» (м. Вінниця, 16 – 17 червня 2022 року).

Публікації, які додатково відображають наукові результати роботи, опубліковані в матеріалах Всеукраїнській науково-практичній інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2022)» [24, 103].

Структура та обсяг роботи. Магістерська кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Повний обсяг становить 152 сторінки, з них 104 сторінки основного тексту. Робота містить 11 таблиць, 34 рисунка, 5 додатків. Список використаних джерел налічує 115 найменувань.

РОЗДІЛ 1
ПРОБЛЕМИ СУЧАСНОГО СТАНУ КІБЕРЗАХИСТУ

1.1 Основні проблеми ефективності кіберзахисту

Ще в період 2012-2013 років у різних засобах масової інформації з’явилася серія публікацій, присвячених проблемному процесу в сфері комп'ютерної та інформаційної безпеки. Так The New York Times, в статті [1] привела висновки відомого професіонала з комп’ютерної безпеки Петера Нойманна, що «складні системи зламуються складними способами», маючи на увазі, що зростаюча складність сучасного обладнання та програмного забезпечення робить фактично неможливим виявлення недоліків та вразливостей в комп’ютерних системах, а тому «достовірно невідомо, що вони безпечні та надійні» та що «потрібно починати з чистого аркушу». Потім, на сайті наукового журналу IEEE Spectrum, з’явилася публікація Роберта Вотсона [2], а в галузевому журналі Communications of the ACM його оглядово-аналітична стаття [3], присвячені осмисленню значних проблем кібербезпеки та констатації факту появи «системного глухого кута» в галузі захисту інформації. В статтях приведені обґрунтовані доводи, що сучасний стан кіберзахисту можна описати терміном «перегони озброєнь»: ці «перегони» відбувається між людьми, що створюють механізми безпеки IT-систем, та людьми, які атакують ці системи на щоденній основі, між фахівцями, які розробляють та підтримують системи антивірусного захисту, та людьми, які створюють нове шкідливе програмне забезпечення. Особливістю цього процесу стало те, що кібербезпека постфактум «сторона, що обороняється», та перебуває в більш невигідній позиції, ніж «сторона, що атакує».

Ілюстрацією цього системного глухого кута, та відповідно, проблемами сучасного стану кіберзахисту є:

Проблема 1. Зростаюча динаміка кількості та видів шкідливого програмного забезпечення.

Проблема 2. Поява у вільному доступі «конструкторів вірусів».

Проблема 3. Низька ефективність антивірусних засобів та сумнівні перспективи їх розвитку.

Проблема 4. Наявність вразливостей «нульового дня» (від англ. *zero day, 0-day*), «люків» (від англ. *trapdoor*), незадокументованих «входів» (англ. *back door*) в системному та прикладному програмному забезпеченні.

Проблема 5. Відсутність національної системи верифікації іноземного програмного забезпечення на відсутність алгоритмічних закладок.

Проблема 6. Процедура оновлення (update) та отримання оновлень програмного забезпечення здійснюються через мережу Інтернет.

Проблема 7. Поява нових методів та способів зламу чи обходу криптографічного захисту інформації.

Проблема 8. Складність структури та технологій сучасних інформаційно-комунікаційних систем внаслідок розвитку інформаційних технологій, їх вразливість перед кіберзагрозами. Відсутність дієвого захисту після подолання порушником периметру безпеки.

Проблема 9. Суттєва зміна тактики, сценаріїв, складності та інструментів проведення кібератак, у тому числі як наслідок проблем 1-8.

Для виявлення причин та факторів розглянемо ці проблеми більш детально.

В ході дослідження не вдалося з’ясувати достовірну кількість існуючих видів та модифікацій шкідливого програмного забезпечення, проте зростаючу динаміку їх появи можна опосередковано (проте з достатньою об’єктивністю) оцінити за зростанням кількості записів в базі даних сигнатур вірусів (рис. 1.1):

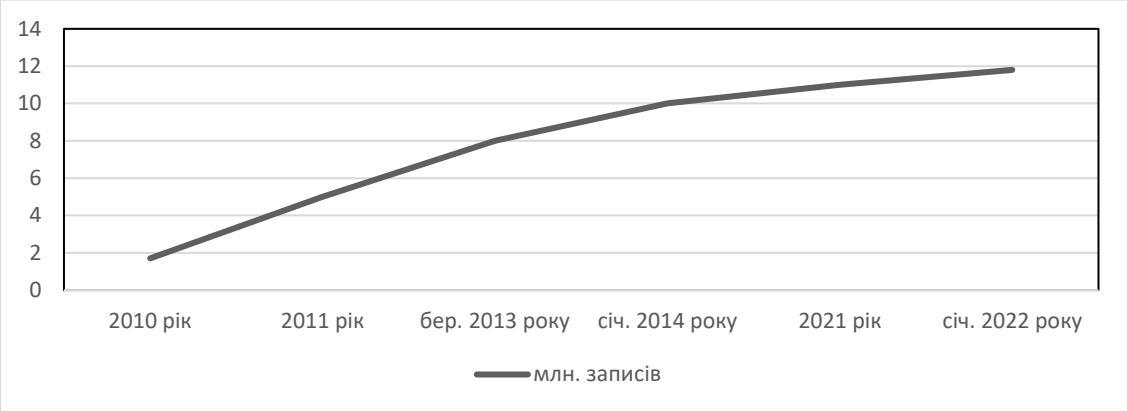


Рисунок 1.1 – Зростання кількості записів вірусних сигнатур в продуктах Zillya!

Незалежна австрійська організація AV-Comparatives, яка спеціалізується на тестуванні антивірусних рішень, періодично публікує результати випробувань корпоративних та споживчих засобів інтернет-безпеки на предмет забезпечення захисту від складних та цільових атак. В останніх випробуваннях [4] протестовані кілька засобів захисту кінцевих пристроїв: Acronis Cyber Protect Cloud with Advanced Security Pack, Avast Business Antivirus Pro Plus, Bitdefender Gravity Zone Elite, CrowdStrike Falcon Pro, Eset Protect Entry with Eset Protect Cloud, G Data Endpoint Protection Business, Kaspersky Endpoint Security for Business - Select with KSC, Vipre Endpoint Cloud. Cloud. У тестах AV-Comparatives використовуються різні сценарії атак, від яких повинен здійснюватися захист програмами, що випробуються. У цільових атаках застосовуються методи, що дозволяють уникнути виявлення захисними програмними засобами. До них відносяться безфайлові атаки, заплутування коду та використання легальних засобів операційної системи. Маскування шкідливого коду також ускладнює розпізнавання захисною програмою. Зловживання легальними системними програмами у шкідливих цілях також полегшує кіберзлочинцям завдання триматися поза зоною досяжності засобів захисту. У всіх випробуваннях використовується т. зв. підмножина ТТП (тактика, технології, процедури), що фігурує в інформаційній базі даних MITRE ATT&CK. У звіт також включено результати тесту на хибне спрацювання. Умовою тестування антивірусних засобів (як споживчого сегменту, так й корпоративного) було забезпечення захисту від 15 різних таргетованих атак. За результатами тестування, всі перелічені програмні засоби заблокували щонайбільше вісім (!) із п'ятнадцяти таргетованих атак.

В наукових працях [5-8] досліджено причини низької ефективності антивірусних продуктів та сумнівні перспективи їх розвитку. За висновками фахівців, виробники антивірусного програмного забезпечення уникають висвітлювати принципи функціонування своїх продуктів з ряду причин. По-перше, розкриття механізмів роботи може бути використане для створення нових різновидів шкідливих програм, які будуть містити засоби обходу цих механізмів. По-друге, маркетингова політика потребує додання антивірусному продукту

іміджу «закритий, проте більш ефективний за інших аналогічних продуктів», тобто постулат, закладений в основу закритого програмного коду «як саме працює програма - користувачу знати не обов’язково, вона сама все зробить», найбільш повно розкривається як раз в антивірусній індустрії [5]. Проте, основні принципи роботи антивірусних засобів відносно відомі, це: сигнатурний аналіз, евристичний аналіз, емуляція виконання коду, постійний моніторинг операцій.

Сигнатурний аналіз. Самий примітивний вид пошуку вірусів за відомими послідовностями коду – сигнатурами. Суть роботи сигнатурного сканера полягає в пошуку у файлах, пам'яті та завантажувальних секторах вірусних масок (сигнатур) – унікального програмного коду вірусу. Сигнатури відомих вірусів містяться в антивірусній базі даних, та якщо сканер зустрічає програмний код, що збігається з одним із цих описів, то він видає повідомлення про виявлення відповідного вірусу. На сьогодні його ефективність під сумнівом [5, 6]. Головним недоліком сигнатурного аналізу можна назвати розмір антивірусних баз, які сканерам доводиться весь час поповнювати та оновлювати, оскільки найменші модифікації вірусу роблять його «невидимим» для сканера. Недолік настільки критичний, що в середовищі фахівців постійно виникають підозри про навмисне зниження виробниками кількості записів в базах даних сигнатур вірусів антивірусних продуктів, тому що їх обсяг перевищує обсяг дискового простору, який займає системне та прикладне програмне забезпечення. В принципі, це наглядно можна побачити на рисунку 1.1: в продовж періоду 2010-2014 років (а це період активного просування продукту на ринку) база сигнатур зросла з 1,7 млн. записів в 2010 році до 5 млн. записів в 2011 році, до 8 млн. записів в 2013 році, до 10 млн. записів в 2014 році, в подальшому наводилися цифри «близько 11 млн.» та «близько 12 млн.», при ствердженні у релізах на своєму офіційному сайті, що щоденно вірусна база поповнюється на 10-50 тисяч записів, а станом на 01.03.2013 року вірусна колекція Zillya! займає більш ніж 12 ТБ. Іншим проблемним аспектом використання сигнатурного аналізу є так звані поліморфні віруси, тобто віруси, які не мають постійного програмного коду: при зараженні чергового файлу, вони за

допомогою шифрування самостійно змінюють свій вигляд, зберігаючи при цьому свою функціональність.

Евристичний аналіз. Основний вид проактивного захисту в ході якого аналізують код виконуваних файлів, макросів, скриптів, пам'яті або завантажувальних секторів для виявлення в ньому різних типів шкідливих комп'ютерних програм, що не визначаються звичайними (сигнатурними) методами. Цей метод дозволяє пошук невідомого шкідливого програмного забезпечення. Технологія може бути використана в усіх антивірусних продуктах, як на робочих станціях, так й на файлових, поштових серверах та Internet-шлюзах. Зазвичай евристичні аналізатори розташовуються на периметрі мережі - між внутрішніми мережами та Internet та відстежують мережевий трафік на наявність ознак атак. Усередині мережі евристичні аналізатори відстежують поведінку програмних кодів на комп'ютерах користувачів та блокують будь-які програми, дії яких визначаються ними як шкідливі або підозрілі. Проте, рівень детектування евристичних аналізаторів на сьогоднішній день не дуже високий, тому що існують десятки різних методів «введення їх в оману», якими користуються автори вірусів [6, 7]. Крім цього, для евристичних аналізаторів з високим рівнем виявлення характерний високий рівень хибних спрацьовувань.

Емуляція виконання коду. Вважається прогресивним методом. Підозрілий код запускається у рамках віртуальної машини, в ізольованих зонах. Після цього віртуальна машина зупиняється для аналізу стану щодо ознак зараження. Досить прогресивний метод, проте існують антиналагоджувальні прийоми (вони ж використовуються при розробці систем захисту програмного забезпечення), які визначають справжнє середовище виконання та блокують виконання шкідливого коду на віртуальних машинах. Крім того, логіка шкідливого програмного коду може припускати часові умови його виконання (наприклад, першого числа кожного місяця), або вибором (по генератору випадкових чисел). У цьому випадку емуляція безглузда, тому що аналізатор не знає всіх умов та особливостей роботи вірусу [6].

Постійний моніторинг операцій. Вважається найбільш прогресивним методом, який теоретично дозволяє уникнути більшості загроз, які можуть бути спричинені комп'ютерними вірусами. На практиці реалізується в наступний спосіб. Наприклад, деяка програма намагається встановити з'єднання мережного протоколу. Користувачеві на екран видається повідомлення про це, після чого він може або дозволити цю дію, або заборонити та відправити цю програму для аналізу в антивірусну лабораторію. Те саме стосується операцій з системними файлами, а також специфічними ключами реєстру Windows або конфігураційними файлами Unix. Недоліком цього підходу є суттєве уповільнення роботи комп'ютерів користувачів (при моніторингу файлової системи в реальному часі ресурси на 70% використовуються системою безпеки). До того ж, користувачі можуть не мати достатньої кваліфікації для самостійної оцінки ступеня небезпеки та дозволяти будь-які дії, нівелюючи цим функції антивірусного продукту.

Щодо перспектив розвитку антивірусного захисту. Безумовно, провідними компаніями індустрії антивірусного захисту, науковцями та ентузіастами проводяться дослідження в цій галузі, кожен рік анонсуються десятки різних проектів, направлених на розробку нових технологій та принципів антивірусного захисту та аналізу із використанням штучного інтелекту та машинного навчання, нейронних мереж, розробки штучних імунних систем для IoT-пристроїв тощо. В серпні 2022 року компанія Microsoft на своєму офіційному сайті оприлюднила новину, що вони мають великий обсяг даних про сучасне шкідливе програмне забезпечення, шкідливі коди та атаки на системи, які отримуються від різних пристроїв, платформ, поштових серверів та мобільних застосувань. Зважаючи на те, що кількість таких сигналів щодня складає понад 43 мільярди, для їх збору, узагальнення, класифікації та аналізу використовується штучний інтелект. Згідно зі статистикою [11], 93% ситуаційних центрів інформаційної безпеки використовують інструменти штучного інтелекту та машинного навчання для виявлення загроз. Зрозуміло, що використання таких технологій потребує значних обчислювальних ресурсів, тому застосування таких прогресивних методів для захисту кінцевих пристроїв користувачів в найближчий час є сумнівним. За

даними досліджень [9, 10] самі технології штучного інтелекту, машинного навчання, нейронних мереж занадто вразливі внаслідок технологічних особливостей та є привабливою ціллю зловмисників.

Суттєвою проблемою стала поява у вільному доступі так званих «конструкторів вірусів», за допомогою яких будь-який бажаючий може модифікувати відомий вірус, спотворюючи його сигнатуру таким чином, щоб вона відрізнялася від запису в сигнатурної базі будь-якого антивірусу. Функціональні можливості таких конструкторів дозволяють: перестановку незначних ділянок коду із збереженням функціоналу, додавання довільного коду, стискання, шифрування (рис. 1.2). Розробники шкідливого програмного забезпечення навіть реалізували розміщення конструктору вірусу на його власному тілі. Такий різновид зараз називають поліморфним генератором.

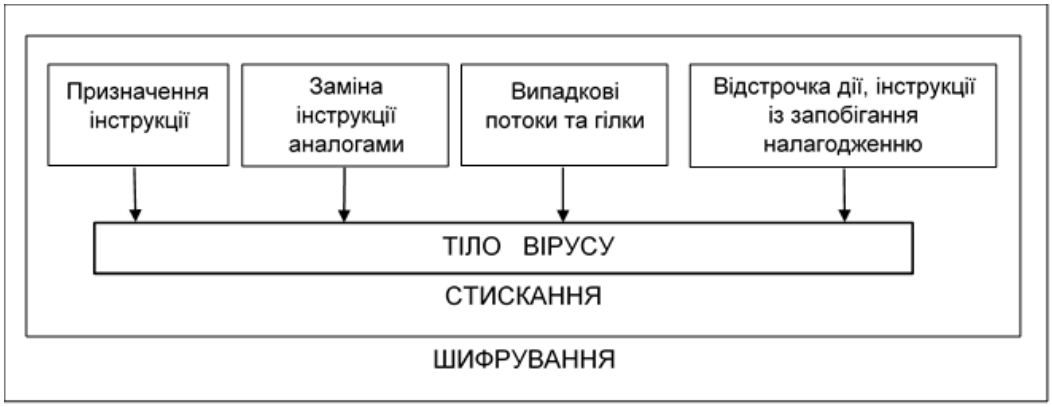


Рисунок 1.2 – Технології конструктора вірусів

Джерело: [6]

Головною проблемою кіберзахисту залишається наявність вразливостей «нульового дня», «люків», незадокументованих «входів» в системному, прикладному програмному забезпеченні та навіть апаратному забезпеченні із вбудованими функціями безпечного завантаження. Майже 600 сторінок інформаційно-аналітичних дайджестів [4, 11, 12] висвітлюють виявлені в 2021 - 2022 роках вразливості технічних засобів та програмного забезпечення. Незважаючи навіть на використання закритого коду розробниками програмного забезпечення, існують процедури для виявлення вразливостей та недокументованих можливостей (наприклад, дизасемблювання програмного коду,

зворотна розробка коду, пошук некоректних параметрів команд, використання Fuzz-тестування тощо). Ця проблема настільки масштабна, що навіть в указі Президента Сполучених Штатів Америки про підвищення національної кібербезпеки від 12 травня 2021 року [13], це питання фігурує в більшості розділів та завдань. Зокрема, в указі визначається, що «розробці комерційного програмного забезпечення часто не вистачає прозорості, достатньої уваги до здатності програмного забезпечення протистояти атакам та належного контролю для запобігання втручанню зловмисників», що «існує нагальна потреба впровадити більш суворі та передбачувані механізми для забезпечення безпечного та належного функціонування продуктів», «безпека та цілісність «критичного програмного забезпечення» - програмного забезпечення, яке виконує критично важливі для довіри функції (наприклад, надання або вимагання підвищених системних привілеїв або прямого доступу до мережевих і обчислювальних ресурсів), викликає особливе занепокоєння». Указом профільним відомствам та установам ставляться завдання: «розробити нові стандарти, інноваційні інструменти, найкращі практики та критерії, які можна використовувати для оцінки безпеки програмного забезпечення, «розробити та опублікувати визначення термінів «важливе та безпечне програмне забезпечення», опублікувати рекомендації щодо мінімальних стандартів для тестування постачальниками свого вихідного коду програмного забезпечення, включаючи визначення рекомендованих типів ручного або автоматизованого тестування (таких як інструменти перегляду коду, статичний і динамічний аналіз, інструменти компонування програмного забезпечення та тестування на проникнення), стимулювати розробку безпечного програмного забезпечення».

В дослідженнях [14-16] окремою проблемою кіберзахисту зазначається наявність програмних та алгоритмічних закладок в програмному забезпечені, та, як наслідок, кіберзагрози, пов’язані з використанням іноземного програмного забезпечення. Будь-який комерційний продукт може бути використаний в якості кіберзброї, шляхом впровадження в нього програмних та алгоритмічних закладок на етапах його розробки та логістичних ланцюжків постачання [16].

Таким чином, можна виокремити три основних фактори:

Фактор 1. Еволюція кібератак. Прогрес у створенні шкідливого програмного забезпечення значно випереджає розвиток антивірусного захисту. Також розвиваються самі техніки виконання атак: тепер ціль вибирається не випадково, а цілеспрямовано, з використанням різних векторів. Кіберзлочинність стала привабливим та вигідним бізнесом. Зловмисники використовують значні економічні ресурси, що дозволяє проводити більш складні атаки. Як результат, зростаюча масштабність, багатовекторність кібератак, колосальні збитки.

Фактор 2. Цифрова трансформація. Розвиток інформаційних технологій змінює структуру, складність, масштабність інформаційно-комунікаційних систем, впроваджуються хмарні технології, IoT, тощо. На законодавчому рівні введено поняття «кіберпростору» [12], внаслідок того, що навіть об’єкти критичної інформаційної інфраструктури ускладнено будувати в концепції локалізованих або ізольованих кіберфізичних систем. Як наслідок, периметр захисту змістився до середовища користувача та кінцевих пристроїв IT-системи. Складність IT-систем підвищує їх вразливість перед кіберзагрозами.

Фактор 3. Необхідність зміни парадигми кіберзахисту. Провідні розробники програмних та апаратних засобів кібербезпеки, постачальники послуг безпеки все частіше позиціонують свої нові продукти, як рішення захисту «наступного покоління». Тобто, традиційні підходи до захисту не здатні забезпечити ефективність захисту, швидко морально та фізично застарівають. Тому є об’єктивне пояснення. У звіті IDG Research (DARK Reading) «State of Enterprise Secure Access» за 2019 рік зазначено, що 18% нових шкідливих програм залишаються непоміченими протягом перших 24 годин, а 2% загроз можуть залишатися непоміченими навіть протягом 3 місяців після зараження. За даними Verizon Data Breach Investigations Report, у 99% зразків шкідливого коду життєвий цикл складає не більше 58 секунд. Фактично, більшість шкідливих програм спостерігаються лише один раз. Це показує, наскільки швидко хакери для уникання виявлення модифікують упаковку свого коду, щоб сигнатура нового зразка була відмінною від попередньої версії.

1.2 Аналіз сценаріїв реалізації складних та комплексних кібератак

Згідно законодавчо визначеної термінології [17] кібератака - це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту.

Відомим українським дослідником з питань кібербезпеки професором В.Л.Бурячком сформульоване власне визначення поняття «кібератака» - сукупність узгоджених щодо мети, змісту й часу дій або заходів, так званих кіберакцій, спрямованих на певний об’єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи ІТ-систем і мереж зазначеного об’єкта [18]. Обидва визначення надають змогу зрозуміти, що кібератаки можуть бути таргетованими, тобто спрямованими проти конкретної цілі з приховуванням слідів активності на всіх її етапах, складними та різними чинниками (наприклад, в часі), комплексними (поєднувати різні методи та способи, наприклад, використовувати методи соціальної інженерії у поєднанні із використанням шкідливого програмного забезпечення). Таргетована (цільова) кібератака (від англ. *target*) є безперервним тривалим процесом несанкціонованої активності кіберзлочинності в умовах конкретного об’єкта критичної інфраструктури, покликаним здолати конкретні механізми забезпечення безпеки та завдати конкретного збитку (фізичного, інформаційного, морального тощо). Інструментарієм цільових кібератак є засоби

APT (від англ. *Advanced Persistent Threat*, вдосконалена постійна загроза): комбінація спеціальних утиліт віддаленого доступу, шкідливого програмного забезпечення, механізмів використання вразливостей «нульового дня», а також інших компонентів, спеціально розроблених для реалізації конкретної атаки та досягнення конкретної мети [19-23]. Їх використання в якості кіберзброї має масштабні та руйнівні наслідки, в тому числі й для кіберпростору та об'єктів критичної інфраструктури України [24].

До першого відомого застосування цільової комплексної атаки відносять кіберінцидент з використанням шкідливого програмного забезпечення Win32/Stuxnet. Унікальність цього кіберінциденту полягає в тому, що вперше в історії, наслідком кібератаки на ізольовану локальну мережу, обладнану сучасними засобами безпеки, стало фізичне руйнування критичної інфраструктури. Сценарій кібератаки здійснювався в декілька етапів із взаємоузгодженими діями (у тому числі, із використанням методів соціальної інженерії): із зараження облікованого флеш-накопичувача вірусом, впровадження шкідливого коду в обладнання робочих станцій SCADA-системи Simatic WinCC компанії Siemens, використання вразливостей програмованих логічних контролерів марки Simatic S7, використання чотирьох невідомих на той час та трьох відомих вразливостей «нульового дня» операційної системи Microsoft Windows. Для нейтралізації антивірусних програм були використані справжні цифрові підписи (два дійсні сертифікати, випущені компаніями Realtek та JMicron). Схема кібератаки представлена на рисунку 1.3:

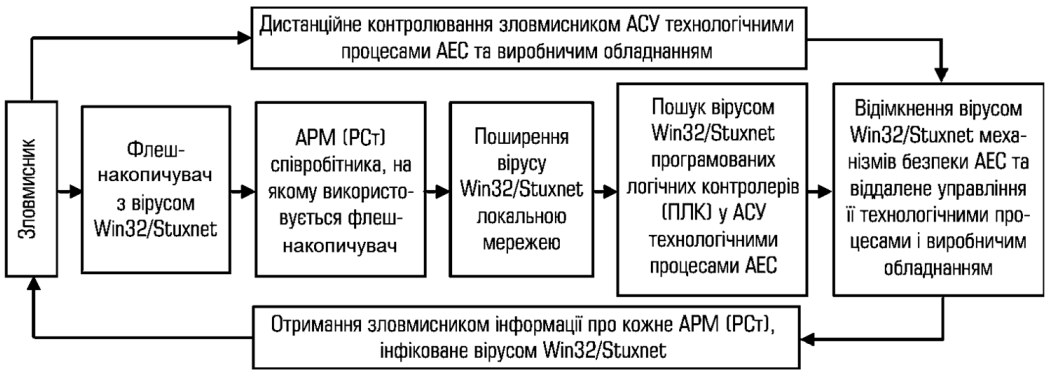


Рисунок 1.3 – Схема кібератаки із використанням вірусу Win32/Stuxnet

Джерело: [21]

Для організації захисту від цільових кібератак APT та їх аналізу, компанією Lockheed Martin’s розроблена модель СКС (англ. *Cyber Kill Chain*) та її розширені версії [25]. Модель СКС - це схематичний опис послідовності дій (етапів) порушника у вигляді взаємопов’язаних ланок ланцюга кібервторгнення. Базова версія моделі СКС включає в себе (припускає) сім етапів, що необхідні для успішної реалізації цільової кібератаки (рис. 1.4):

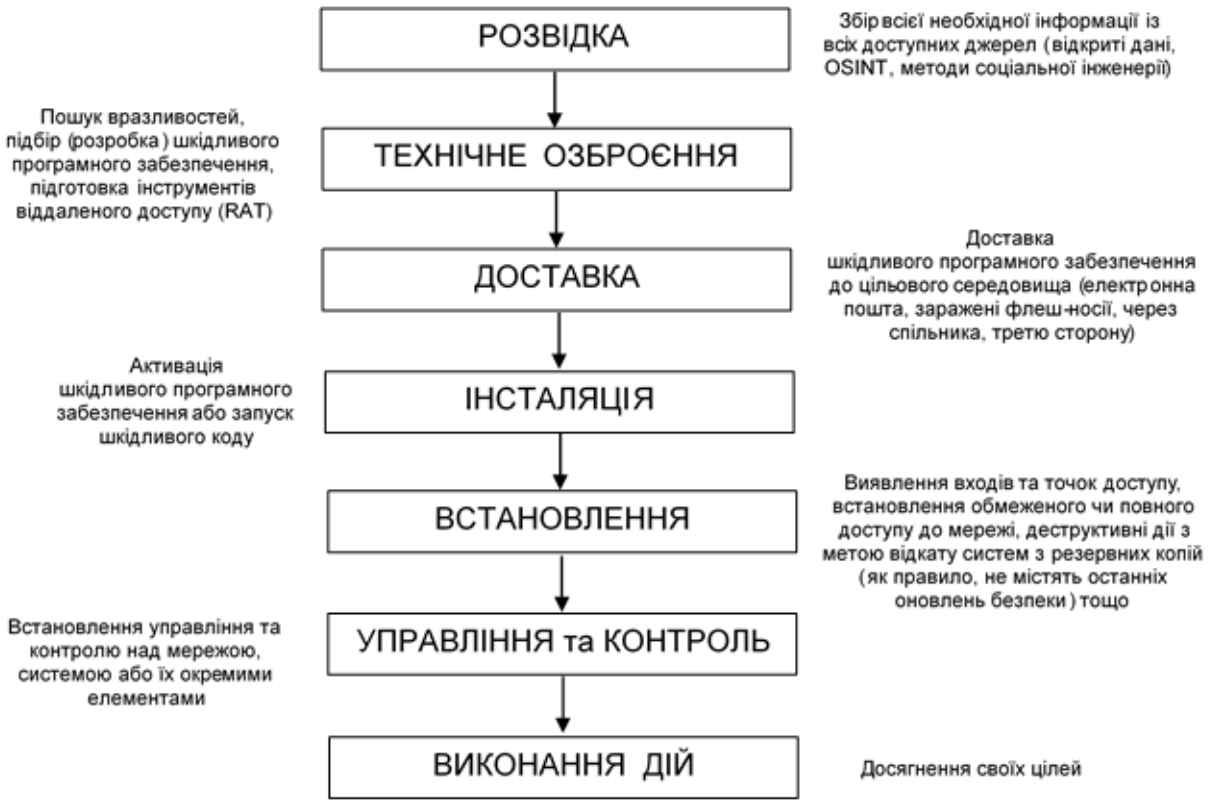


Рисунок 1.4 – Модель Cyber Kill Chain

Джерело: [25], технічний переклад автора

Базова модель неодноразово піддавалася модернізації [27, 28] для застосування в різних областях, у тому числі для кіберфізичних систем [29]. Базова модель СКС ураховує ризики тільки зовнішніх загроз. Таким чином, ця модель не охоплює інші вектори атак, що відбуваються всередині захищеного периметру цільового об'єкта. З урахуванням постійно зростаючого різноманіття векторів атак та розвитку інструментарію порушника, число етапів було збільшено до вісімнадцяти [30]. Така модель отримала назву UCK (від англ. *Unified Kill Chain*) та ураховує як зовнішні так й внутрішні загрози (рис. 1.5):

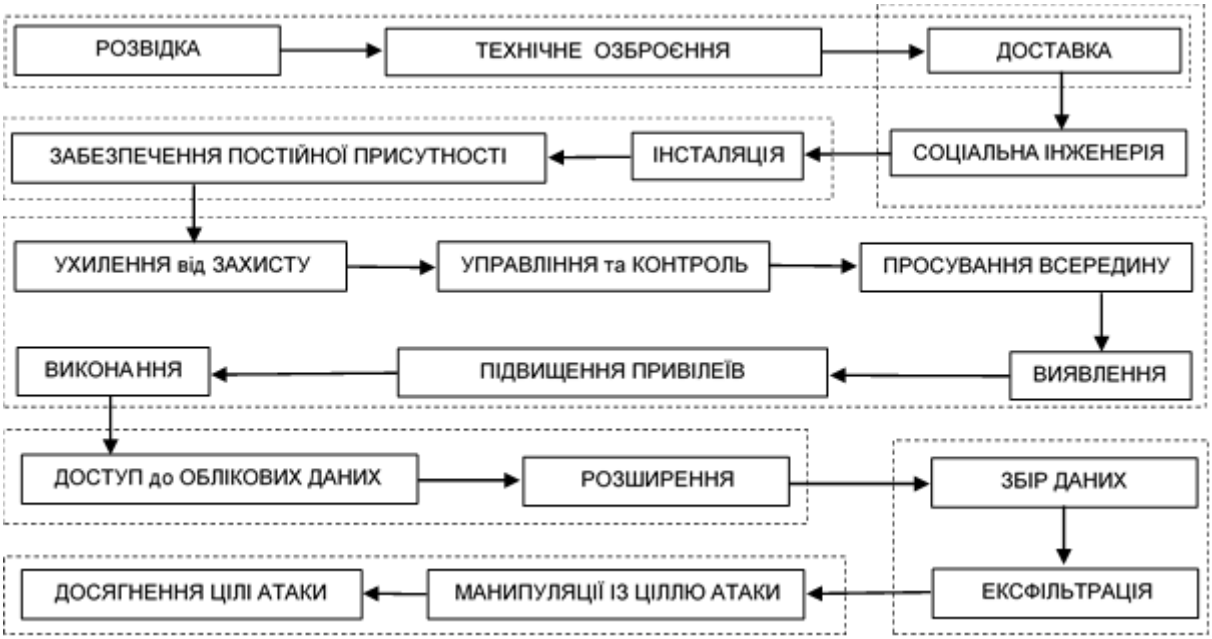


Рисунок 1.5 – Модель Unified Kill Chain

Джерело: [30], технічний переклад автора

Розглянемо етапи, представлені в моделі UCK:

Етап 1. Розвідка (Reconnaissance). На цьому етапі, здійснюється збір інформації про об’єкт, що атакується. Встановлюється організаційна структура, застосовувані інформаційні технології, засоби захисту (зловмисники намагаються ідентифікувати та дослідити існуючі міжмережні екрани, системи запобігання вторгненням, механізми аутентифікації та інше). Для виявлення «вузьких» місць та визначення найменш захищених елементів (служб, сервісів) в інформаційно-комунікаційної інфраструктури потенційної жертви аналізуються технологічними процесами. У випадку з об'єктами критичної інформаційної структури проводиться можлива оцінка шкоди національним та стратегічним інтересам держави. Отримана інформація виступає у ролі бази даних та знань при виконанні наступного етапу.

Етап 2. Технічне озброєння (Weaponization). Виконуються підготовчі заходи, спрямовані на створення інфраструктури, яка потрібна для здійснення атаки. Використовується існуюче або розробляється власне унікальне шкідливе програмне забезпечення, у тому числі шкідливий код, який використовує помилки або недоліки системи безпеки, шифрувальники (ransomware) тощо.

Етап 3. Доставка (Delivery). Активна фаза атаки, головне завдання якої впровадження та поширення розробленого шкідливого рішення у цільовому середовище.

Етап 4. Соціальна інженерія (Social Engineering). Застосовуються методи, створені задля маніпулювання персоналом (користувачами) з метою здійснення необхідних зловмиснику (небезпечних) дій.

Етап 5. Інсталяція (Exploitation). Активація шкідливого рішення на скомпрометованому цільовому об'єкті. На етапі експлуатації зловмисники шукають додаткові вразливості чи слабкі місця, які вони можуть використовувати у системах організації. Наприклад, ззовні зловмисник може не мати доступу до баз даних, але після вторгнення він може побачити, що база даних використовує неоновлену версію програмного забезпечення та має відомої вразливості.

Етап 6. Забезпечення постійної присутності (Persistence). Здійснюється будь-який доступ, дія або зміна в довіреному середовищі з метою забезпечення тривалої (постійної) присутності зловмисника у цільовій системі.

Етап 7. Ухилення захисту (Defense Evasion). Застосовуються методи та засоби для обходу засобів захисту та приховування присутності у цільовій системі.

Етап 8. Управління та контроль (Command and Control). Здійснюється адміністрування розробленого рішення, його оновлення, отримання нового функціоналу, реалізація повного спектру команд для досягнення поставленої мети.

Етап 9. Просування всередину (Pivoting). Зловмисники встановлюють доступ через контрольовану систему до інших систем, до яких до цього моменту не мали прямого доступу.

Етап 10. Виявлення (Discovery). Застосовуються методи та засоби, що дозволяють зловмиснику орієнтуватися в системі-жертві для подальших дій, отримувати інформацію про цільову систему, інформаційне та обчислювальне середовище, мережеве оточення та нові можливості.

Етап 11. Підвищення привілеїв (Privilege Escalation). Реалізуються методи та засоби, які дають можливість зловмиснику отримати більше широкі права

цільової системі. Мета порушника ‑ отримати привілеї для доступу в інші сегменти системи або облікових записів. Здійснюються атаки методом «грубої сили», пошук незахищених сховищ облікових даних, здійснюється стеження за мережевим трафіком, що не шифрується тощо.

Етап 12. Виконання (Execution). Застосовуються методи та засоби, що дозволяють виконувати шкідливий код у локальній або віддаленій системі.

Етап 13. Доступ до облікових даних (Credential Access). Використовуються методи та засоби, які забезпечують доступ або контроль над обліковими даними системи, служби чи домену.

Етап 14. Розширення (Lateral Movement). Також поширені терміни: «рух у бік» та «горизонтальне просування». Використовуються методики отримання порушниками доступу до інших віддалених систем, підключених до скомпрометованого цільового середовища для управління або деструктивного впливу, пошуку конфіденційної інформації або доступу до критично важливих активів. При розширенні зловмисник часто використовує вразливість «нульового дня» або конфіденційні дані з віддалених систем без застосування спеціалізованого інструментарію.

Етап 15. Збір даних (Collection). Здійснюються ідентифікація об’єктів інтересу та збирання необхідних конфіденційних даних з цільової мережі.

Етап 16. Ексфільтрація (Exfiltration). Використовуються методи та засоби прихованого вивантаження даних за межі цільового середовища з метою крадіжки конфіденційних даних або видаленню даних із цільової мережі (спроби приховати сліди несанкціонованої діяльності). Ексфільтрація може включати такі методи, як обфускація (наприклад, за допомогою фальсифікації часових міток, видалення або зміни журналів подій та спостереження, маніпуляцій в системі безпеки, щоб приховати попередні етапи в ланцюжку кіберпроникнення та створити враження, що конфіденційні дані або системи незатронуті), відмова в обслуговуванні або шифрування даних тощо.

Етап 17. Маніпуляції із ціллю атаки (Impact). Реалізуються методи та засоби маніпулювання, переривання або знищення цільової системи та (або) даних (атаки

на доступність та цілісність) для досягнення кінцевої мети та (або) приховування слідів.

Етап 18. Досягнення цілі атаки (Objectives). Виконання дій щодо реалізації сценарію кібератаки, спрямованих на досягнення кінцевої мети порушників.

Модель UKC дає розуміння сутності та можливих сценаріїв складних кібератак [31, 32]. У ході їх реконструкції кожен етап можна розбити на окремі блоки характерні для конкретної APT. Блоки можуть характеризуватись індивідуальними атрибутами (включаючи специфікацію поведінки, методів та засобів, що використовуються).

Власну розширену модель CKC використовує [33] антивірусна лабораторія PandaLabs компанії Panda Security SL (рис. 1.6):

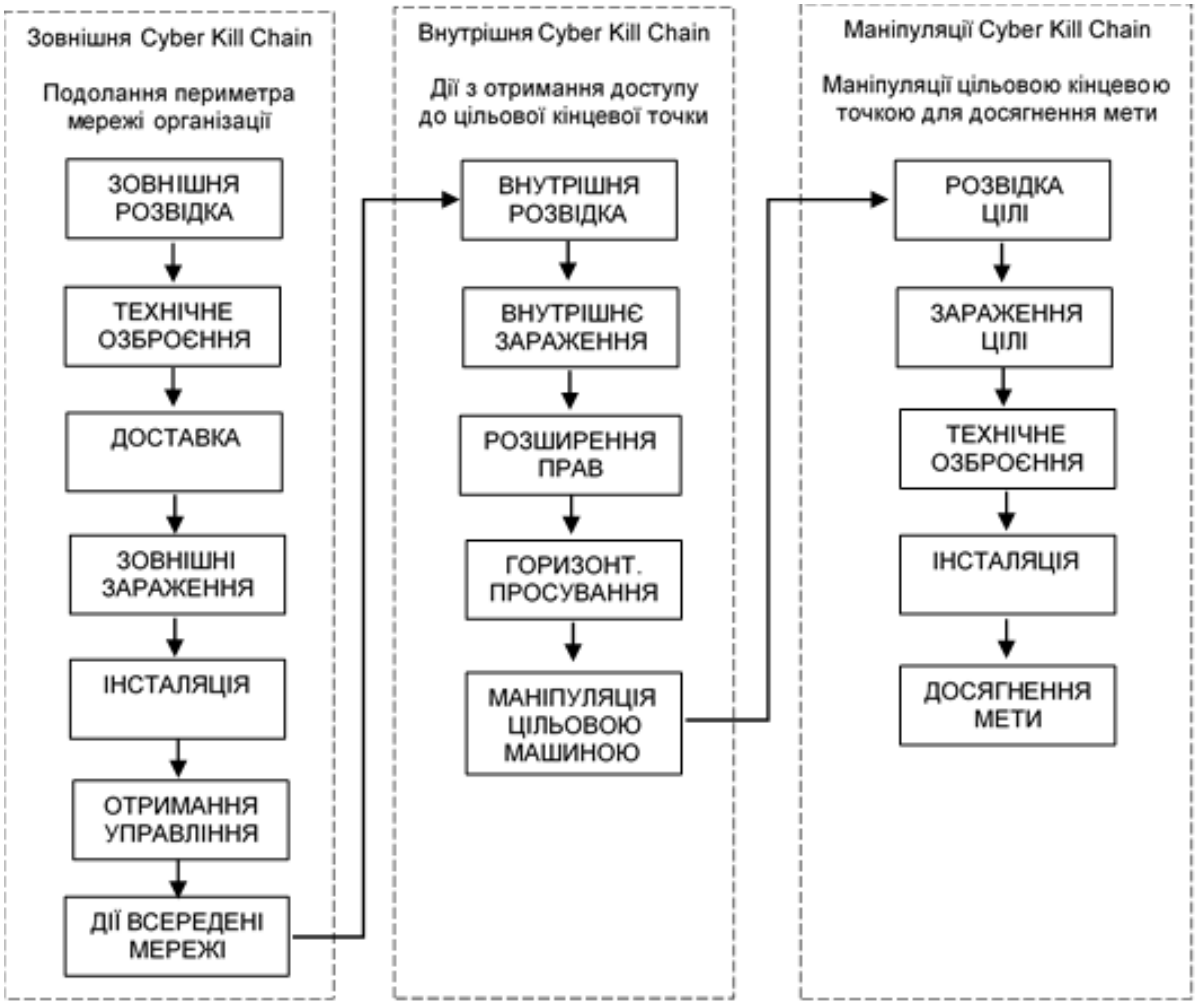


Рисунок 1.6 – Модель Cyber Kill Chain компанії Panda Security

Джерело: [33] в інтерпретації автора

Різноманітність загроз, частота появи, складність та цільовий характер кібератак вимагає перегляду існуючих правил безпеки з переходом до поєднання технологій запобігання, виявлення та реагування на кібератаки. Некомерційною організацією MITRE розроблено так звані матриці ATT&CK (англ. *Adversarial Tactics, Techniques & Common Knowledge*, тактики, техніки та загальнодоступні знання про зловмисників), як спосіб описати та класифікувати поведінку зловмисників на основі реальних спостережень [34]. ATT&CK являє собою структурований список відомих типів поведінки зловмисників, які об'єднані в тактики та техніки та згруповані у кількох матрицях. Оскільки цей список досить повно відображає різну поведінку зловмисників під час компрометування мереж, можливо його практичне використання для оцінки різних заходів захисту, вивчення фактів, можливих сценаріїв кібератак з урахуванням наявного обладнання та програмного забезпечення, що використовується в системах. База знань ATT&CK успішно використовується для аналізу існуючих та потенційних кіберзагроз, планування засобів управління захистом, пошуку загроз, виявлення та розслідування кіберінцидентів, інтеграції інструментів безпеки, обміну аналітичною та оперативною інформацією про атаки, джерела загроз або злочинні групи, для підвищення ефективності використання засобів управління захистом, тестування на проникнення та імітації цілеспрямованих кібератак з метою оцінки кібербезпеки систем та інфраструктури в цілому [35-37].

Компанія Panda Security опублікувала звіт «Розуміння загроз 2020» [38], який містить висновки про необхідність перегляду існуючих стратегій кіберзахисту, та висвітлює погляди на майбутнє інформаційної безпеки. Зазначається, що мережеві кінцеві пристрої всіх типів: від робочих станцій до ноутбуків та серверів, вимагають такого підходу, що об'єднує разом передовий захист кінцевих пристроїв (EPP) та можливості виявлення та реагування на атаки проти них (EDR) з системою безпеки по принципу «нульової довіри» (zero-trust). Така технологія «забезпечить безпрецедентний рівень контролю, видимості та гнучкості, необхідний у динамічній війні з невідомими зловмисниками та загрозами» [38].

1.3 Концепція архітектури нульової довіри

Описані в підрозділах 1.1 та 2.2 проблеми та фактори в сфері кіберзахисту змушують шукати альтернативу моделі кібербезпеки периметру, тобто будь-які системи повинні бути готовими як до зовнішніх векторів атак, так й до внутрішніх. Одна з найбільш популярних концепцій у даному напрямку - архітектура нульової довіри (від англ. *Zero Trust Architecture, ZTA*), що підтверджують результати дослідження Microsoft: згідно проведеного в 2021 році опитування осіб, які приймають рішення у сфері безпеки: 90% опитаних ознайомлені із стратегією нульової довіри, 35% заявили про повне її впровадження у своїй організації, 42% підтвердили процес впровадження, 24% опитаних планують застосування (зауваження: в підрахунок увійшли відповіді тільки тих, хто взагалі має уявлення про існування моделі ZTA) [39, 40]. Крім цього, в травні 2021 року Президентом Сполучених штатів Америки підписаний Указ про підвищення рівня національної кібербезпеки [13], в якому архітектура нульової довіри визнається «найкращим методом безпеки», а федеральному уряду та різним відомствам встановлюються завдання та терміни впровадження архітектура нульової довіри.

Проте, в ході пошуку та опрацювання джерел інформації, не знайдено жодної наукової праці чи статті, що присвячена дослідженню практичного застосування концепції нульової довіри. Більшість публікацій носять декларативний характер освітлення принципів архітектури або маркетингового позиціювання нових програмних продуктів, що використовують концепцію ZTA. Можливо, це пов’язане з тим, що єдиний офіційний документ Національного інституту стандартів і технологій США (NIST) – NIST 800-207 [41], який опублікований в серпні 2020 року, містить лише абстрактний опис принципів нульової довіри, прогнозовану сферу застосування та план створення систем із застосуванням принципів Zero Trust, а наступна публікація NIST 1800-35B [42], що описує порядок впровадження архітектури нульової довіри та наводить конкретні практичні приклади такого впровадження, опублікована нещодавно: в липні 2022 року. Тому дослідження можливості практичного застосування принципів та архітектури нульової довіри для забезпечення кіберзахисту

державних інформаційних ресурсів та інформаційно-комунікаційних систем проводиться вперше.

В документі NIST 800-207 [41] зазначені кілька важливих аспектів, які необхідно виділити:

Аспект 1. Концепція ураховує, що інфраструктури організацій стають все більш складними та розподіленими (відокремлені офіси та філіали зі своєю локальною інфраструктурою, включеною до загальної, використання мобільних систем та хмарних технологій тощо). Цей фактор визнається причиною низької ефективності методів мережевої безпеки на основі периметру.

Аспект 2. Враховується практичний досвід того, що методи мережевої безпеки на основі периметру вже не достатні для захисту: після подолання периметру, порушнику вже ніщо не заважає подальше «горизонтальне переміщення» (*довідково: описано в підрозділі 1.2 та на рис. 1.5, 1.6*).

Аспект 3. Саме складність сучасної інфраструктури та відсутність дієвого захисту після подолання периметру безпеки призвело до розробки нової моделі кібербезпеки, яка позиціонується як «нульова довіра» (англ. *zero trust, ZT*).

Аспект 4. Концепція нульової довіри базується на раніше розробленій концепції «чорного ядра» (від англ. *black core*), яка пропонує перехід від моделі безпеки на основі периметру до моделі, що орієнтована на безпеку окремих транзакцій.

Аспект 5. В першу чергу підхід ZT орієнтований на захист даних та послуг, але може та має бути розширений для включення всіх активів організації (пристроїв, компонентів інфраструктури, застосунків, віртуальних та хмарних компонентів тощо) та суб'єктів (кінцевих користувачів, застосунків та інших об'єктів-процесів, що запитують інформацію із ресурсів).

Аспект 6. Встановлюється правило постійної автентифікації та авторизації користувачів при кожному запиті на доступ. Доступ повинен надаватися з мінімальними привілеями.

Аспект 7. Головним завданням ZT вважається запобігання несанкціонованого доступу до ресурсів із забезпеченням максимального контролю за доступом.

Аспект 8. Підхід ZT – це не єдина архітектура, а по суті набір керівних принципів для робочого процесу проектування систем та операцій, які можна використовувати для покращення стану безпеки будь-якої класифікації та рівня чутливості. Підхід ZT не передбачає повної заміни існуючих технологій безпеки.

Аспект 9. Ефективність нульової довіри забезпечується комплексними методами забезпечення інформаційної безпеки та стійкістю IT-систем до відмов. Існуючі підходи на основі оцінки ризиків повинні залишатися без змін.

Аспект 10. Принципи нульової довіри доповнюють та поєднуються з існуючими політиками безпеки та рекомендаціями з кібербезпеки, управління ідентифікацією та доступом, безперервним моніторингом стану безпеки.

В розділі 2.1 NIST 800-207 сформульовано сім принципів архітектури нульової довіри:

Принцип 1. Всі джерела даних та послуг вважаються ресурсами. Мережа може складатися з кількох пристроїв різного класу. Організація має право класифікувати особисті пристрої як ресурси, якщо вони можуть отримати доступ до даних та послуг, що належать організації.

Принцип 2. Всі комунікації захищаються незалежно від їхнього розташування в мережі. Розташування у внутрішній мережі само по собі не вважається довірою. Довіра не пов'язується із місцезнаходженням. Запити на доступ від користувачів, розміщених у мережній інфраструктурі організації (наприклад, усередині традиційного периметра), повинні відповідати тим самим вимогам безпеки, що й запити, що надходять із будь-якої іншої мережі. Комунікації повинні здійснюватися максимально безпечним способом, забезпечувати конфіденційність та автентифікацію джерела.

Принцип 3. Доступ до окремих корпоративних ресурсів надається для кожної сесії та сеансу. Доступ надається з мінімально можливими привілеями, що необхідні для виконання завдання користувача. Проходження процедури

автентифікація та авторизація користувача або процесу для доступу до одного ресурсу не дають доступу до іншого.

Принцип 4. Доступ до ресурсів визначається динамічною політикою, що включає стан ідентифікації користувача, процесу, застосунку та інших атрибутів (наприклад, вимірюваних відхилень в спостережній моделі використання). Політика - це набір правил доступу на основі атрибутів, які організація призначає користувачеві, процесу, ресурсу або застосунку.

Принцип 5. Організація повинна забезпечувати максимально можливий безпечний стан всіх пристроїв, що належать їй, та відстежувати свої активи, щоб гарантувати їх максимальну безпеку. «Максимально можливий безпечний стан» означає, що пристрій перебуває в найбільш практичному безпечному стані та виконує тільки ті дії, що відповідають його місії. Жоден актив не вважається надійним за своєю суттю. Організація повинна оцінювати стан безпеки активу при оцінці запиту на ресурс.

Принцип 6. Процедури автентифікації та авторизації є динамічними та суворо контролюються до самого моменту, коли доступ буде дозволений. Це постійний цикл отримання доступу, моніторингу та оцінки загроз, адаптації та переоцінки довіри до поточного зв'язку. Передбачається, що організація, що реалізує ZTA, має всі необхідні системи керування обліковими даними, активами та доступом, включаючи багатофакторну автентифікацію.

Принцип 7. Організація повинна здійснювати збір максимально можливого обсягу інформації про поточний стан активів, мережної інфраструктури та комунікацій, використовуючи її для підвищення власної безпеки, а також дані про мережний трафік та запити доступу, необхідні для покращення створення та застосування політики безпеки.

При цьому із тексту документу можна виокремити кілька застережень стосовно застосування принципів:

Застереження 1. Викладені принципи є «ідеальною метою». Визначається, що не всі принципи можуть бути реалізовані так, як вони сформульовані.

Застереження 2. Не встановлюються умови, за яких викладені принципи повинні бути задіяні, а не виключені.

Застереження 3. Викладені принципи слід розуміти як «технологічно незалежні» (в тексті наведено термін англ. *technology agnostic*). Тобто найкращі рішення слід обирати із урахуванням їх переваг, незалежно від того, на чому вони засновані.

Інновація архітектури нульової довіри полягає в новому підході до принципів використання двох основних компонентів безпеки: процедури автентифікації при наданні доступу до кожного ресурсу та механізму надання доступу. В документі NIST 800-207 представлена абстрактна модель надання доступу представлена на рисунку 1.7:

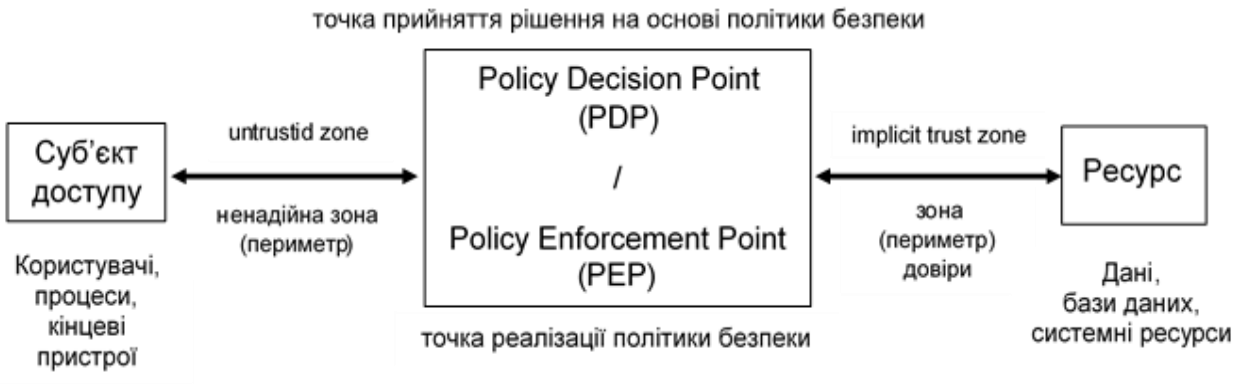


Рисунок 1.7 – Абстрактна модель доступу з нульовою довірою

Джерело: [41], технічний переклад автора

У моделі ZTA користувачу (або кінцевому пристрою) процес отримання доступу до корпоративного ресурсу надається через своєрідний «контрольно-перепускний пункт» (PDP)/(PEP). Користувач проходить перевірку через точку прийняття рішення про доступ на основі політики безпеки (від англ. *Policy Decision Point, PDP*) та через точку реалізації політики безпеки (від англ. *Policy Enforcement Point, PEP*), що відповідає за виклик PDP та правильну обробку відповіді. Ідея концепції ZTA полягає в тому, щоб перемістити точку застосування політики якомога ближче до ресурсу. PDP/PEP не можуть застосовувати додаткові політики поза межами свого розташування в потоці трафіку.

В NIST 800-207 описується ядро логічних компонентів, як складової для розгортання архітектури нульового дня в інфраструктурі організації. Концептуальна рамкова модель (рис. 1.8) показує базові відносини між компонентами та їх взаємодіями:

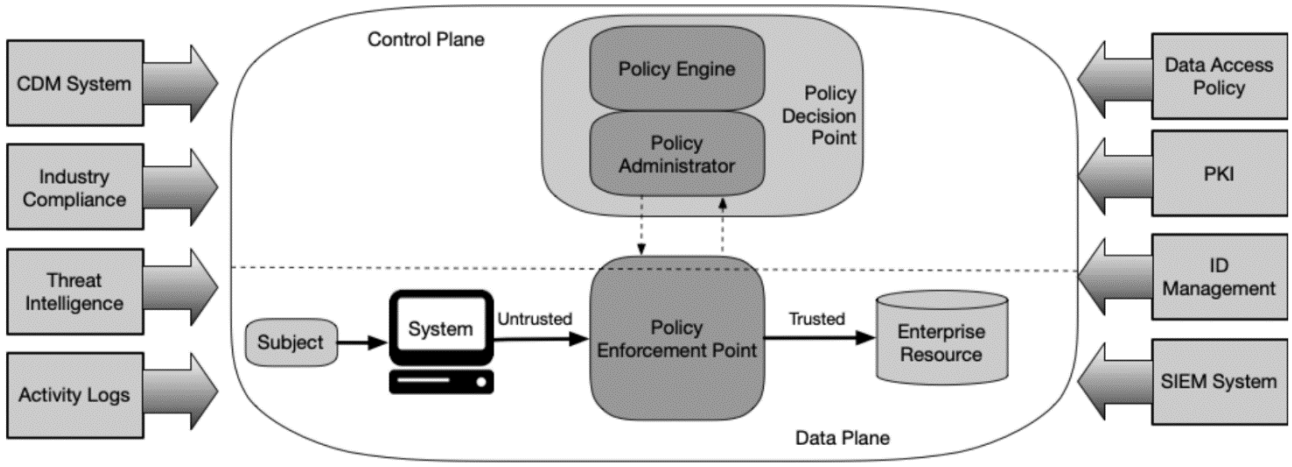


Рисунок 1.8 – Концептуальна рамкова модель доступу з нульовою довірою

Джерело: [41]

Точка прийняття рішення про доступ на основі політики безпеки представлена двома логічними компонентами: механізмом реалізації політики та управлінням політикою. Механізм реалізації політики відповідає за остаточне рішення щодо надання суб'єкту доступу до ресурсу. Механізм реалізації політики використовує політику безпеки, встановлену в організації, а також вхідні дані із будь-яких зовнішніх джерел (наприклад, служб аналізу загроз) в якості вхідних даних для алгоритму довіри для надання чи відмови доступу до ресурсу. Механізм реалізації політики пов'язаний з компонентом управління політикою. Механізм політики приймає та реєструє рішення (дозволено або заборонено), а управління політикою виконує це рішення. Ці компоненти може бути реалізовані як одна служба, так й окремими елементами. Точка прийняття рішення про доступ на основі політики безпеки належить до середовища управління (*Control Plan*), а точка реалізації політики безпеки реалізується в середовищі даних (*Data Plan*) та розділяє суб’єктів доступу та ресурси. Звертається увага на те, що це ідеальна модель.

В документі NIST 800-207 [41] зазначені прогнозовані ризики складності застосування моделі нульової довіри:

Складність 1. Відсутність сталої термінології для однозначного трактування концепції та принципів ZTA.

Складність 2. Знаходження стратегії застосування архітектури нульової довіри (проектування, планування, закупок компонентів) на стадії формування та накопичення досвіду використання ZTA.

Складність 3. Відсутність стандартів для застосування ZTA та стандартизації інтерфейсів взаємодії між компонентами ZT.

Складність 4. Відсутність єдиного рішення для розробки ZTA. Публікація NIST 800-207 залишає ці «сірі зони» для майбутньої роботи дослідників з розробки протоколів або середовищ, що «допоможуть організаціям впровадити архітектуру нульової довіри» [41, п.п. B.2., B.3, B.4].

Складність 5. Відсутність методології застосування «технологічної незалежності» (в тексті наведено термін англ. *technology agnostic*) принципів ZTA.

Тому саме аналіз NIST 1800-35B [42], що опублікований в липні 2022 року, та містить опис практичного впровадження архітектури нульової довіри на прикладах застосування конкретних комерційних продуктів, дає можливість дослідження застосування архітектури нульової довіри при розробці вдосконалених моделей автентифікації, доступу, політики безпеки для підвищення кіберзахисту державних інформаційних ресурсів та інформаційно-комунікаційних систем та їх практичної реалізації в реальній системі. Дослідження може бути проведено із застосуванням методів вивчення аналога (прототипу) та еталонного оцінювання (англ. *benchmarking*).

В додатку F NIST 1800-35B наведений приклад реалізації моделі доступу з нульовою довірою із використанням Microsoft Azure AD (сервіс із використанням хмарних технологій для формування облікових даних суб’єктів доступу на основі багатофакторної автентифікації при доступі до ресурсів організації).

Логічна архітектура реалізації моделі доступу з нульовою довірою із використанням Microsoft Azure AD представлена на рисунку 1.9:

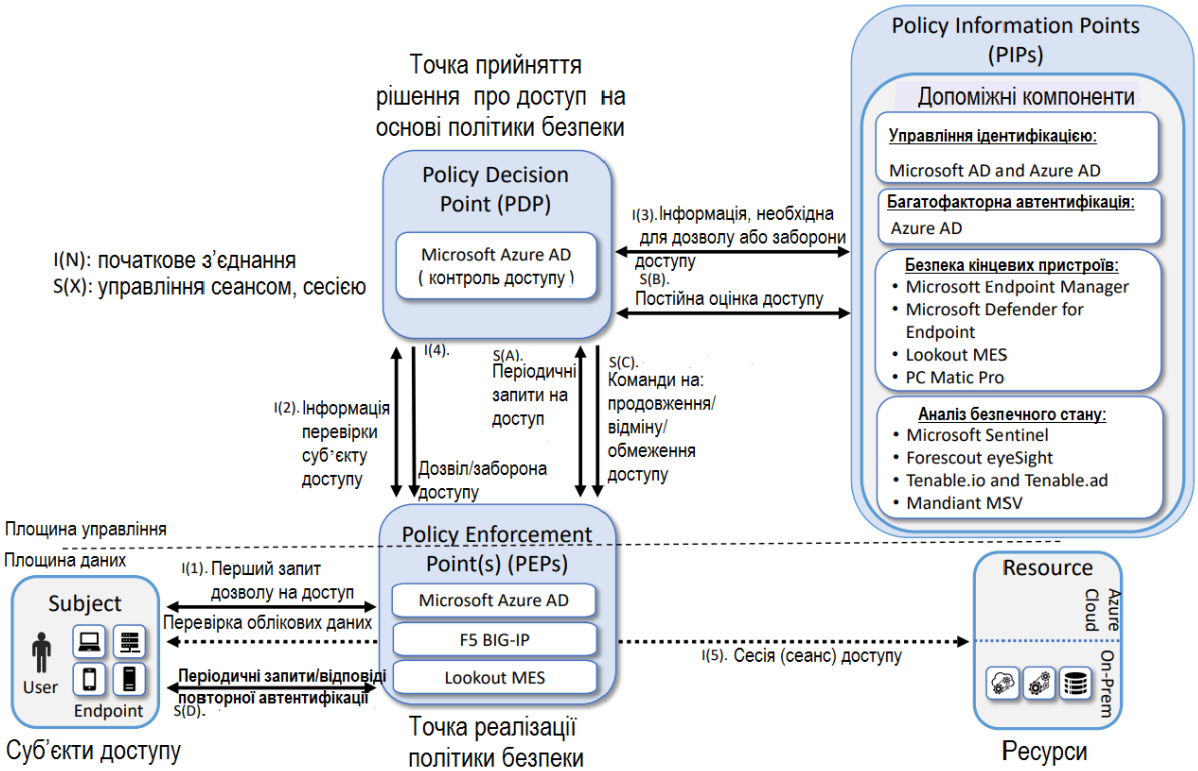


Рисунок 1.9 – Приклад реалізованої моделі доступу з нульовою довірою

Джерело: [42], технічний переклад автора

Перелік програмних засобів, які використовуються для реалізації такої моделі доступу з нульовою довірою, зазначені в таблиці 1.1:

Таблиця 1.1 – Програмні засоби, що використані для практичної реалізації моделі доступу з нульовою довірою, згідно NIST 1800-35B

№ з/п	Компонент архітектури	Найменування програмного засобу	Функції
1	(PE)	Microsoft Azure AD	Приймає рішення про надання, відмову або відкликання доступу до ресурсу на основі корпоративної політики, інформації від допоміжних компонентів та алгоритму довіри
2	(PA)	Microsoft Azure AD	Виконує рішення (PE) про політику, надсилаючи команди в точку реалізації політики безпеки (PEP), який встановлює або відключає канал зв'язку між суб'єктом та ресурсом
3	(PEP)	Microsoft Azure AD, F5 BIG-IP, Lookout MES	Забезпечують захист зони довіри, в якій розміщено один або кілька корпоративних ресурсів; встановлює, відстежує та розриває з'єднання між суб'єктом та ресурсом за вказівкою (PA), пересилає запити та отримує команди від (PA)

1.4 Вимоги з кіберзахисту, встановлені законодавством України

Приватні організації можуть застосовувати будь-які технічні, апаратні, програмні засоби та рішення з інформаційної безпеки без обмежень, на свій власний розсуд. Проте захист державних інформаційних ресурсів, здійснення технічного та криптографічного захисту інформації, сфера електронних довірчих послуг та кіберзахист критичної інфраструктури регламентується низкою законодавчих та нормативно-правових актів, вимоги яких необхідно ураховувати при практичній реалізації конкретних рішень кібербезпеки, а саме:

Вимога 1. Повинні використовуватися засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації [43, ст. 8].

Вимога 2. Повинні використовуватися засоби технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації [43, ст. 8].

Вимога 3. Електронна ідентифікація, як процедура використання ідентифікаційних даних особи в електронній формі, повинна однозначно визначати фізичну, юридичну особу або представника юридичної особи [44, ст. 1].

Вимога 4. Автентифікація, як електронна процедура, повинна підтверджувати електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних [44, ст. 1].

Вимога 5. Процедура електронної ідентифікації повинна здійснюватися за допомогою засобів електронної ідентифікації, що підпадають під схему електронної ідентифікації, затверджену Кабінетом Міністрів України [44, ст. 14]. Схема такої електронної ідентифікації описана в [45].

Вимога 6. Високий рівень довіри до схем електронної ідентифікації забезпечується тільки використанням кваліфікованих електронних підписів та печаток [44, ст. 15].

Вимога 7. Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, для засвідчення

чинності відкритого ключа повинні використовувати лише кваліфікований сертифікат відкритого ключа, та застосовувати виключно засоби кваліфікованого електронного підпису чи печатки, які мають вбудовані апаратно-програмні засоби, що забезпечують захист записаних на них даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання [44, ст. 17].

Вимога 8. Вибір кваліфікованого надавача електронних довірчих послуг (англ. *Certification authority, CA*) здійснюється тільки із Довірчого списку кваліфікованих надавачів електронних довірчих послуг [44, ст. 30].

Вимога 9. Повинні використовуватися виключно захищені носії особистих ключів - засоби кваліфікованого електронного підпису чи печатки, що призначені для зберігання особистого ключа та мають вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання [46, п. 4].

Вимога 10. Управління доступом користувачів та адміністраторів до об’єктів захисту (механізм розподілу прав доступу) повинно відповідати вимогам, зазначеним в [47, п. 11, 12].

Вимога 11. Процедура ідентифікація та автентифікація користувачів та адміністраторів повинна ураховувати вимоги, зазначені в [47, п.п. 13-18].

Вимога 12. Політика інформаційної безпеки повинна ураховувати вимоги, зазначені в [47, п. 7].

Вимога 13. Використання програмного та апаратного забезпечення здійснюється у відповідності до умов, визначених в [47, п.п 44-28].

Вимога 14. У засобах криптографічного захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, реалізуються криптоалгоритми та криптопротоколи, які є національними стандартами в обсязі функцій безпеки згідно з [48].

Вимога 15. Автентифікація суб'єктів та механізми з використанням методу цифрового підпису, повинні відповідати вимогам та описам в [49-51].

Висновки до розділу 1

Розкрито сутність проблем кіберзахисту: приведено висновки провідних спеціалістів в сфері комп'ютерної безпеки зі світовим ім'ям Петера Ноймана (Peter G. Neumann) та Роберта Вотсона (Robert N. M. Watson) з констатацією факту появи «системного глухого кута» в галузі захисту інформації. Сучасний стан кіберзахисту ними описується терміном «гонка озброєнь», в якій «сторона, що обороняється» перебуває в більш невигідній позиції, ніж «сторона, що атакує».

Визначено основні проблеми сучасного стану кіберзахисту: 1) зростаюча динаміка кількості та видів шкідливого програмного забезпечення; 2) поява у вільному доступі «конструкторів вірусів»; 3) низька ефективність антивірусних засобів та сумнівні перспективи їх розвитку; 4) наявність вразливостей «нульового дня», «люків», незадокументованих «входів» в системному та прикладному програмному забезпеченні; 5) відсутність національної системи верифікації іноземного програмного забезпечення на відсутність програмних та алгоритмічних закладок; 6) необхідність проведення процедури оновлення (update) та отримання оновлень програмного забезпечення через мережу Інтернет; 7) поява нових методів та способів зламу чи обходу криптографічного захисту інформації; 8) складність структури та технологій сучасних інформаційно-комунікаційних систем внаслідок розвитку інформаційних технологій, їх вразливість перед кіберзагрозами, відсутність дієвого захисту після подолання порушником периметру безпеки; 9) суттєва зміна тактики, сценаріїв, складності та інструментів проведення кібератак.

Наведено коротку характеристику та огляд виявлених проблем.

Виокремлено три основних фактори проблем кіберзахисту: 1) еволюцію кібератак; 2) цифрову трансформацію; 3) необхідність зміни парадигми кіберзахисту.

Проаналізовано небезпеку еволюції кібератак, зростання їх складності та ефективності.

З'ясовано, що фактично єдиним (щодо реальності практичного впровадження) та перспективним рішенням зміни парадигми кіберзахисту є

архітектура нульової довіри. Приведено непрямі та прямі доводи: 1) звіт компанії Panda Security; 2) результати дослідження компанії Microsoft; 3) указ Президента США про підвищення рівня національної кібербезпеки від 12.05.2021 року, в якому архітектура нульової довіри визнається «найкращим методом безпеки», а федеральному уряду та різним відомствам встановлюються завдання та терміни впровадження архітектури нульової довіри.

Акцентовано увагу на факт відсутності у вільному доступі наукових праць чи статей з дослідження практичного застосування концепції нульової довіри, зроблено припущення з причини цього факту.

Констатовано, що дослідження можливості практичного застосування концепції архітектури нульової довіри для кіберзахисту інфраструктури України проводиться вперше.

Приведено достовірні джерела інформації про архітектуру нульової довіри: спеціальні публікації NIST 800-207 та NIST 1800-35B, зроблено їх короткий огляд на основі авторського технічного перекладу, виділено необхідні аспекти.

Висвітлено принципи архітектури нульової довіри, необхідні для розуміння цієї концепції та застосування в ході дослідження.

Визначено інновацію архітектури нульової довіри в новому підході до принципів використання двох основних компонентів безпеки: процедур автентифікації та авторизації при наданні доступу до кожного ресурсу, та механізм надання такого доступу.

Підтверджено можливість застосування архітектури нульової довіри при розробці вдосконалених моделей автентифікації, доступу, політики безпеки для підвищення кіберзахисту державних інформаційних ресурсів та інформаційно-комунікаційних систем з метою їх практичної реалізації в реальних системах.

Проаналізовано норми чинного законодавства України у сферах захисту інформації, захисту державних інформаційних ресурсів, кіберзахисту об’єктів критичної інфраструктури, здійснення технічного та криптографічного захисту інформації, сфері електронних довірчих послуг на предмет виокремлення обов’язкових вимог для урахування в наступних етапах цієї роботи.

РОЗДІЛ 2
ВДОСКОНАЛЕННЯ МОДЕЛЕЙ АВТЕНТИФІКАЦІЇ, ДОСТУПУ ТА ПОЛІТИКИ БЕЗПЕКИ З НУЛЬОВОЮ ДОВІРОЮ

2.1 Обґрунтування вибраних рішень та методів їх реалізації

Для вирішення проблем 1-9 кіберзахисту та їх виокремлених факторів 1-3, визначених в підрозділі 1.1 розділу 1, з метою підвищення кіберзахисту від складних та комплексних кібератак, унеможливлення етапів 5-18 їх проведення, визначених моделями Cyber Kill Chain та Unified Kill Chain, що описані в підрозділі 1.2, пропонується використання архітектури нульової довіри, концепція якої досліджена в підрозділі 1.3 даної роботи.

Визначено, що інновація архітектури нульової довіри полягає в новому підході до принципів використання двох основних компонентів безпеки: процедур автентифікації та авторизації при наданні доступу до кожного ресурсу, та механізму надання такого доступу (по суті, політики безпеки).

Стандартом X.805 [52] процедури автентифікація та управління доступом визначені вимірами захисту (англ. *security dimensions*), та трактуються як комплекс заходів захисту, що призначений для реалізації конкретного аспекту мережевого захисту, проте вони не обмежені тільки мережею, а також поширюються на додатки та інформацію кінцевого користувача. Зазначається, що належним чином розроблені та здійснені виміри захисту підтримують політику захисту, яка визначена для конкретної мережі, та спрощують виконання правил, встановлених управлінням захистом.

Створення ефективної процедури автентифікація та управління доступом, як заходів захисту, складне технічне завдання, для вирішення якого можливо застосувати невід’ємну складову системного аналізу – моделювання.

Для побудови моделей автентифікації, управління доступом та політики безпеки з використанням принципів 1-7 концепції архітектури нульової довіри, описаних в підрозділі 1.3 даної роботи, необхідно сформувати вхідні дані. Достовірним джерелом даних визначена публікація NIST 1800-35B [42], що

описує порядок впровадження архітектури нульової довіри та наводить конкретні практичні приклади такого впровадження. Шляхом вивчення та аналізу документу виділені програмні засоби, що використані для практичної реалізації моделі доступу з нульовою довірою (табл. 1.1) та опис практичної реалізації доступу та автентифікації з використанням цих програмних засобів (рис. 2.1):

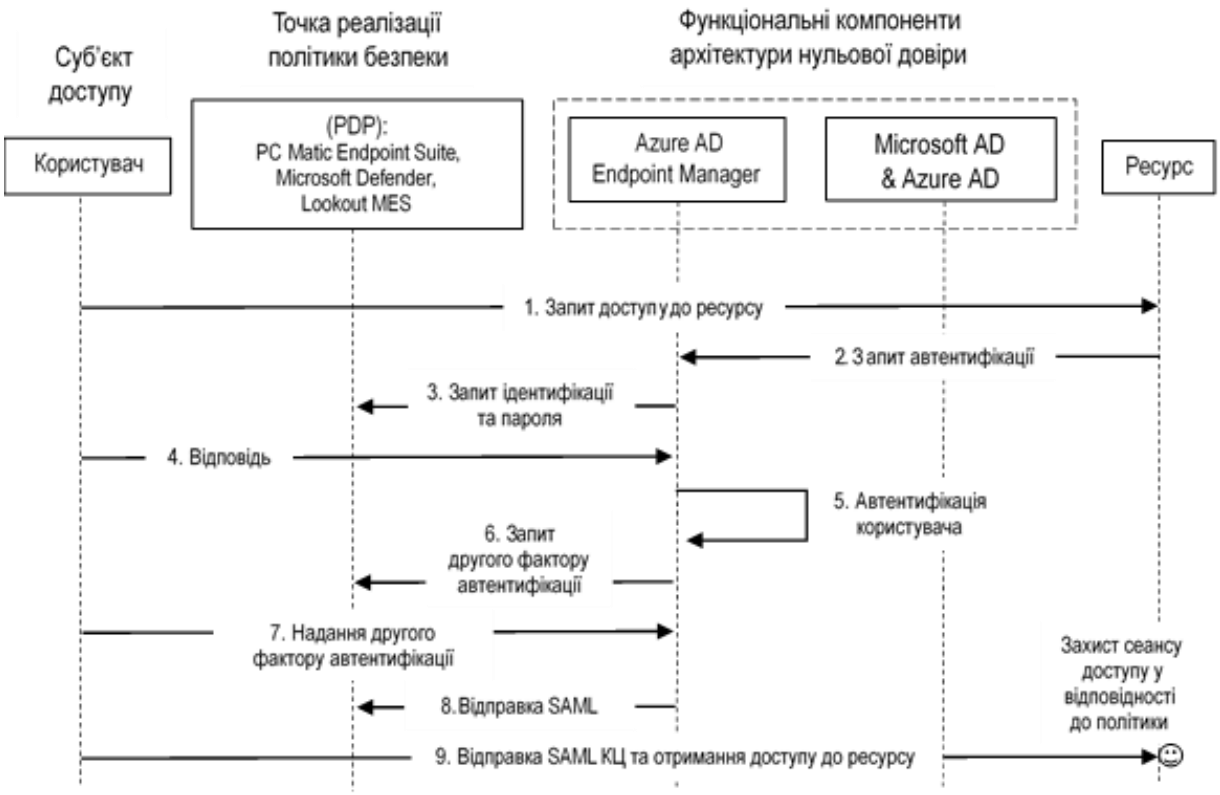


Рисунок 2.1 – Приклад практичної реалізації доступу та автентифікації в концепції архітектури нульової довіри, наведений в NIST 1800-35B

Джерело: [37], технічний переклад автора

Шляхом вивчення та аналізу технічної документації, що доступна на офіційних сайтах розробників програмних засобів, дослідженням характеристик самих програмних засобів, їх властивостей, сформувати вхідні дані для моделювання.

Розробку моделей автентифікації, доступу до ресурсів та політики безпеки доцільно здійснити з опорю на досвід подібного моделювання та методик, що запропоновані в [53-85], за можливості, із з використанням єдиного понятійного апарату. Розробку моделей завершити їх аналізом, перевіркою достовірності одержаних результатів та висновком щодо можливості їх практичної реалізації.

2.2 Вдосконалення моделі автентифікації

Вхідні дані для моделювання. З рис. 2.1 та даних, наведених в табл. 1.1 відомо, що процедура автентифікації суб'єктів доступу із використанням концепції нульової довіри здійснюється із використанням Azure Active Directory (Azure AD), корпоративною службою ідентифікації, яка підтримує єдиний вхід, багатофакторну автентифікацію та умовний доступ. З технічної документації, яка доступна на офіційному сайті Microsoft відомо, що в Azure AD використовується модифікація протоколу Kerberos, який в свою чергу побудований на протоколі Нідгема-Шредера. Наведених даних достатньо для складання формалізованої моделі з опорю на методики, що запропоновані в [53-60].

Побудова базової моделі. Для формалізованого представлення моделі введемо наступні визначення:

U - суб'єкт доступу: користувач (англ. *user*);

S – система (англ. *system*) або сервер (англ. *server*) прикладної системи, що надає сервіс доступу до ресурсу (наприклад, бази даних);

C - центрі автентифікації (англ. *CA, Certification Authority*), так звана «третя довірча сторона».

Процес реалізації протоколу автентифікації здійснюється в сім етапів:

Етап 1. Користувач запитує відкритий ключ (англ. *public key*) в центрі автентифікації:

$$U \rightarrow C: K_p(S), \tag{2.1}$$

де: $K_p(S)$ – відкритий ключ серверу.

Етап 2. Центр автентифікації надсилає користувачу завірений електронним підписом відкритий ключ та ідентифікатор:

$$C \rightarrow U: \{ K_p(S), K_{ss}(S, C)\} \cdot K_s(C), \tag{2.2}$$

де: $K_{ss}(S, C)$ – спільний ключ сесії або сеансу (англ. *shared session key*) серверу та центру автентифікації,

$K_s(C)$ – особистий (англ. *secret key*) ключ центру автентифікації.

Етап 3. Користувач надсилає серверу одноразовий код та ідентифікатор:

$$U \rightarrow S: \{ K_p(U), N(U)\} \cdot K_{ss}(U, C), \quad (2.3)$$

де: $K_p(U)$ – відкритий ключ користувача;

$N(U)$ – одноразовий код (англ. *nonce*) обраний випадковим або псевдовипадковим чином користувачем;

$K_{ss}(U, C)$ – спільний ключ сесії або сеансу користувача та центру автентифікації.

Етап 4. Сервер запитує відкритий ключ (параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів) користувача в центрі автентифікації:

$$S \rightarrow C: K_p(U), \quad (2.4)$$

де: $K_p(U)$ – відкритий ключ користувача.

Етап 5. Центр автентифікації надсилає серверу завірений кваліфікованим електронним підписом відкритий ключ (взаємопов'язані параметри алгоритму асиметричного криптографічного перетворення) та ідентифікатор:

$$C \rightarrow S: \{ K_p(U), K_{ss}(U, C)\} \cdot K_p(C), \quad (2.5)$$

де: $K_p(U)$ – відкритий ключ користувача;

$K_{ss}(C, U)$ – спільний ключ сесії або сеансу користувача та центру автентифікації.

$K_p(C)$ – відкритий ключ центру автентифікації.

Етап 6. Сервер генерує одноразовий код та передає його разом із кодом користувача, зашифрував через відкритий ключ користувача:

$$S \rightarrow U: N(U, K_p(U)), N(S, K_p(U)), \quad (2.6)$$

де: $K_p(U)$ – відкритий ключ користувача;

N – формування одноразового коду шифруванням через відкритий ключ користувача.

Етап 7. Користувач надсилає назад серверу одноразовий код, який при цьому зашифрований відкритим ключем серверу:

$$U \rightarrow S: N(S, K_{ss}(S, C)), \quad (2.7)$$

де: $K_p(U)$ – відкритий ключ користувача;

$K_{ss}(S, C)$ – спільний ключ сесії (сеансу) серверу та

N – формування одноразового коду шифруванням через відкритий ключ серверу центру автентифікації.

Таким чином модель автентифікації (вважатимемо її базовою), що описана на рисунку 2.1, прийме наступного вигляду у формалізованому представленні (табл. 2.1):

Таблиця 2.1 - Базова модель автентифікації користувачів

№ з/п	Етап	Позначення
1	Користувач запитує відкритий ключ в центрі автентифікації	$U \rightarrow C: K_p(S)$
2	Центр автентифікації надсилає користувачу завірений кваліфікованим електронним підписом відкритий ключ та ідентифікатор	$C \rightarrow U: \{ K_p(S), K_{ss}(S, C) \} \cdot K_s(C)$
3	Користувач надсилає серверу одноразовий код та ідентифікатор	$U \rightarrow S: \{ K_p(U), N(U) \} \cdot K_{ss}(U, C)$
4	Сервер запитує відкритий ключ користувача в центрі автентифікації	$S \rightarrow C: K_p(U)$
5	Центр автентифікації надсилає серверу завірений кваліфікованим електронним підписом відкритий ключ та ідентифікатор	$C \rightarrow S: \{ K_p(U), K_{ss}(U, C)\} \cdot K_p(C),$
6	Сервер генерує одноразовий код та передає його разом із кодом користувача, зашифрував через відкритий ключ користувача	$S \rightarrow U: N(U, K_p(U)), N(S, K_p(U))$
7	Користувач надсилає назад серверу одноразовий код, який при цьому зашифрований відкритим ключем серверу	$U \rightarrow S: N(S, K_{ss}(S, C))$

Аналіз базової моделі. Базова модель автентифікації включає сім етапів. Багатоетапна (застосовується також термін «багатораундова») методика перевірки ключів двох сторін (користувач та сервіс) через центр автентифікації із використанням надійного алгоритму дозволяє забезпечити надійний захист сервісу від зовнішніх кіберзагроз. Разом із цим, базова модель має ряд характерних недоліків, детально описаних в дослідженнях [58, 59]. Також відомо, що на сьогоднішній день існує кілька методик обходу захисту [61]. Модель однієї з таких атак може бути побудована через введення суб'єкта процесу атаки - порушника, який почергово може видавати себе за сервер або користувача, а також функцій, які відповідають ключам, які використовує даний порушник з метою обходу захисних алгоритмів протоколу автентифікації:

I – порушник (англ. *intruder*);

$K_p(I)$ – відкритий ключ порушника;

$K_{ss}(I, C)$ – спільний ключ сесії (сеансу) порушника та центру автентифікації;

$K_{ss}(I, U)$ – спільний ключ сесії (сеансу) порушника та користувача.

Розглянемо втручання порушника в процес автентифікації, описаний в базовій моделі, у вигляді додатковий дій на етапах 1-7 автентифікації.

Дія 1. Користувач надсилає порушнику (який видає себе за сервер) одноразовий код та ідентифікатор:

$$U \rightarrow I: \{ K_p(I), N(U) \} \cdot K_{ss}(I, C), \tag{2.8}$$

де: I – порушник (англ. *intruder*);

$K_p(I)$ – відкритий ключ порушника;

$N(U)$ – одноразовий код користувача;

$K_{ss}(I, C)$ – відкритий

Дія 2. Порушник надсилає серверу одноразовий код та ідентифікатор:

$$I \rightarrow S: \{ K_p(I), N(U) \} \cdot K_{ss}(S, C), \tag{2.9}$$

де: $K_p(I)$ – відкритий ключ порушника;

$N(U)$ – одноразовий код користувача;

$K_{ss}(S, C)$ – спільний ключ сесії (сеансу) серверу та центру автентифікації.

Дія 3. Користувач надсилає порушнику одноразовий код серверу, який при цьому зашифрований відкритим ключем сесії порушника та центру автентифікації:

$$U \rightarrow I: N(S, K_{ss}(I, C)), \quad (2.10)$$

де: N – формування одноразового коду;

$K_{ss}(I, C)$ – спільний ключ сесії (сеансу) порушника та центру автентифікації.

Дія 4. Порушник надає серверу одноразовий код сервера, зашифрований спільним ключем сесії сервера та центру автентифікації:

$$I \rightarrow S: N(S, K_{ss}(S, C)), \quad (2.11)$$

де: N – формування одноразового коду;

$K_{ss}(I, C)$ – спільний ключ сесії (сеансу) порушника та центру автентифікації.

Отримана модель атаки з обходу алгоритмів автентифікації представлена у таблиці 2.2:

Таблиця 2.2 - Модель атаки на алгоритм автентифікації

№ з/п	Етап	Позначення
1	Користувач запитує відкритий ключ в центрі автентифікації	$U \rightarrow C: K_p(S)$
2	Центр автентифікації надсилає користувачу завірений кваліфікованим електронним підписом відкритий ключ та ідентифікатор	$C \rightarrow U: \{ K_p(S), K_{ss}(S, C) \} \cdot K_s(C)$
3	Користувач надсилає порушнику (який видає себе за сервер) одноразовий код та ідентифікатор	$U \rightarrow I: \{ K_p(I), N(U) \} \cdot K_{ss}(I, C)$
4	Порушник надсилає серверу одноразовий код та ідентифікатор	$I \rightarrow S: \{ K_p(I), N(U) \} \cdot K_{ss}(S, C)$
5	Сервер запитує відкритий ключ користувача в центрі автентифікації	$S \rightarrow C: K_p(U)$
6	Центр автентифікації надсилає серверу завірений кваліфікованим електронним підписом відкритий ключ та ідентифікатор	$C \rightarrow S: \{ K_p(U), K_{ss}(U, C)\} \cdot K_p(C),$
7	Сервер генерує одноразовий код та передає його разом із кодом користувача, зашифрував через відкритий ключ користувача	$S \rightarrow U: N(U, K_p(U)), N(S, K_p(U))$
8	Користувач надсилає порушнику одноразовий код серверу, який при цьому зашифрований відкритим ключем сесії порушника та центру автентифікації	$U \rightarrow I: N(S, K_{ss}(I, C))$
9	Порушник надає серверу одноразовий код сервера, зашифрований спільним ключем сесії сервера та центру автентифікації	$I \rightarrow S: N(S, K_{ss}(S, C))$

Можна побачити, модель атаки відповідає базовій моделі, що представлена в табл. 2.1, але до неї додані пункти 3, 4, 8, 9, які відповідають діям 1-4 порушника, який видає себе (маскується) за сервер (атака типу «маскарад»). Очевидно, що базова модель потребує вдосконалення.

Вдосконалення базової моделі. Описаний в базовій моделі протокол автентифікації використовує відкритий ключ центру автентифікації (так звана «третя довірча сторона»). У відповідності до вимог 4-8, наведених в підрозділі 1.4 даної роботи, функції центру автентифікації в Україні виконують кваліфіковані надавачі електронних довірчих послуг із Довірчого списку [62], які у відповідності до вимог [48], використовують алгоритми електронного підпису, визначені ДСТУ ETSI TS 119 312:2015 [50] , ДСТУ 4145-2002 [51] та механізми автентифікації згідно ДСТУ ISO/IEC 9798-3:2014 [49].

Таким чином, при заміні алгоритму автентифікації з'являється можливість включити в протокол автентифікації спільний ключ між користувачем та центром автентифікації $K(U, C)$, що надає можливість створення двох послідовностей одноразового коду, обраних випадковим (або псевдовипадковим) чином сервером $N_1(U)$ та користувачем $N_2(U)$ відповідно.

Відобразимо цю вдосконалену модель в таблиці 2.3:

Таблиця 2.3 – Вдосконалена модель автентифікації

№ з/п	Етап	Позначення
1	Користувач, з використанням загального ключа та послідовності одноразового коду, отримує в центрі автентифікації відкритий ключ та ідентифікатор	$U \rightarrow C: \{ K_p(I), N_1(U) \} \cdot K_p(C)$
2		$C \rightarrow U: \{ N_1(U), K_{ss}(S, C) \} \cdot K(U, C)$
3	Користувач надсилає серверу другий одноразовий код та ідентифікатор	$U \rightarrow S: \{ N_2(U), K_p(I) \} \cdot K_{ss}(S, C)$
4	Сервер запитує відкритий ключ користувача в центрі автентифікації	$S \rightarrow C: \{ S, N_1(U), K_p(I) \} \cdot K_p(C)$
5	Центр автентифікації надсилає серверу відкритий ключ та ідентифікатор	$C \rightarrow S: \{ N_1(U), K_{ss}(U, C), K_p(I) \} \cdot K_{ss}(S, C)$
6	Сервер генерує одноразовий код та передає його разом із кодом користувача, зашифрував через відкритий ключ користувача	$S \rightarrow U: \{ N_2(U), N_2(S) \} \cdot K_{ss}(U, C)$
7	Користувач надсилає порушнику одноразовий код серверу, який при цьому зашифрований відкритим ключем сесії порушника та центру автентифікації	$U \rightarrow S: N_2(S) \cdot K_{ss}(S, C)$

Аналіз вдосконаленої моделі автентифікації. На рис. 2.2 представлено порівняння базової моделі, на яку здійснюється атака з обходу алгоритму автентифікації (рис. 2.2 *а*) та вдосконаленої моделі, яка блокує дії потенційного порушника (рис. 2.2 *б*):

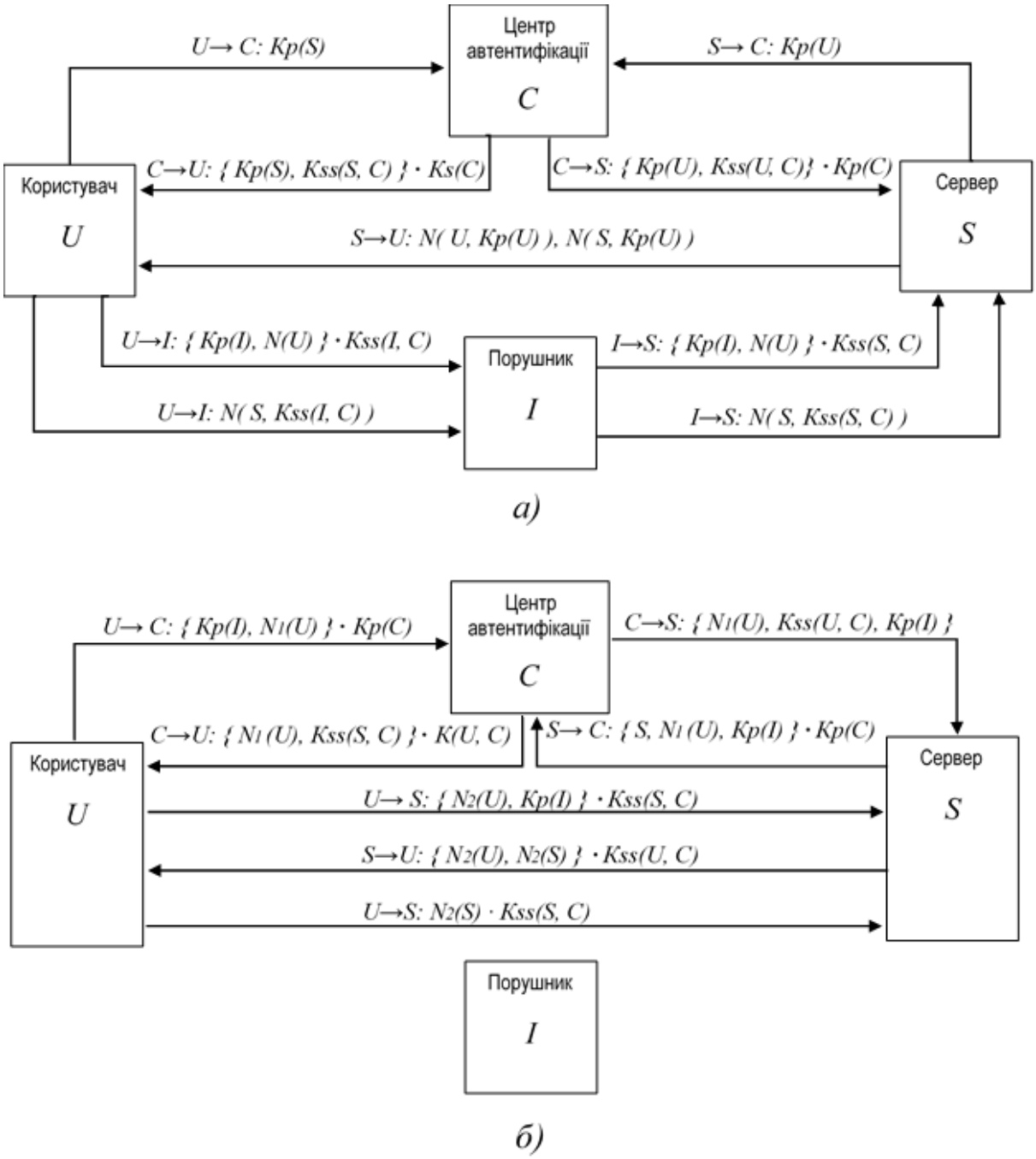


Рисунок 2.2 – Порівняння моделей автентифікації: *а* - базової , *б* - вдосконаленої

Як видно, вже на етапах 1 та 2 (табл. 2.3) новий алгоритм автентифікації не дає порушнику можливість ввести користувача в оману, оскільки на цих етапах відбувається шифрування за допомогою загального ключа з центром

автентифікації. На етапі 3 порушник також не може відправити одноразовий код та маскуватися під користувача, що подає запит на сервер. Відповідно, якщо порушник отримує дані на етапах 5-7, у нього не залишається можливості розшифрувати їх вміст. Вдосконалена модель дозволяє застосовувати рекомендовану стандартом X.509 [63] специфіковану схему автентифікації, засновану на використанні кваліфікованого електронного підпису, міток часу та випадкових чисел. Одностороння автентифікація із застосуванням міток часу:

$$U \rightarrow C: cert(U), t(U), C, p(U)(t(U), C), \quad (2.12)$$

де: t – мітка часу;

$p(U)$ – підпис, згенерований користувачем;

$cert(U)$ – сертифікат відкритого ключа користувача;

Такий запит дозволяє центру автентифікації перевірити правильність мітки часу $t(U)$, отриманий свій ідентифікатор C, та використовуючи відкритий ключ з сертифікату $cert(U)$ користувача, коректність (справжність) кваліфікованого електронного підпису.

Одностороння автентифікація з застосуванням випадкових чисел:

$$C \leftarrow U: r(U), \quad (2.13)$$

$$U \rightarrow C: cert(U), r(U), C, p(U)(r(U), r(C), C), \quad (2.14)$$

де: r – мітка часу.

Центр автентифікації після отримання повідомлення (2.14) від користувача використовує підписане випадкове число $r(U)$ для запобігання атакам з вибіркою відкритого тексту.

Саме підтримка моделлю специфікованої схеми автентифікації стандарту X.509 [63], дозволяє використовувати алгоритми електронного підпису, визначені ДСТУ ETSI TS 119 312:2015 [45] , ДСТУ 4145-2002 [46] та механізми автентифікації згідно ДСТУ ISO/IEC 9798-3:2014 [44], що задовольняє вдосконаленою моделлю вимоги 4-8, 15, що визначені в підрозділі 1.4 даної роботи та забезпечує можливість її практичного впровадження із застосуванням вітчизняних програмних та апаратних засобів криптографічного захисту інформації.

2.3 Вдосконалення моделі доступу до ресурсів

Методи керування доступом. В основі підсистем авторизації лежить формальний метод керування доступом. Прийнято розрізнювати [64] три методи управління доступом: дискреційний (англ. *discretionary access control, DAC*), мандатний (англ. *mandatory access control, MAC*), рольовий (англ. *role-base access control, RBAC*). Дискретним методом керування доступом називають метод управління доступом між поіменованими суб'єктами та пойменованими об'єктами, в яких власник об'єкта сам вирішує, хто має доступ до об'єкта, а також вид доступу. Цей метод керування доступом орієнтований на ідентифікаційну інформацію суб'єкта та асоційований з ним ряд операцій доступу (читання, запис тощо). Така політика може бути реалізована за допомогою: списку доступу (англ. *access control list, ACL*), матриці доступу (англ. *access control matrix, ACM*). Метод простий і поширений у більшості систем захисту інформації. Проблема дискретного методу а цьому, що він забезпечує контроль передачі прав. Суб'єкт із певним правом доступу може передати це право будь-якого іншого суб'єкта без повідомлення власника об'єкта. Мандатний метод управління доступом заснований на ієрархічній класифікації об'єктів та суб'єктів системи. Кожному суб'єкту та об'єкту системи призначається певний ієрархічний рівень безпеки. Рівень безпеки об'єкту характеризує цінність об'єкта (можливі збитки у разі порушення конфіденційності, цілісності та доступності). Кожен об'єкт відповідно до рівня має мітку безпеки (англ. *security label*). Рівень безпеки суб'єкта характеризує ступінь довіри щодо нього. Кожен суб'єкт має допуск до відповідного рівня. На відміну від дискретного методу у мандатному методі користувачі не можуть змінювати стратегію доступу щодо об'єктів системи. При створенні об'єкта власне сама операційна система автоматично призначає йому відповідні атрибути. У цьому сенсі метод називають ще примусовим чи обов'язковим. Формально мандатний метод керування доступом описується моделлю Ла-Падула та моделлю Біба [65, 66]. Поряд із рівнями безпеки мандатний метод допускає використання смислових категорій (областей використання), яких суб'єкти і об'єкти ставляться. Введення смислових категорій дозволяє реалізувати

принцип «належить знати лише те, що належить до посадових обов'язків» (англ. *need-to-know*) [64]. Мандатний метод застосовується при реалізації систем з вищими рівнями довіри, наприклад, які обробляють інформацію з обмеженим доступом. Рольовий метод керування доступом орієнтований на ролі або функції безпеки системи. Наприклад, в системі вводиться активний «рольовий» об'єкт (англ. *organization role*), який виконує деяку чергову роль та, відповідно, має необхідні права доступу до заданим об'єктам системи. У такому разі супровід системи безпеки полягає у призначенні (у разі потреби) відносини еквівалентності між суб'єктами системи та рольовим об'єктом. Використання рольового методу спрощує адміністрування системи (для чергових ролей не потрібно знову визначати права у разі постійної зміни обов'язків користувачів). На окремі ролі може бути накладена деяка семантика, наприклад, заборонено поєднувати привілейовані ролі. Допускається побудова ієрархічних ролей. З точки зору інформаційної безпеки такий метод визнається корисним для зниження небезпечного впливу, що містять широкі повноваження адміністративних ролей (наприклад, роль адміністратора мережі можна поділити на дві окремі ролі: відповідального за відновлення/копіювання системи та відповідального за оперативне функціонування системи). Крім того, рольовий метод дозволяє реалізувати принцип найменших привілеїв. Рольовий метод принципово відрізняється від попередніх тим, що у методі політика безпеки не закріплена та налаштовується у процесі зміни ролей користувачів (та визначення їх прав) за необхідними потребами організації.

Вхідні дані для моделювання. З рис. 2.1 та даних, наведених в табл. 1.1 відомо, що процедура доступу із використанням концепції нульової довіри здійснюється із використанням Azure Active Directory (Azure AD). Вивчення та аналіз технічної документації, яка доступна на офіційному сайті Microsoft, виявили, що в Azure AD використовується модель RBAC (англ. *Role Based Access Control*, управління доступом на основі ролей) у власній модифікації Azure RBAC, яка дозволяє керувати доступом користувачів до ресурсів, включаючи налаштування дозволів на виконання операцій з цими ресурсами та визначення

областей доступу. Технічна документація Azure RBAC, що доступна на офіційному сайті Microsoft, містить деталізовану інформацію про механізми реалізації. Модель Azure RBAC планується покращити видозміненням для застосування її функцій та можливостей в забезпеченні архітектури нульової довіри іншим продуктом-аналогом «IT-Enterprise» українського виробника, комплекс засобів якого має експертний висновок за результатами державної експертизи у сфері технічного захисту інформації, що відповідає вимогам, зазначеним в підрозділі 1.4 даної роботи. ERP-система «IT-Enterprise» інтегрується з системою безпеки Windows, підтримує роботу з особистими ключами на захищених носіях з використанням JavaScript-бібліотеки та з використанням агенту підпису, підтримує двофакторну автентифікацію та використовує рольове розмежування доступу до ресурсів. Технічна документація з детальною інформацією доступна на офіційному сайті виробника. Наведених даних достатньо для дослідження та складання моделі доступу до ресурсів з використанням понятійного апарату, що запропонований в [67], досвіду подібного моделювання та методик, що використовується в [64, 65, 70-74].

Дослідження базової моделі RBAC. В якості базової моделі доцільно застосувати формальні вирази рольових основ управління доступу стандартизованої Національним інститутом стандартів та технологій (NIST) США моделі RBAC [75]. З метою розрізнення та наступного порівняння позначимо базову модель як $RBAC_0$. Базова модель управління доступом на основі ролей $RBAC_0$ у формалізованому представленні задається наступним набором елементів:

$$<U, R, P, S, UA(U), PA(R), user(S), roles(S)>, \quad (2.15)$$

де: U – множина користувачів;

R – множина ролей користувачів;

P – множина прав доступу користувачів;

S – множина сесій (сеансів) користувачів;

UA – функція, що визначає для кожного користувача множину ролей, на які він може бути авторизований;

PA – функція, що визначає для кожної ролі множину прав доступу;

user – функція, що задає для кожної сесії користувача, від імені якого вона авторизована;

roles – функція, що задає для кожного користувача множину ролей.

Функція, що визначає для кожного користувача множину ролей, на які він може бути авторизований, задається як:

$$UA: U \rightarrow 2^R \tag{2.16}$$

Функція, що визначає для кожної ролі множину прав доступу задається як:

$$PA: R \rightarrow 2^P \tag{2.17}$$

Функція, яка задає користувача для кожної сесії, від імені якого вона авторизована, визначається як:

$$user: S \rightarrow U \tag{2.18}$$

Функція, що задає для кожного користувача множину ролей, на які він авторизований у даній сесії, задається як:

$$roles: S \rightarrow 2^R \tag{2.19}$$

В $RBAC_0$ для функції $PA: R \rightarrow 2^P$ (по суті множина повноважень для ролі) задається правило $\forall p \in P,\ \exists r \in R$ за якого $p \in PA(r)$.

В моделі $RBAC_0$ для функції $roles: S \rightarrow 2^R$ задається правило, що в сесії кожний момент часу $\forall s \in S$ повинна виконуватися умова $roles(s) \subseteq UA(user(s))$.

Множина ролей сесії обмежена множиною ролей користувача з тими, що успадковуються ним з сесій, на які він може бути авторизований

$$s \in S \Rightarrow roles(s) \subseteq user(s)\ user(s) \subseteq UA \tag{2.20}$$

На рисунку 2.3 представлена схема базової моделі управління доступом на основі ролей $RBAC_0$, яка відображає набір її елементів, взаємозв'язок між ними та функціями:

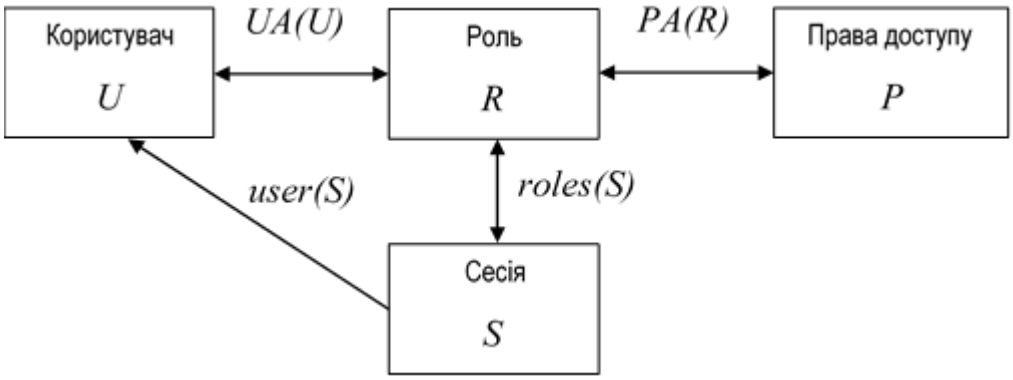


Рисунок 2.3 – Схема моделі $RBAC_0$

Аналіз базової моделі $RBAC_0$. Базова модель управління доступом на основі ролей $RBAC_0$ не враховує специфіку функціонування веб-додатків, зокрема, ієрархічну організацію запитів та посилань. $RBAC_0$ обмежена у способах завдання умов доступу. Також в базовій моделі рольового управління доступом передбачається, що множини *U, R, P* та функції *PA, UA* з часом не змінюються. Множина ролей, на які авторизується користувач протягом однієї сесії, модифікується самим користувачем. При цьому відсутні механізми, що дозволяють одній сесії активізувати іншу сесію. Всі сесії активізуються тільки користувачем. Вірогідно, що вказані недоліки змусили компанію Microsoft застосовувати власну модифікацію Azure RBAC.

Вивчення моделі Azure RBAC. З метою розрізнення та наступного порівняння позначимо цю модель як $RBAC_A$. В $RBAC_A$ (як видно з рис. 2.1) при автентифікації користувача застосовується багатофакторна автентифікація, тому використовуються обидві пари токену *Tk* : (ім’я, пароль) та (сертифікат відкритого ключа, особистий ключ). Також для опису $RBAC_A$ необхідно додати додаткові елементи, які ураховують специфіку функціонування веб-додатків.

Модель управління доступом на основі ролей $RBAC_A$ у формалізованому представлені можна задати наступним набором елементів:

$$<U, R, P, S, Tk, Rq, RqP, UA(U), PA(R), RqA(P), RqPA(P), user(S), roles(S), token(Tk), requests(S)>, \quad (2.21)$$

де: *U* – множина користувачів;

R – множина ролей користувачів;

P – множина прав доступу користувачів;

S – множина сесій (сеансів) користувачів;

Tk – токен (англ. *token*), набір атрибутів користувача, який дозволяє здійснювати його автентифікацію в системі: пара (ім’я, пароль) або пара (сертифікат відкритого ключа, особистий ключ);

Rq –запит (англ. *request*), набір інформації що пересилається користувачу сервером по протоколу HTTP, який в свою чергу містить набір заголовків, унікальний ідентифікатор ресурсу, набір параметрів (ім’я, значення) та тіло запиту.

RqP – параметр запиту, набір пар (ключ, значення) запиту HTTP, який належить запиту *Rq* та використовується для передавання додаткових даних в запиті;

UA(U) – функція, яка визначає для кожного користувача множину ролей, на які він може бути авторизований;

PA(R) – функція, яка визначає для кожної ролі множину прав доступу;

RqA(P) – множина параметрів запиту;

RqPA(P) – функція, яка відображає множину параметрів запиту;

user(S) – функція, яка задає користувача для кожної сесії, від імені якого вона авторизована;

roles(S) – функція, що задає для кожної для користувачів множину ролей.

В $RBAC_A$ параметр запиту *RqP* належить запиту *Rq*.

Функцію *RqA*, яка відображає права доступу на множину запитів, можна відобразити як:

$$RqA\colon P \rightarrow 2^{Rq} \tag{2.22}$$

Функція *RqPA*, що відображає дозволи на множину параметрів, задається як:

$$RqPA\colon P \rightarrow 2^{RqP} \tag{2.23}$$

На рисунку 2.4 представлена схема моделі управління доступом на основі ролей $RBAC_A$, яка відображає набір її елементів, взаємозв’язок між ними та функціями:

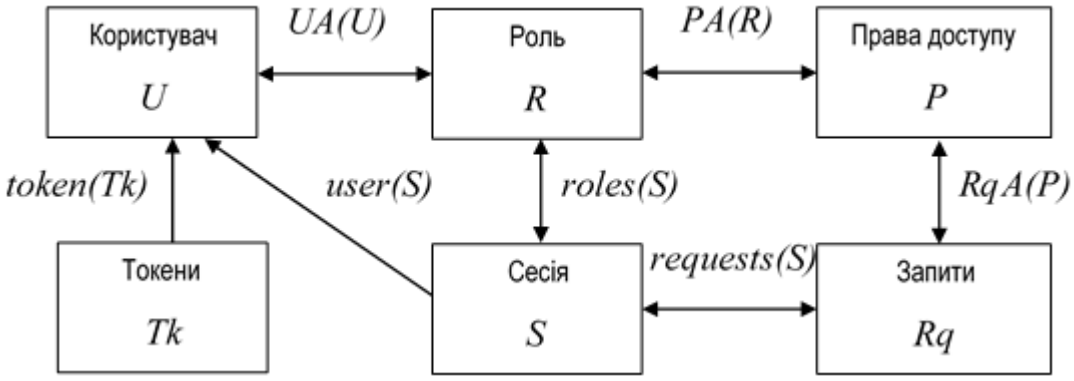


Рисунок 2.4 – Схема моделі RBAC$_A$

Аналіз моделі RBAC$_A$. Модифікована рольова модель RBAC$_A$ доповнює RBAC$_0$ такими елементами: токен (t*oken*), запит (*request*). Токен (*Tk*) являє собою набір атрибутів користувача, що дозволяють здійснити його автентифікацію в системі. При автентифікації користувача застосовується багатофакторна автентифікація, тому використовуються обидві пари токену *Tk:* (ім'я, пароль) та (сертифікат відкритого ключа, особистий ключ). Запит (*Rq*) являє собою набір інформації, яка пересилається між користувачем та сервером за протоколом HTTP(S). Модель RBAC$_A$ враховує специфіку роботи веб-додатків та дозволяє розмежовувати доступ на основі шляхів запиту (URI). Однак її впровадження та використання в інформаційних системах, що не використовують Azure Active Directory, неможливе, тому що RBAC$_A$ не дозволяє виконувати розмежування з використанням параметрів запитів, це здійснюється в інший спосіб.

Вдосконалення моделі RBAC$_A$. З метою розрізнення та наступного порівняння позначимо цю модель як RBAC$_B$. Для застосування можливості розмежування доступу з використанням параметрів запитів, модель RBAC$_A$ необхідно доповнити додатковими елементами, які ураховують специфіку функціонування веб-додатків без використання рішень технології Azure Active Directory.

Нову модель можна описати наступним набором елементів:

$$<U, R, P, S, Tk, Rq, RqP, RqH, RH, UA(U), PA(R), RqA(P), RqPA(P), user(S), roles(S), token(Tk), requests(S), params(Rq)>, \quad (2.24)$$

де: U – множина користувачів;

R – множина ролей користувачів;

P – множина прав доступу користувачів;

S – множина сесій (сеансів) користувачів;

Tk – токен (англ. *token*), набір атрибутів користувача, який дозволяє здійснювати його автентифікацію в системі: пара (ім’я, пароль) або пара (сертифікат відкритого ключа, особистий ключ);

Rq –запит (англ. *request*), набір інформації що пересилається користувачу сервером по протоколу HTTP, який в свою чергу містить набір заголовків, унікальний ідентифікатор ресурсу, набір параметрів (ім’я, значення) та тіло запиту.

RqP – параметр запиту, набір пар (ключ, значення) запиту HTTP, який належить запиту *Rq* та використовується для передавання додаткових даних в запиті;

RH – ієрархія ролей;

RqH – ієрархія запитів;

UA(U) – функція, яка визначає для кожного користувача множину ролей, на які він може бути авторизований;

PA(R) – функція, яка визначає для кожної ролі множину прав доступу;

RqA(P) – множина параметрів запиту;

RqPA(P) – функція, яка відображає множину параметрів запиту;

user(S) – функція, яка задає користувача для кожної сесії, від імені якого вона авторизована;

roles(S) – функція, що задає для кожної для користувачів множину ролей;

params(Rq) – функція, яка відображає запити на множину параметрів запиту.

Функція *params(Rq)* задається як:

$$params: Rq \rightarrow 2^{RqP} \qquad (2.25)$$

В новій моделі параметр запиту *RqP* належить запиту *Rq*, причому один запит може мати кілька параметрів. Запит належить сесії, в рамках однієї сесії може виконуватися кілька запитів. На множину запитів необхідно впровадити

правило бінарного відношення включення, яке дозволить впорядкувати запити згідно з ієрархією. Фактично, ієрархія запитів *RqH* –це співвідношення включень, що задане на множині запитів *Rq*.

Для уникнення випадкового або несанкціонованого блокування доступу в ієрархії запитів необхідно виконання наступних умов:

$$PA(r') \subseteq PA(r), \tag{2.26}$$

$$PqA(p') \subseteq PqA(p), \tag{2.27}$$

де: роль r успадковує роль r' у множині параметрів запитів *RqA(P)*.

На множині ролей заданий частковий порядок $RH \subseteq R \times R$, що визначає успадкування ролей: роль r успадковує роль r' виключно при $(r, r') \in RH$.

Виконання умови (2.26) забезпечує поширення дозволів ролей углиб по ієрархії запитів. Друга умова (2.27) забезпечує несуперечність завдання набору запитів, які можна виконувати у межах заданих дозволів.

На рисунку 2.5 представлена схема моделі управління доступом на основі ролей RBACв, яка відображає набір її елементів, взаємозв'язок між ними та функціями:

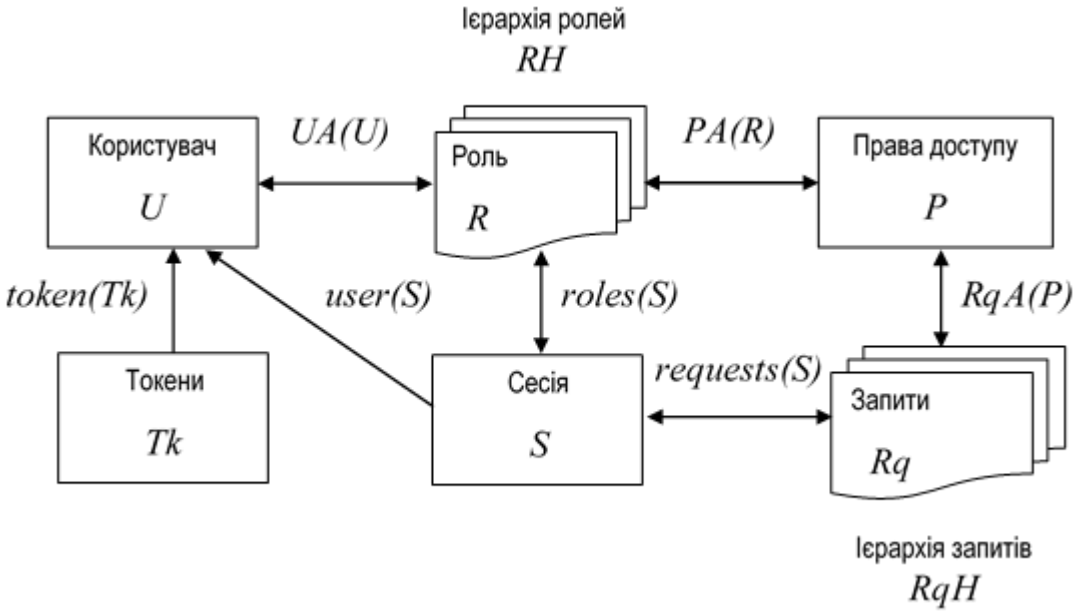


Рисунок 2.5 – Схема вдосконаленої моделі RBACв

Аналіз вдосконаленої моделі RBAC$_B$. Вдосконалена рольова модель доступу RBAC$_B$ допускає її впровадження в будь-яких інформаційних системах та дозволяє виконувати розмежування доступу на підставі параметрів запитів без використання технологій та рішень Azure Active Directory. Для множини запитів впроваджується правило бінарного відношення включення, яке дозволяє впорядкувати запити згідно з ієрархією запитів *RqH*. Для забезпечення бінарного відношення, для множини запитів *Rq* створюється ієрархія ролей *RH*, заснована на множині ролей *R* та обмеженні функцій *UA(U), roles(S), PA(R).* Для автентифікації користувача залишена багатофакторна автентифікація з використанням обох пар токену *Tk*: (ім'я, пароль) та (сертифікат відкритого ключа, особистий ключ).

В моделі RBAC$_B$, на відміну від RBAC$_0$, процес введення ролей призводить зміни послідовності двоетапної організації системи розмежування доступу:

1) створення ролей та визначення їх повноважень (прав доступу до об'єктів);

2) призначення ролей користувачам системи.

Суттєвою відміною RBAC$_B$ від RBAC$_A$ є введення ієрархічної організації системи ролей *RH* та введення ієрархії запитів *RqH*. Такий підхід віддзеркалює реальні організаційно-технологічні та організаційно-управлінські схеми на підприємствах та в організаціях: посади співробітників підприємств, організацій у більшості випадків утворюють ієрархічно підлеглі структури. Відповідно RBAC$_B$ легко впроваджується на основі «ролей-посад». Проте такий підхід має складність реалізації у випадку складної ієрархічної структури посадових осіб (як наприклад, в органах місцевого самоврядування), особливо при організації колективного доступу до ресурсів в складній IT-системі з великою кількістю користувачів та великою кількістю ресурсів. В дослідженнях [65, 66, 76] визначається складність проектування в подібних системах доступу робочих груп та необхідність застосування при цьому додаткових теоретико-графових методів або просторово-векторних моделей, що й буде ураховано при розробці моделі політики безпеки доступу.

На рис. 2.2 представлено порівняння базової моделі RBAC$_0$, модифікованої моделі RBAC$_A$ та розробленої вдосконаленої моделі RBAC$_B$:

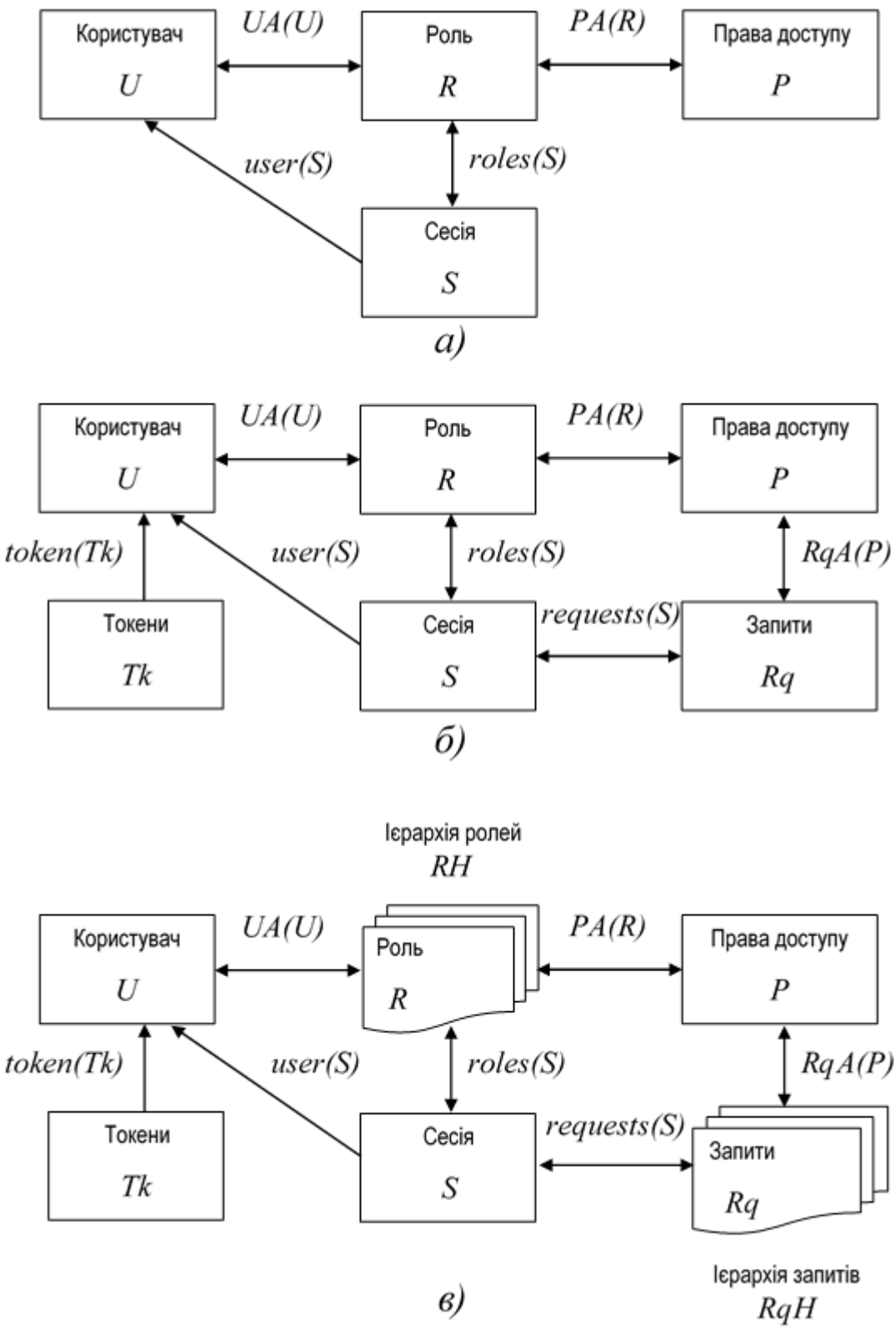


Рисунок 2.6 – Порівняння моделей RBAC:

а - базової , *б* - Azure AD, *б* – вдосконаленої

2.4 Вдосконалення моделі політики безпеки доступу

Вхідні дані для моделювання. Під політикою безпеки доступу в загальному випадку прийнято розуміти правила розмежування доступу та порядок надання такого доступу - сукупність правил, що регламентують права доступу суб'єктів (користувачі, процеси, кінцеві пристрої) до об'єктів (ресурсів) у певній ІТ-системі. Із урахуванням того, що одним із завдань даного дослідження є впровадження концепції та принципів архітектури нульової довіри, при створенні моделі політики безпеки доступу необхідно врахувати аспекти 1-10, принципи 1-7, застереження 1-3, описані в підрозділі 1.3, розроблені модель автентифікації та модель доступу до ресурсів, описані в підрозділах 2.2 та 2.4 даної роботи із збереженням понятійного апарату, що використаний при побудові цих моделей.

Умови моделювання. Так як відомо, що практичне впровадження моделі безпеки доступу до ресурсів буде здійснюватися із використанням інструментарію конкретного програмного продукту ERP-системи «IT-Enterprise», що надає механізми реалізації багатофакторної автентифікації та використовує рольове розмежування доступу до ресурсів, модель доцільно побудувати максимально простою (при достатній для вирішення завдань функціональності) та інтуїтивно зрозумілою. При моделюванні використовується досвід подібного моделювання та методики, що запропоновані в [64, 65, 77-85].

Розробка вдосконаленої моделі. В дослідженнях [64, 65, 77] для визначення рівнів повноважень запропоновано використання теоретико-графової формалізації рольової політики розмежування доступу за якою ієрархія ролей *RH* співвідноситься з рольовим графом G (рис. 2.7):

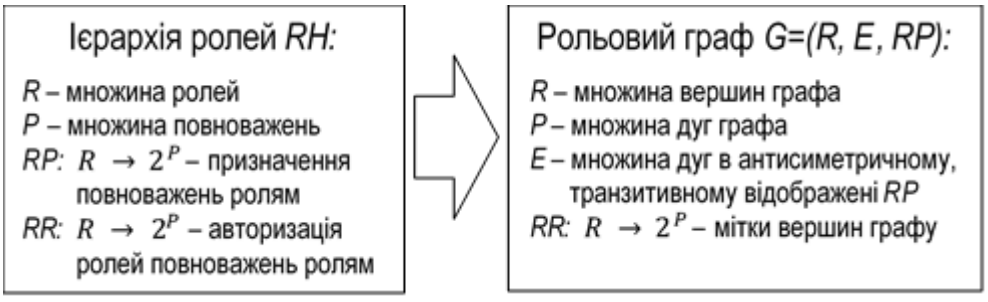


Рисунок 2.7 – Теоретико-графове представлення ієрархії ролей

Джерело: [77]

Розглядаються такі елементи моделі, як ієрархія ролей *RH*, яка задається множиною ролей:

$$RH = \{r_1, \ldots, r_n\}, \quad (2.28)$$

де: $r_1, \ldots, r_n$ – множина ролей.

При цьому, якщо $r_2 \leq r_1$, то r_1 знаходиться за ієрархією ролей «вище» за r_2. Таким чином ієрархія ролей *RH* може бути заданою у вигляді орієнтованого графу:

$$G = (R, E, RP, RR), \quad (2.29)$$

де: *R* – множина вершин графу;

E – множина дуг в антисиметричному транзитивному відображені *RP*;

RP – множина дуг графу;

RR – мітки вершин графу.

Орієнтований граф застосовують побудовою дерева ролей (рис. 2.8). Такий метод широко застосовується в практичній діяльності [80-82] .

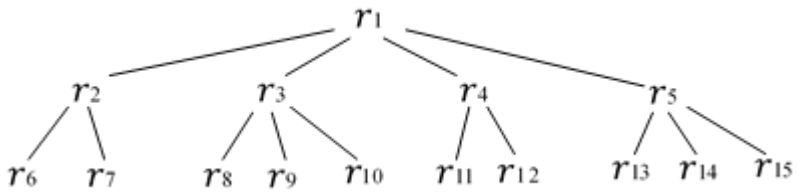


Рисунок 2.8 – Приклад побудови дерева ролей

Джерело: [64, 77]

В нашому випадку пропонується видозмінити побудову дерева ролей, як запропоновано (враховуючи новизну такого рішення) в [64] та доповнити орієнтовний граф *G* (2.26) новим елементом - множиною повноважень *P*:

$$P = \{p_1, \ldots, p_n\}, \quad (2.30)$$

де: $p_1, \ldots, p_n$ – множина ролей.

Це дозволяє доповнити та видозмінити дерево ролей (рис. 2.8). В розширеному дереві ролей (рис. 2.9) листові вузли будуть асоційовані не з ролями, а з повноваженнями. За практичної необхідності, при надані доступу до ресурсу, повноваження можуть бути замінені привілеями.

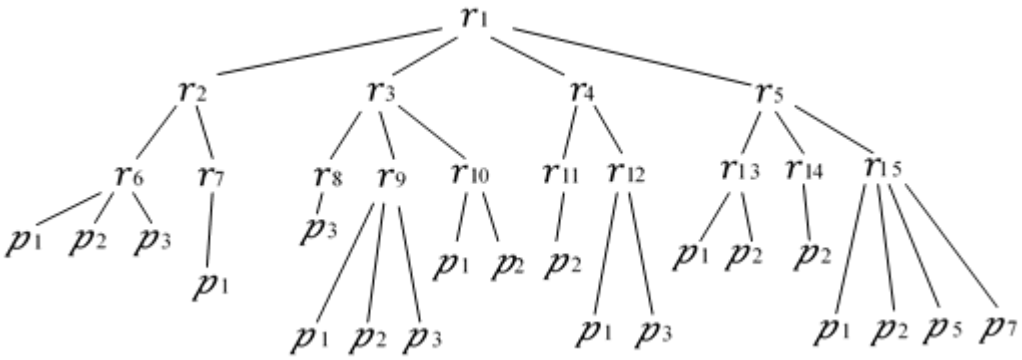


Рисунок 2.9 – Розширене повноваженнями дерево ролей

Джерело: [64]

Аналіз вдосконаленої моделі політики безпеки доступу. Сутність розглянутого рішення полягає в поєднанні відомих методів аналізу ієрархій та побудови рольового дерева системи розмежування доступу. Така модель політики безпеки дозволяє вирішити декілька завдань при реалізації механізму доступу до ресурсів.

По-перше, рішення може бути застосоване для визначення ймовірності реалізації загроз інформаційній безпеці через уразливості, що породжуються структурою ролей політики розмежування доступу:

1) чим більше повноважень містить роль, тим вище ймовірність атаки (спроби несанкціонованої авторизації) на цю роль, тим більше рівні критичності повноважень, зіставлених у ролі;

2) чим частіше зустрічається повноваження у наборах повноважень ролей, тим вища ймовірність його несанкціонованого використання, тим більший рівень критичності;

3) чим ближче роль до вершини ієрархії, тим вища ймовірність атаки на цю роль, тим більші рівні критичності повноважень, зіставлених ролі.

Наявність у системі повноважень, рівень критичності яких перевищує деяке граничне значення, сигналізує про необхідність реструктуризації рольової ієрархії з метою зменшення цих показників.

По-друге, такий підхід дозволяє користувачу разом з роллю отримувати певний набір (список) повноважень, закріплених за цією роллю, що дозволяє в цілях практичного застосування легко з’ясовувати:

1) скільки та які ролі може бути призначено одному користувачеві;

2) скільки та які повноваження в одній ролі може бути призначено користувачеві;

3) скільки та які ролі може задіяти користувач в одному сеансі роботи з системою (на які ролі може бути авторизовано користувач);

4) чи можливе делегування (передача) повноважень від одних ролей іншим ролям.

Перевагою такої моделі рольового підходу є можливість поділу обов'язків, простота адміністрування та застосування ієрархії ролей, на відміну від застосування матриць прав доступу, що запропоновані в [83] та заповнення яких є процесом, затратним за часом. Проте недоліком запропонованої рольової моделі безпеки є неможливість зміни набору повноважень, що відповідає ролі, під час сеансу, зав'язаного на цій ролі.

Визначена модель політики доступу дозволяє забезпечити реалізацію побудованої моделі доступу до ресурсів із застосуванням вдосконаленої моделі автентифікації, на концептуальних принципах архітектури нульової довіри, оскільки забезпечує системотехнічний підхід, що включає вирішення наступних найважливіших завдань:

1) вибір базових принципів архітектури захищеної системи, що визначають механізми реалізації засобів та методів захисту інформації;

2) підтвердження властивостей (захищеності) системи, шляхом формального доказу дотримання політики безпеки (вимог, умов, критеріїв);

3) складання формальної специфікації політики безпеки.

Запропонована модель політики доступу ураховує особливості, задані у вхідних даних та може бути практично реалізована із використанням інструментарію ERP-системи «IT-Enterprise», вказаної в умовах моделювання.

Висновки до розділу 2

Уточнено сутність процедур автентифікація та управління доступом з позицій визначення цих термінів NIST 800-207 та X.805.

Визначено, що створення ефективної процедури автентифікація та управління доступом, як заходів захисту, складне технічне завдання, для вирішення якого необхідно застосувати невід'ємну складову системного аналізу – моделювання.

Акцентовано увагу, що для побудови моделей автентифікації, управління доступом та політики безпеки з використанням принципів 1-7 концепції архітектури нульової довіри, описаних в підрозділі 1.3 даної роботи, необхідно сформувати вхідні дані. Достовірним джерелом таких даних визначена публікація NIST 1800-35B, що описує порядок впровадження архітектури нульової довіри та наводить конкретні практичні приклади такого впровадження.

З'ясовано склад програмного забезпечення, що використане для практичної реалізації моделі доступу та автентифікації з нульовою довірою згідно опису практичної реалізації доступу та автентифікації в NIST 1800-35B.

Проведено вивчення та аналіз технічної документації, що доступна на офіційних сайтах розробників програмних засобів, з метою дослідження технічних характеристик програмних засобів, їх властивостей, особливостей використання для сформування вхідних даних для моделювання.

Проведено дослідження програмного забезпечення із застосуванням методів вивчення аналога (прототипу) та еталонного оцінювання (benchmarking) для доповнення вхідних даних для моделювання.

Сформовано вхідні дані та умови для моделювання кожної моделі окремо.

Побудовано базову модель автентифікації у вигляді формалізованого представлення з метою введення понятійного апарату, проведено її аналіз, виявлено характерні недоліки, з'ясовано, що на сьогоднішній день існує методика обходу захисту реальних систем, побудованих на основі базової моделі.

Проведено моделювання атаки на модифіковану модель, досліджено механізм обходу захисту, з'ясовано можливість захисту.

Вдосконалено модель автентифікації, аналіз якої показав ефективність роботи цієї моделі в порівнянні з базовим та модифікованим варіантами, які були взяті за основу.

Доведено, що вдосконалена модель автентифікації задовольняє вимогам 4-8, 15, що визначені в підрозділі 1.4 даної роботи та забезпечує можливість її практичного впровадження із застосуванням вітчизняних програмних та апаратних засобів криптографічного захисту інформації.

Проаналізовано відомі методи керування доступом: дискреційного (відомого як DAC), мандатного (відомого як MAC), рольового (відомого як RBAC) у форматі короткого опису та порівняння.

Сформовано вхідні дані та умови для моделювання моделей рольового доступу.

Досліджено базову модель рольового доступу $RBAC_0$, наведено її формалізоване представлення, визначені функції, порядок застосування, особливості використання, проведено аналіз, виявлено недоліки.

Розглянуто модель рольового доступу $RBAC_A$ (відому як Azure RBAC, модифікацію базової моделі $RBAC_0$), наведено її формалізоване представлення, визначені функції, порядок застосування, особливості використання, проведено аналіз, виявлено недоліки.

Вдосконалено модель рольового доступу $RBAC_B$, проведено її аналіз та порівняння з моделями $RBAC_0$, $RBAC_A$, визначено її переваги та можливі складності у практичному застосуванні.

Уточнено зміст поняття політики безпеки доступу, сформовано вхідні дані та визначено умови для вдосконаленої моделі політики безпеки доступу.

Вдосконалено модель політики безпеки доступу, яка враховує основні принципи архітектури нульової довіри, із використанням запропонованого раніше новітнього способу поєднання двох відомих методів: аналізу ієрархій та побудови рольового дерева розмежування доступу на основі теоретико-графового представлення ієрархії ролей; зазначено переваги такої моделі для практичного застосування.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНИХ МОДЕЛЕЙ

3.1 Пошук програмних засобів-аналогів вітчизняного виробництва

Вхідні дані. З рис. 2.1 відомо, що процедури автентифікації та доступу із застосуванням концепції нульової довіри здійснюються із використанням програмних та апаратних засобів, перелік та функції яких зазначені в таблиці 1.1. В нашому випадку, програмне забезпечення та апаратні засоби, їх функції, повинні відповідати нормам чинного законодавства України у сферах захисту інформації, захисту державних інформаційних ресурсів, кіберзахисту об'єктів критичної інфраструктури, здійснення технічного та криптографічного захисту інформації, сфері електронних довірчих послуг, обов'язкові вимоги яких визначені в підрозділі 1.4 даної роботи.

Результати пошуку засобів-аналогів. Пошук проведено із застосуванням методу вивчення аналога (прототипу) та методу еталонного оцінювання (англ. *benchmarking*) із застосуванням методик, що описані в [86-89].

Перелік вибраних програмних засобів, наведено в таблиці 3.1:

Таблиця 3.1 – Програмні засоби для практичної реалізації моделей автентифікації, доступу та політики безпеки з архітектурою нульової довіри

№ з/п	Найменування програмного засобу	Виробник
1	Комп'ютерна програма системи управління підприємством «IT-Enterprise»	НВП «Інформаційні технології» (м. Київ, Україна)
2	Комплекс програмний захисту SAP-системи «ІІТ Захист SAP-системи»	ПрАТ «Інститут інформаційних технологій» (м. Харків, Україна)
3	Комплекс програмний користувача центру сертифікації ключів «ІІТ Користувач ЦСК-1»	ПрАТ «Інститут інформаційних технологій» (м. Харків, Україна)
4	Комплекс програмний клієнта захисту мережних з'єднань «ІІТ Захист з'єднань-2. Клієнт захисту з'єднань»	ПрАТ «Інститут інформаційних технологій» (м. Харків, Україна)

Обґрунтування вибраних рішень. Вибрані програмні засоби мають позитивний експертний висновок за результатами державної експертизи у сфері технічного або криптографічного захисту інформації [90-92], відповідно

реалізують криптоалгоритми та криптопротоколи, які є національними стандартами в обсязі функцій безпеки згідно з [48], відповідають умовам, визначеним в [47, п.п 44-28] та задовольняють обов'язкові вимоги, визначені в підрозділі 1.4 даної роботи.

Комп'ютерна програма системи управління підприємством «IT-Enterprise» є ERP-системою з широким та гнучким набором функцій та інструментів: інтегрується з системами безпеки Windows, підтримує роботу з кваліфікованими електронними підписами з використанням JavaScript-бібліотеки, з використанням агенту підпису, підтримує двофакторну автентифікацію, використовує рольове розмежування доступу до ресурсів за моделями RBAC, маючи для цього вбудовані програмні модулі ідентифікації, автентифікації та розмежування доступу.

Проте, в ході вивчення технічної документації та експертного висновку на цей програмний продукт, з'ясовано, що модуль ідентифікації та автентифікації здійснює автентифікацію windows-клієнта із використанням захищеного механізму за технологію безпечного з'єднання між клієнтом (комп'ютером користувача) та сервером на основі протоколу автентифікації Kerberos [90, п. 6.1.16], так само як Azure AD, для заміни якого й передбачається використання «IT-Enterprise».

Саме вразливість протоколу автентифікації Kerberos спонукала розробку вдосконаленої моделі автентифікації, що описана в підрозділі 2.2 цієї роботи.

Проста заміна вказаного протоколу неприйнятна з причини порушення ліцензійної угоди на використання програмного продукту та вимог до умов використання об'єкта експертизи, зазначених в експертному висновку [90, п. 8.2].

Проте можлива зміна конфігурації налаштувань модулів «IT-Enterprise», за якої можливо політику цілісності при обміні, що реалізується комплексом засобів захисту «IT-Enterprise», передати іншому програмному засобу. Таким засобом обраний програмний комплекс користувача центру сертифікації ключів «ІІТ Користувач ЦСК-1» (п. 3 табл. 3.1), який згідно експертного висновку [91] відноситься до програмних засобів криптографічного захисту інформації.

Таким чином, здійснення зміни конфігурації налаштувань та додавання додаткового програмного засобу, забезпечить автентифікацію (крім процедури формування сертифікатів відкритих ключів та списку відкликаних сертифікатів, що використовуються для механізму кваліфікованого електронного підпису) користувачів та цілісність при обміні інформацією, що зберігається в базах даних, двома способами:

- шляхом вироблення імітовставки за алгоритмом ДСТУ ГОСТ 28147:2009, який реалізовується програмною бібліотекою програмного комплексу «ІІТ Користувач ЦСК-1» (замість протоколу TLS (версії 1.2) на базі стандартних засобів забезпечення безпеки Microsoft .Net Framework 2.0/4.0);

- або шляхом формування електронного підпису за алгоритмом ДСТУ 4145-2002, що також реалізується програмною бібліотекою програмного комплексу «ІІТ Користувач ЦСК-1» (що й потрібно для практичної реалізації моделі).

Таке рішення відповідає результатам аналізу розробленої вдосконаленої моделі автентифікації, зазначеної в підрозділі 2.2 та задовольняє вимоги, визначені в підрозділі 1.4 даної роботи.

Для забезпечення автентифікації та доступу користувачів, розташованих в розподілених сегментах реальної інформаційно-комунікаційної системи, необхідно встановлення на їх робочі станції програмного комплексу клієнта захисту мережних з’єднань «ІІТ Захист з’єднань-2. Клієнт захисту з’єднань» (п. 4 табл. 3.1).

Процедуру формування сертифікатів відкритих ключів та списку відкликаних сертифікатів, що використовуються для механізму кваліфікованого електронного підпису, забезпечить незалежна третя сторона, якою виступає кваліфікований надавач електронних довірчих послуг, включений до Довірчого списку [62], що задовольняє вимоги, визначені в [44].

Програмний комплекс захисту SAP-системи «ІІТ Захист SAP-системи» (п. 2 табл. 3.1) обирається як альтернатива ERP-системі «IT-Enterprise» з метою порівняння їх можливостей та, при необхідності, продовження експерименту з реалізації моделей на його базі.

3.2 Опис інфраструктури, умови впровадження

Практична реалізація розроблених моделей автентифікації, доступу до ресурсів та політики безпеки доступу (із застосуванням концепції архітектури нульової довіри) з метою перевірки їх працездатності та ефективності здійснювалась в департаменті інформаційних технологій Вінницької міської ради.

Практична реалізація розроблених моделей здійснювалась на кількох реальних інформаційно-комунікаційних системах, об'єднаних ERP-системою «IT-Enterprise» (далі - ERP-система). Для порівняння можливостей була створена альтернативна експериментальна платформа: на реальну локалізовану систему SAP R/3 встановлений програмний комплекс захисту «ІІТ Захист SAP-системи».

Опис функціонування ERP-системи. ERP-система складається з трьох компонентів, пов'язаних через клієнт-серверну архітектуру: рівень баз даних, рівень застосунків, рівень користувачів.

Логічна структура ERP-системи «IT-Enterprise», а також додаткове програмне забезпечення, що бере участь у взаємодії, наведена на рисунку 3.1:

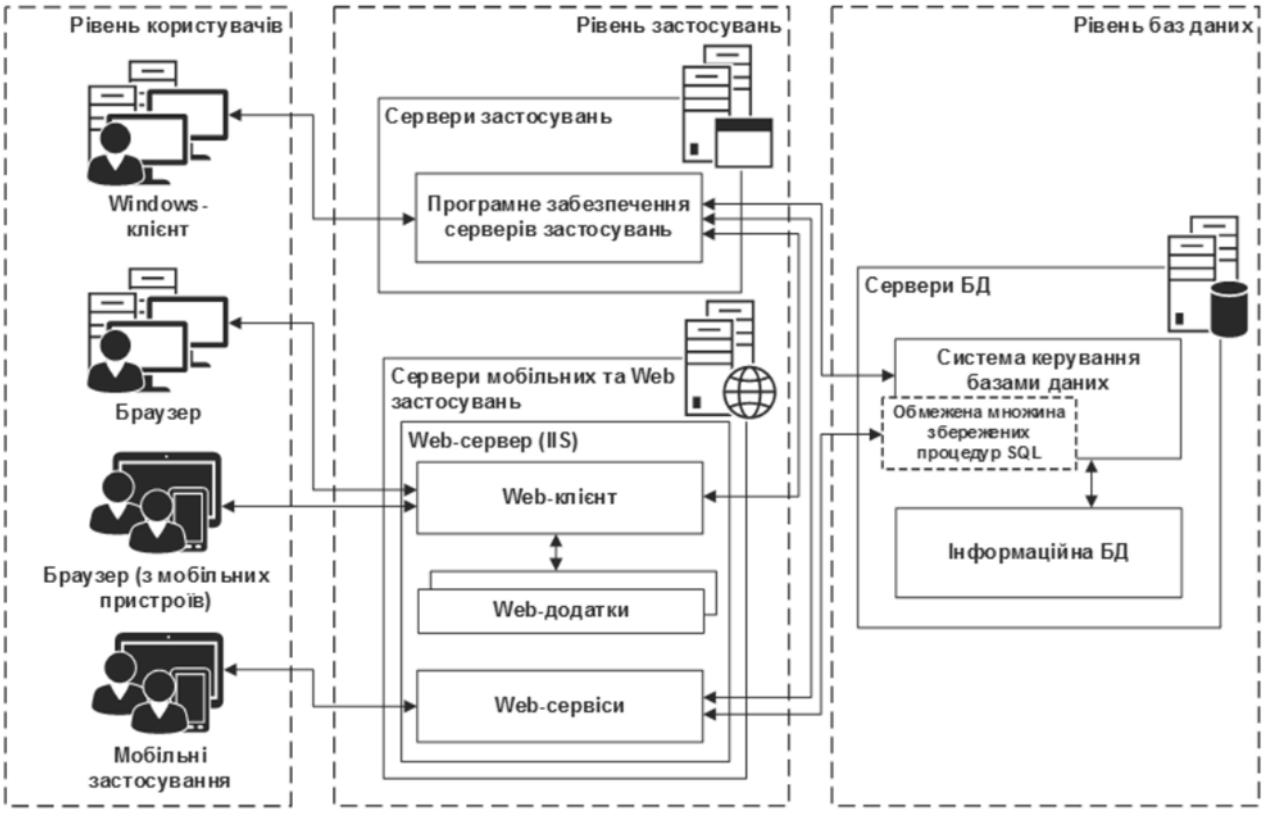


Рисунок 3.1 – Логічна структура ERP-системи «IT-Enterprise»

Джерело: [90]

Рівень баз даних: інформаційна база даних зберігається в системі управління базами даних (далі - СКБД). В якості СКБД використовуються: Microsoft SQL Server, Oracle Database.

Рівень серверів застосувань: на сервері застосувань зосереджено всю логіку обробки інформації. Сервер застосувань формує запити на сервер БД, виконує розрахунки та надсилає результати розрахунків користувачу. Кількість серверів застосувань не обмежується. Обробка інформації здійснюється за допомогою програмного забезпечення сервера застосувань. Web-клієнт реалізовано у вигляді web-застосування, яке надає інтерфейс для взаємодії з ресурсами ERP-системи у браузері користувача. Обробка інформації за допомогою web-клієнта здійснюється у взаємодії з серверами застосувань, а саме, web-клієнт надсилає запити серверам застосувань, ініціює виконання розрахунків на сервері застосувань та відображає результати обробки користувачу. Множина функціональних можливостей, що надається користувачу web-клієнта, еквівалентна множині функцій windows-клієнта, за винятком наявності у користувача web-клієнта додаткового шляху автентифікації за допомогою особистого ключа кваліфікованого електронного підпису (далі - ЕЦП).

Рівень користувачів: доступ користувачів до можливості виклику застосунків визначається адміністратором ERP-системи. Web-сервер (штатне програмне забезпечення ОС Windows серверного типу), яке розгортається в рамках ролі «Веб-сервер (IIS)» та призначено для обробки у взаємодії з web-клієнтом та web-сервісами «IT-Enterprise» запитів за протоколами HTTP/HTTPS, що надходять від браузерів та мобільних застосувань, відповідно. При обробці інформації за допомогою мобільних застосувань та програмних засобів від інших розробників, функціональні можливості користувача обмежуються множиною функцій, які стають доступні користувачу після проходження процедури ідентифікації та автентифікації, а також набором завдань та дозволів, які закладено у логіку роботи застосування.

Загальна схема реалізації комплексу засобів захисту ERP-системи «IT-Enterprise» наведена на рис. 3.2:

Рисунок 3.2 – Загальна схема реалізації комплексу засобів захисту ERP-системи

Джерело: [90]

Функції безпеки, що надаються комплексом засобів захисту, реалізовані у наступних модулях ERP-системи: модуль ідентифікації і автентифікації, модуль розмежування доступу, модуль балансування навантаження, модуль аудиту, модуль оперативного моніторингу роботи користувачів, модуль контролю цілісності та самотестування. Модуль ідентифікації і автентифікації реалізує механізми автентифікації користувачів за будь-яким з наведених варіантів: логіном/паролем, доменним обліковим записом Active Directory, обліковим записом служби каталогів LDAP, за допомогою особистого ключа КЕП. Перелік механізмів автентифікації, доступних для того чи іншого суб'єкта доступу (або групи суб'єктів доступу) визначається адміністратором ERP-системи.

Умови впровадження. У відповідності до обґрунтування, наведеного в підрозділі 3.1, до ERP-системи додається серверна версія програмного комплексу користувача центру сертифікації ключів «ІІТ Користувач ЦСК-1» (п. 3 табл. 3.1). На робочі станції користувачів, розташованих в розподілених сегментах інформаційно-комунікаційних систем, встановлюється програмний комплекс клієнта захисту мережних з'єднань «ІІТ Захист з'єднань-2. Клієнт захисту з'єднань» (п. 4 табл. 3.1).

Окрім використання програмних засобів криптографічного захисту інформації, зазначених в табл. 3.1, необхідною умовою практичної реалізації рішення є обов'язкове застосування апаратних засобів криптографічного захисту інформації (далі – КЗІ), перелік яких зазначено в табл. 3.2:

Таблиця 3.2 – Перелік апаратних засобів КЗІ

№ з/п	Найменування апаратних засобів криптографічного захисту інформації	Примітка
1	Мережний криптомодуль (наприклад, «ІІТ МКМ Гряда-301») або аналогічний	Один на ERP (SAP) - систему
2	Захищений носій особистих ключів (наприклад, «ІІТ Е. ключ «Кристал-1») або аналогічний	Персональний, у кожного користувача

Функціональне поєднання засобів, перелік яких заначений в табл. 3.1, та засобів, перелік яких заначений в табл. 3.2, дозволяє реалізувати комплекс автентифікації користувачів ERP(SAP)-системи при доступі до серверів прикладних систем (ресурсів), структурна схема якого представлена на рис. 3.3:

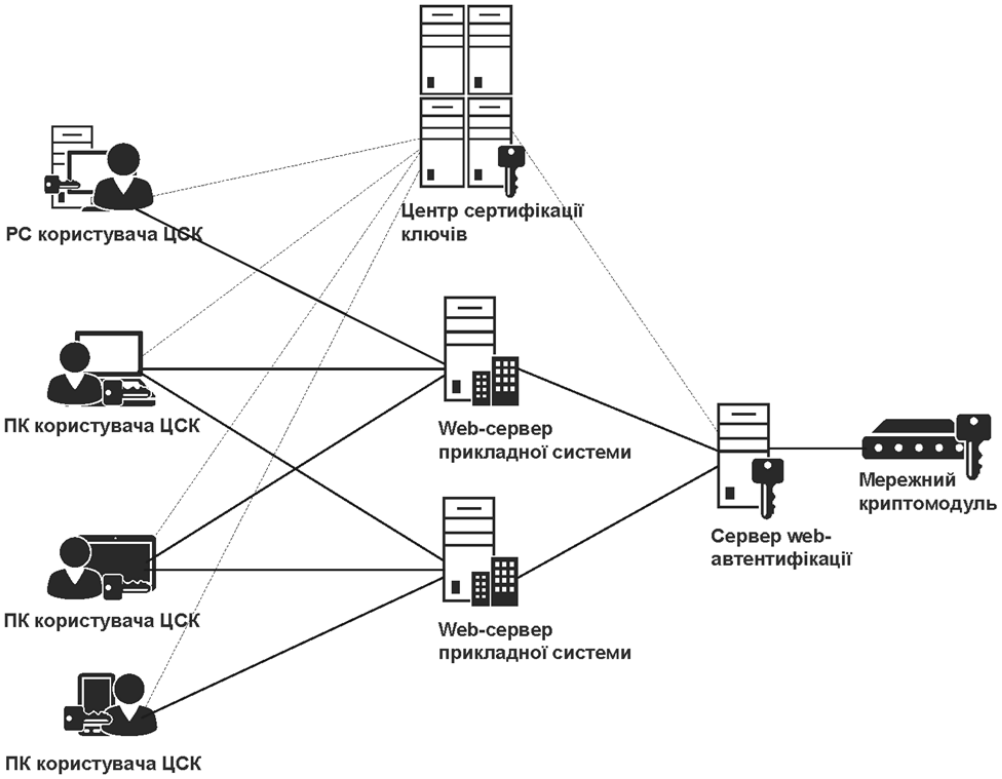


Рисунок 3.3 – Структурна схема комплексу автентифікації користувачів у складі ERP(SAP)-системи

Джерело: [93]

3.3 Практична реалізація розроблених моделей

Практична реалізація моделі автентифікації. Як було зазначено в підрозділі 3.1 даного розділу необхідно провести зміну конфігурації налаштувань «IT-Enterprise» та додати додатковий програмний засіб «ІІТ Користувач ЦСК-1», що забезпечить автентифікацію (крім процедури формування сертифікатів відкритих ключів та списку відкликаних сертифікатів, що використовуються для механізму кваліфікованого електронного підпису) користувачів та цілісність при обміні інформацією, що зберігається в базах даних, шляхом формування електронного підпису за алгоритмом ДСТУ 4145-2002, що також реалізується програмною бібліотекою програмного комплексу «ІІТ Користувач ЦСК-1»

За допомогою панелі адміністрування в модулі автентифікації «IT-Enterprise» «Формування параметру автентифікації» обираємо параметр «Вхід по ключу електронного підпису» як показано на рис. 3.4:

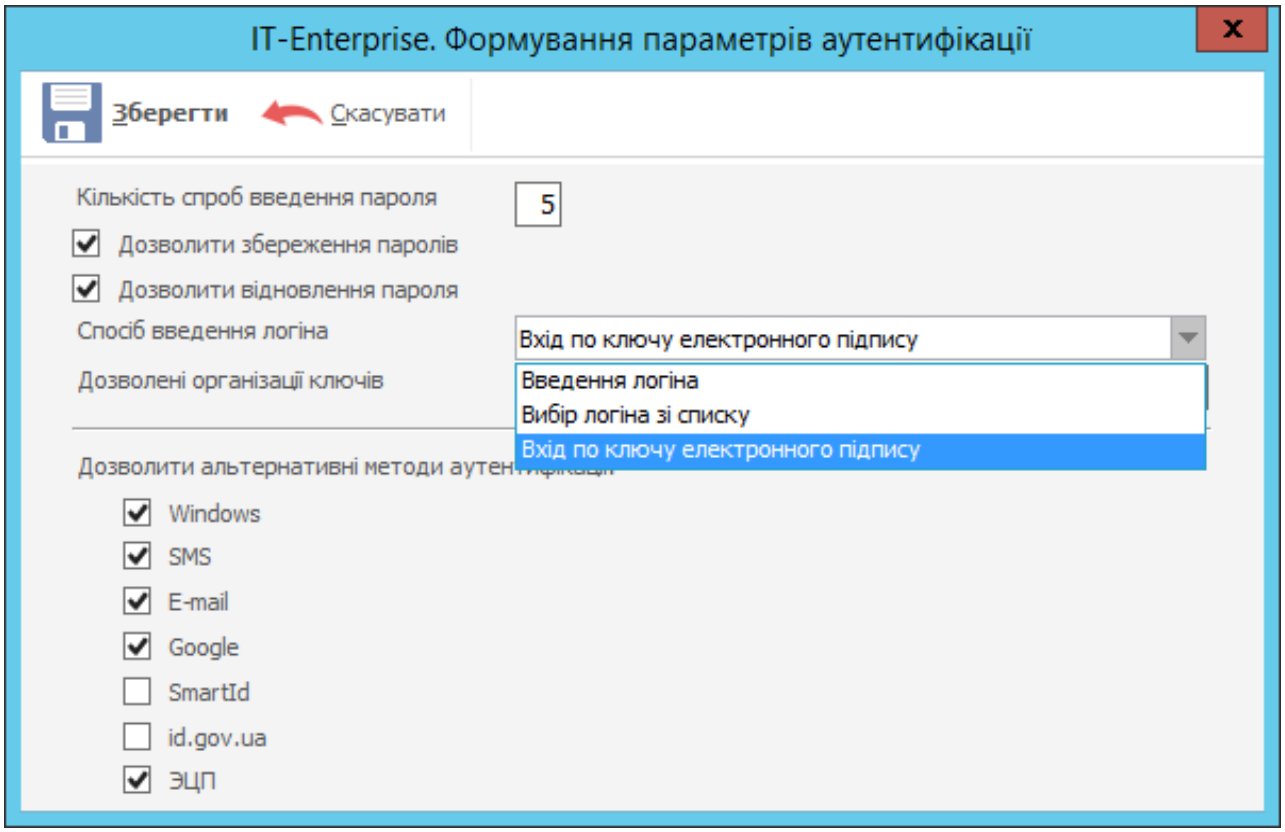


Рисунок 3.4 – Перехід на режим двофакторної автентифікації по ключу електронного підпису в ERP-системі «IT-Enterprise»

Так як модуль ідентифікації та автентифікації «IT-Enterprise» за замовчуванням налаштований на автентифікацію windows-клієнта із використанням захищеного механізму за технологію безпечного з'єднання між клієнтом (комп'ютером користувача) та сервером на основі протоколу автентифікації Kerberos [90, п. 6.1.16], необхідно скоректувати деякі налаштування (лістинг програмного коду зміни налаштувань наведено в п. В.1 додатку Б).

Наступним моментом є вибір важливого параметру в програмному комплексі «ІІТ Користувач ЦСК-1» (що необхідно здійснити як на серверній стороні, так й на персональних комп'ютерах користувачів) для використання електронного підпису саме за алгоритмом ДСТУ 4145-2002. Це вибір параметру «Використання ключів», необхідно встановити «ЕЦП. Протоколи розподілу ключів у державних алгоритмах і протоколах», як показано на рис. 3.5:

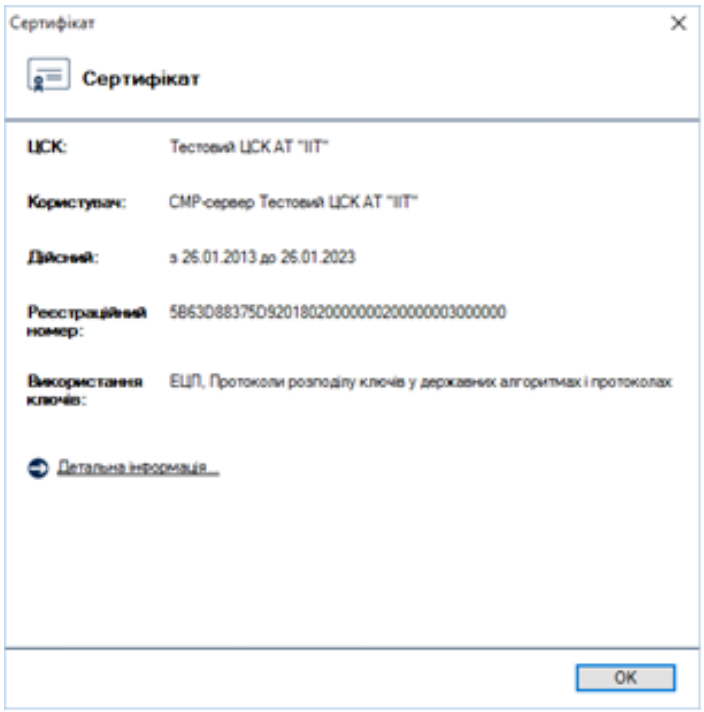


Рисунок 3.5 – Вікно підтвердження вибору переходу на протоколи розподілу ключів у державних алгоритмах та протоколах

Налаштування цього параметру здійснюється відповідно до настанов програміста [95, 96]. Лістинг коду налаштувань наведено в п. В.2 додатку В.

Таким чином, після проведення вказаних налаштувань, доступ користувача до серверу прикладної системи (ресурсу) здійснюється після його автентифікації за моделлю, що описана в підрозділі 2.2 (табл. 2.3, рис. 2.2а).

Користувач вмикає ПК та підключає до нього свій персональний захищений носій особистих ключів (п. 2 табл. 3.1), наприклад, «Електронний ключ «Кристал-1».

Після підключення запускається «Захищений робочий стіл» програмного комплексу клієнта захисту мережних з'єднань «ІІТ Захист з'єднань-2. Клієнт захисту з'єднань» (п. 4 табл. 3.1), в якому необхідно вибрати носій з особистим ключем (рис. 3.6):

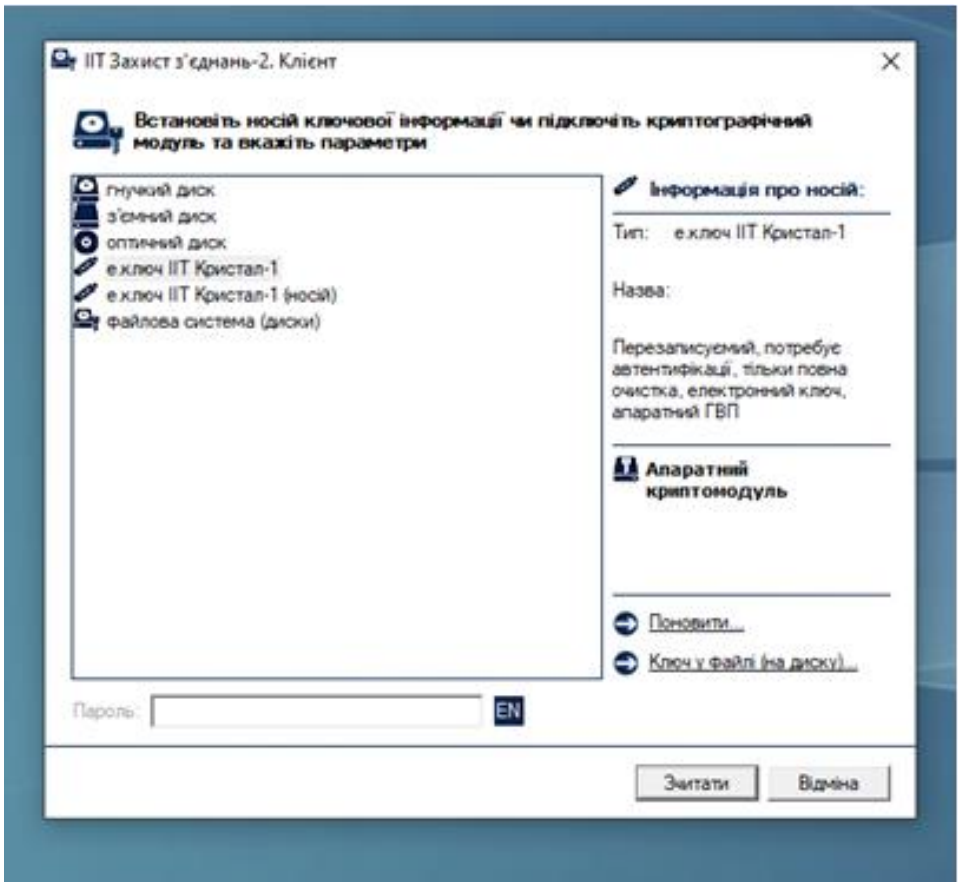


Рисунок 3.6 – Вікно «Захищений робочий стіл» програмного засобу КЗІ

Серед можливих варіантів користувач обирає свій носій (електронний ключ «Кристал-1») та вводить пароль доступу до особистого ключа (рис. 3.7):

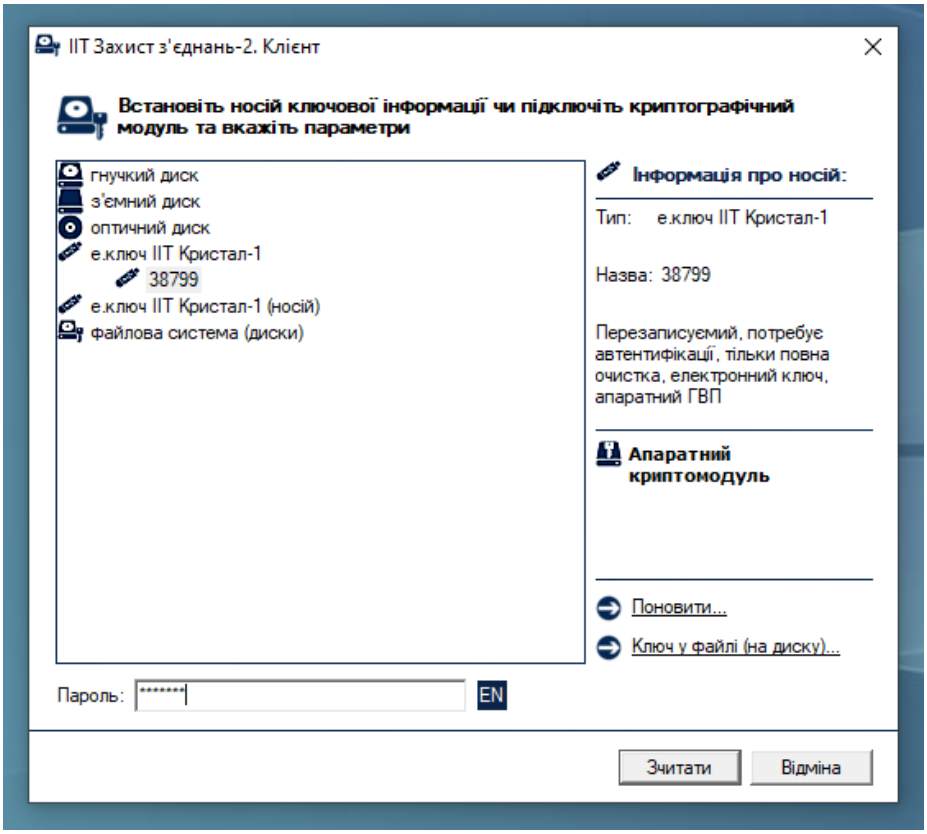


Рисунок 3.7 – Дії користувача з вибору носія особистого ключа

Ці два прості кроки запускають процес взаємодії користувача та сервера, який представлений на структурно-функціональній схемі (рис. 3.8):

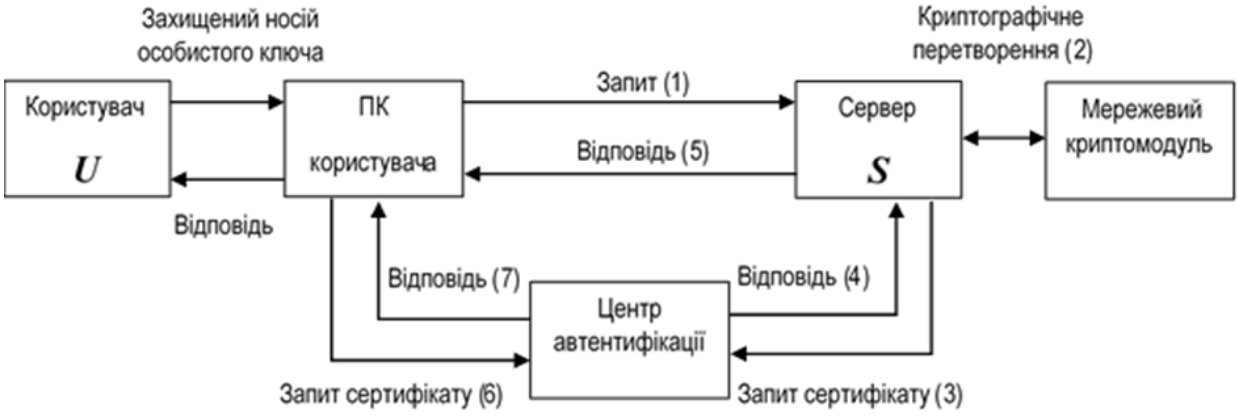


Рисунок 3.8 – Структурно-функціональна схема автентифікації користувача та сервера (ресурсу) в ERP(SAP)-системі

Протокол автентифікації користувача та встановлення захищеного сеансу передачі даних реалізовано на основі протоколу взаємної автентифікації з двома проходами згідно ДСТУ ISO/IEC 9798-3 (п. 5.2.1) та включає:

– формування користувачем та передачу даних автентифікації (запит (1) на сервер, при цьому користувач виконує наступні дії:

– генерує випадкове число;

– підписує випадкове число та власний сертифікат (за необхідності) власним особистим ключем ЕЦП;

– передає сформовані дані автентифікації (запит) на сервер;

– обробку запиту (1) від користувача сервером, при цьому сервер виконує наступні дії:

– отримує дані автентифікації від користувача;

– здійснює пошук (за відсутності сертифіката у запиті) та перевірку чинності сертифіката користувача (3), перевіряє ЕЦП (4) на даних;

– у разі успішної обробки отриманих даних автентифікації – генерує сеансові ключі шифрування та вектори початкової ініціалізації (2);

– підписує отримане випадкове число та сеансові ключі з векторами початкової ініціалізації власним особистим ключем ЕЦП;

– зашифровує сформовані дані (2) разом з ЕЦП та спрямовує на користувача;

– передає підписані та зашифровані дані автентифікації (відповідь) (5) користувачу;

– прийом та обробку відповіді користувача від сервера, при цьому користувач виконує наступні дії:

– отримує відправлені дані автентифікації (відповідь) (5) від сервера;

– здійснює пошук та перевірку чинності сертифіката сервера (6);

– розшифровує дані автентифікації, перевіряє ЕЦП (7) на даних;

– перевіряє відповідність випадкового числа в отриманих даних;

– у разі успішної обробки отриманих даних автентифікації (відповіді) завершує роботу протоколу.

За результатом роботи протоколу на сервері та в користувача встановлюються два сеансових ключа та два вектори початкової ініціалізації для поточного шифрування даних (2), тобто між ПК користувача та сервером встановлюється захищене з’єднання у дуплексному режимі.

Користувач може перейти у вікні браузера на головну сторінку доступної йому прикладної програми роботи з ресурсом за адресою, що видана технічним адміністратором. Відобразиться вікно для здійснення входу у програму для роботи з ресурсом (рис. 3.9):

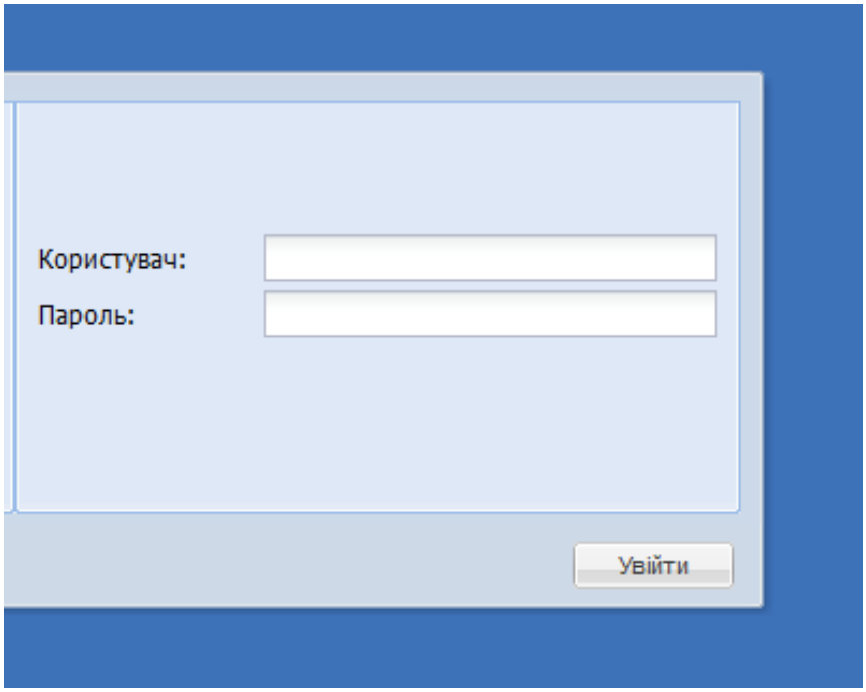


Рисунок 3.9 – Вікно для здійснення входу у програму

Користувач вводить інформацію ідентифікації та пароль (рис. 3.10):

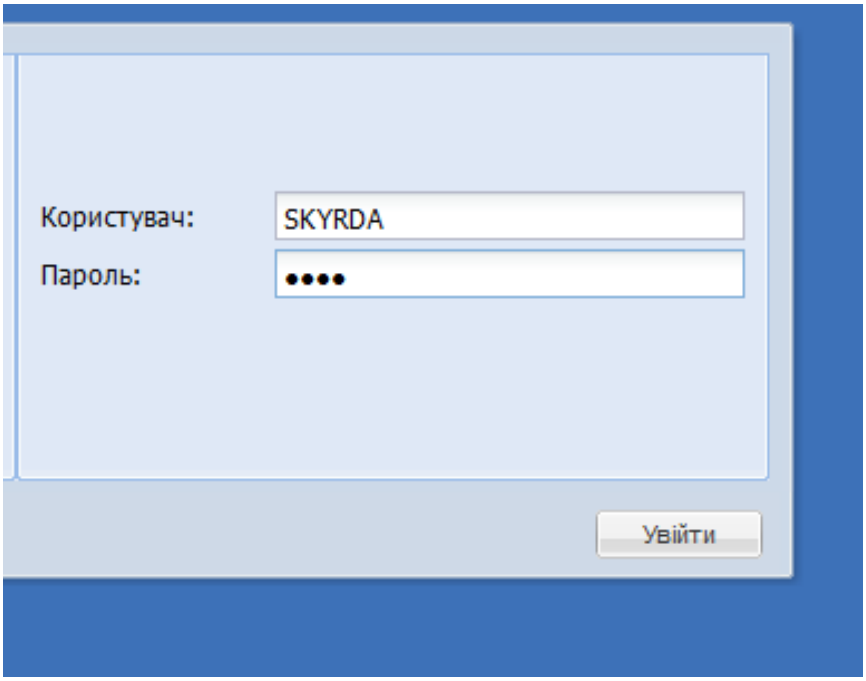


Рисунок 3.10 – Введення інформації ідентифікації користувача та паролю

Після натискання кнопки «Увійти» починається другий етап двофакторної автентифікації користувача. Відображається вікно «Зчитування особистого ключа» (рис. 3.11):

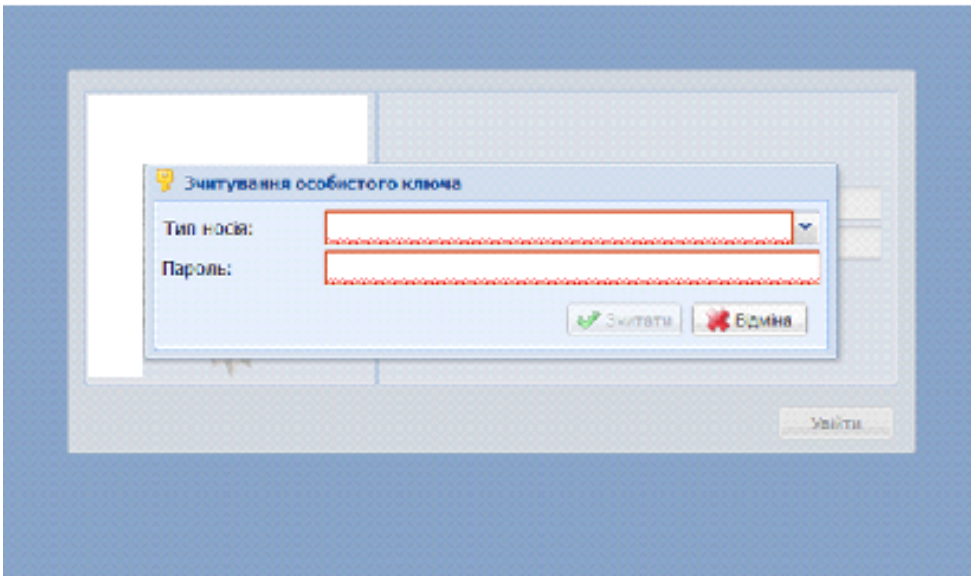


Рисунок 3.11 – Зчитування особистого ключа користувача

Для зчитування ключа, необхідно обрати захищений носій, на якому міститься особистий ключ користувача у полі-списку «Тип носія» (рис. 3.12):

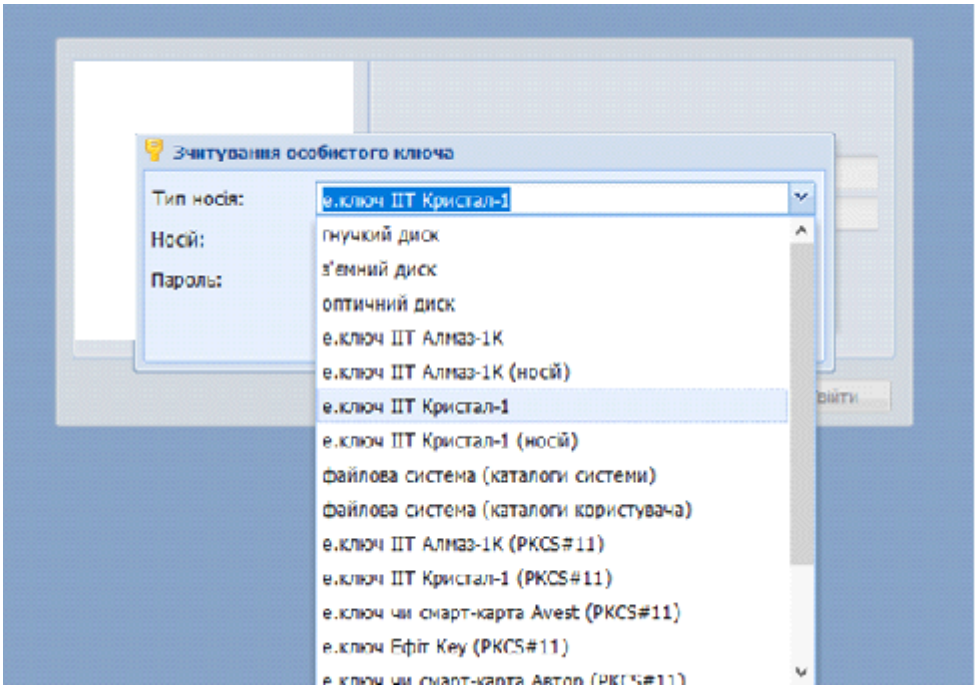


Рисунок 3.12 – Поле-список вибору носія особистого ключа користувача

Необхідно вибрати захищений носій «Кристал-1», його заводський номер, ввести пароль доступу до особистого ключа (рисунок 3.13):

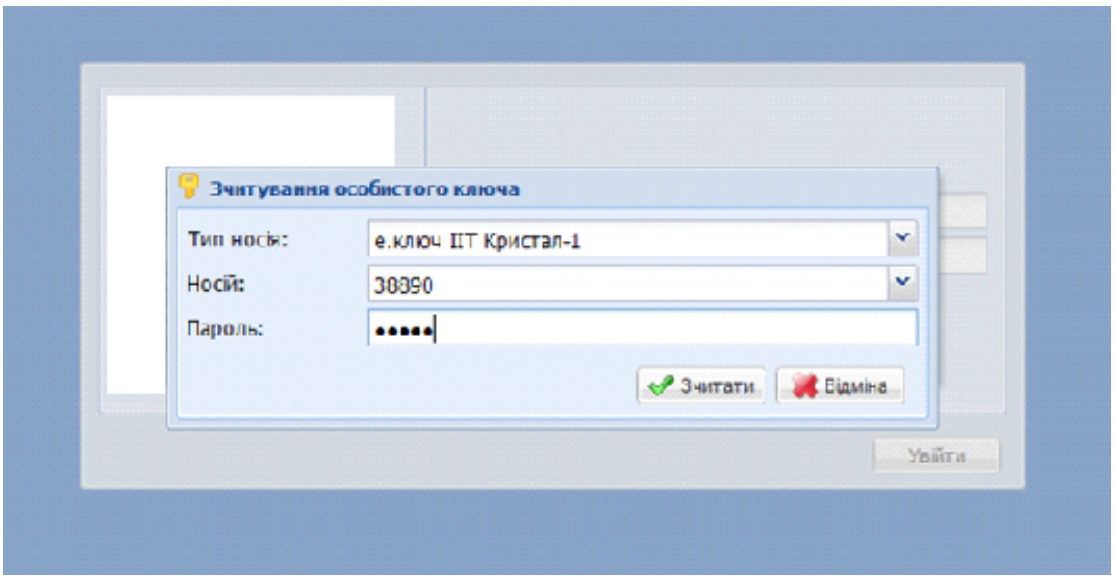


Рисунок 3.13 – Процедура зчитування особистого ключа користувача

Необхідно натиснути кнопку «Зчитати» (рис. 3.13). Зчитується ключ, та користувачу відображається робочий стіл прикладної програми для роботи з деяким ресурсом з доступним його ролі інструментарієм (рис. 3.14):

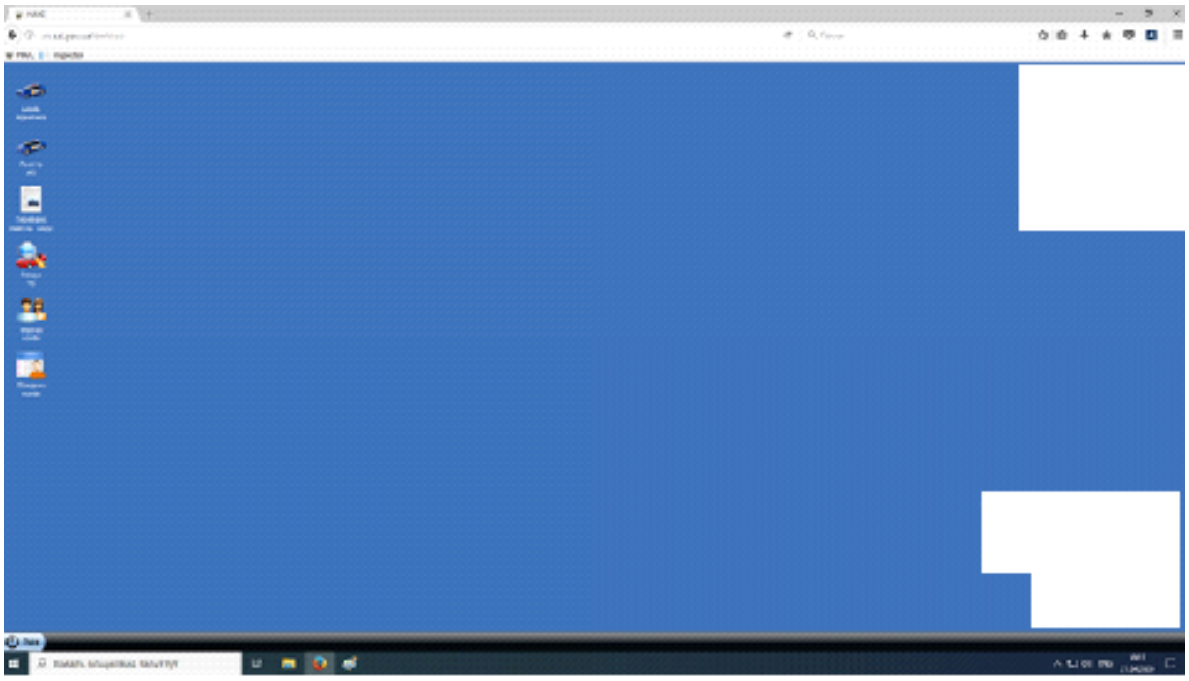


Рисунок 3.14 – Робочий стіл прикладної програми роботи з ресурсом

Наявність технічної документації виробника [93-101] дозволяє розглянути більш детально процес описаних вище кроків автентифікації по функціональній схемі, що представлена на рис. 3.15:

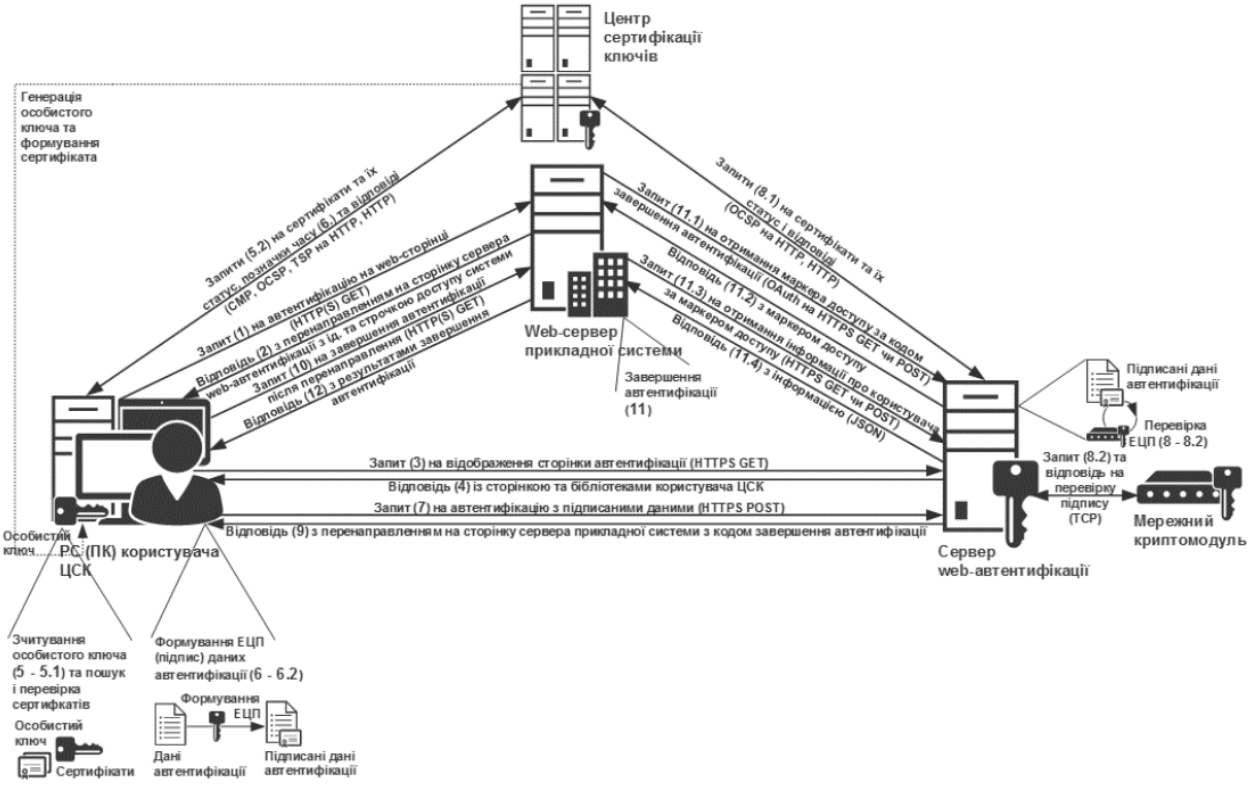


Рисунок 3.15 – Структурно-функціональна схема реалізованої вдосконаленої моделі автентифікації

Джерело: [93, 99]

Функціональне поєднання засобів, перелік яких заначений в табл. 3.1, та засобів, перелік яких заначений в табл. 3.2, реалізовує модель автентифікації користувача за вдосконаленою схемою, що включає (див. рис. 3.15):

- відправку користувачем запиту (1) на автентифікацію з web-браузера РС чи ПК на web-сторінці web-сервера прикладної системи (натискання посилання або контекстна відправка запиту) за методом GET протоколу HTTP(S);

- обробку запиту (2) та відправку web-сервером прикладної системи користувачеві відповіді із перенаправленням браузера користувача на сторінку сервера web-автентифікації (перенаправлене посилання);

- відправку користувачем запиту (3) на відображення сторінки автентифікації серверу автентифікації за методом GET протоколу HTTPS на перенаправлене посилання

- обробку запиту та відправку сервером автентифікації користувачеві відповіді (4) із вмістом web-сторінки автентифікації та бібліотеками підпису

користувача ЦСК (завантаження java-скрипта браузером чи підключення попередньо встановлених web-бібліотек підпису користувача ЦСК);

- зчитування користувачем власного особистого ключа (5) з використанням відповідної бібліотеки підпису, що включає:

- зчитування файлу з особистим ключем java-скрипт-бібліотекою чи зчитування ключа з електронного ключа чи іншого носія ключової інформації або криптомодуля web-бібліотеками підпису з використанням пароля захисту (5.1);

- відправку бібліотекою запиту (5.2) до ЦСК на отримання ланцюжку сертифікатів користувача за протоколом CMP та отримання відповіді з ЦСК або зчитування сертифікату користувача з наданого файлу чи з постійного файлового сховища, відправку запитів на перевірку статусу сертифікатів у ЦСК за протоколом OCSP і отримання відповідей та завантаження з ЦСК поточних CBC і перевірку статусу сертифікатів з використанням завантажених CBC;

- формування користувачем ЕЦП - підпис даних автентифікації (6) з використанням відповідно бібліотеки підпису, що включає:

- відправку бібліотекою запиту (6.1) до ЦСК на формування позначки часу за протоколом TSP та отримання відповіді з ЦСК із сформованою позначкою;

- формування ЕЦП (6.2) з позначкою часу з використанням особистого ключа користувача ЦСК;

- відправку користувачем запиту (7) на автентифікацію із підписаним даними серверу автентифікації за методом POST протоколу HTTPS;

- перевірку (8) сервером автентифікації підписаних даних автентифікації від користувача з використанням бібліотеки підпису у вигляді модуля розширення PHP та прийняття рішення про успішність автентифікації користувача, що включає:

- відправку бібліотекою запиту (8.1) до ЦСК на пошук та перевірку статусу сертифіката користувача за протоколом OCSP і отримання відповіді та завантаження з ЦСК поточних CBC і перевірку статусу сертифіката з використанням завантажених CBC;

- перевірку ЕЦП (8.2) з використанням перевіреного сертифіката особистого ключа користувача ЦСК;

- відправку (у разі успішної автентифікації) сервером автентифікації користувачеві відповіді (9) із перенаправленням браузера користувача на сторінку сервера прикладної системи, яка була вказана в якості зворотного посилання під час попереднього перенаправлення на сервер автентифікації;

- відправку користувачем (за результатом перенаправлення браузеру) запиту (10) на завершення автентифікації серверу прикладної системи за методом GET протоколу HTTP(S) на перенаправлене посилання.

Термін дії коду завершення автентифікації на сервері автентифікації – 30 с;

- обробку сервером прикладної системи запиту (11) на завершення автентифікації користувача, що включає:

- відправку сервером прикладної системи запита (11.1) серверу автентифікації на отримання маркера доступу за кодом завершення автентифікації (code) методом GET чи POST протоколу HTTPS.

- обробку запиту та відправку сервером автентифікації серверу прикладної системи відповіді (11.2) з маркером доступу у вигляді JSON-тексту (текстовий формат обміну даними, що використовує JavaScript);

- відправку сервером прикладної системи наступного запиту (11.3) до сервера автентифікації на отримання інформації про користувача за маркером доступу (access_token) методом GET чи POST протоколу HTTPS;

- обробку запиту та відправку сервером автентифікації серверу прикладної системи відповіді (11.4) з інформацією про автентифікованого користувача у вигляді JSON-тексту;

- відправку сервером прикладної системи відповіді (12) користувачу про завершення автентифікації.

За результатом роботи протоколу, що реалізує вдосконалена модель автентифікації, між ПК користувача та сервером встановлюється захищене з’єднання у дуплексному режимі, користувачеві надається доступ до ресурсу

згідно дозволених для його ролі дій (читання, пошук, додавання даних, зчитування даних, видалення даних тощо).

Таким чином, практична реалізація вдосконаленої моделі автентифікації досягнута комплексним застосуванням програмних засобів, перелік яких заначений в табл. 3.1, та апаратних засобів, перелік яких заначений в табл. 3.2. Функціональна схема практичної реалізації представлена на рис. 3.16:

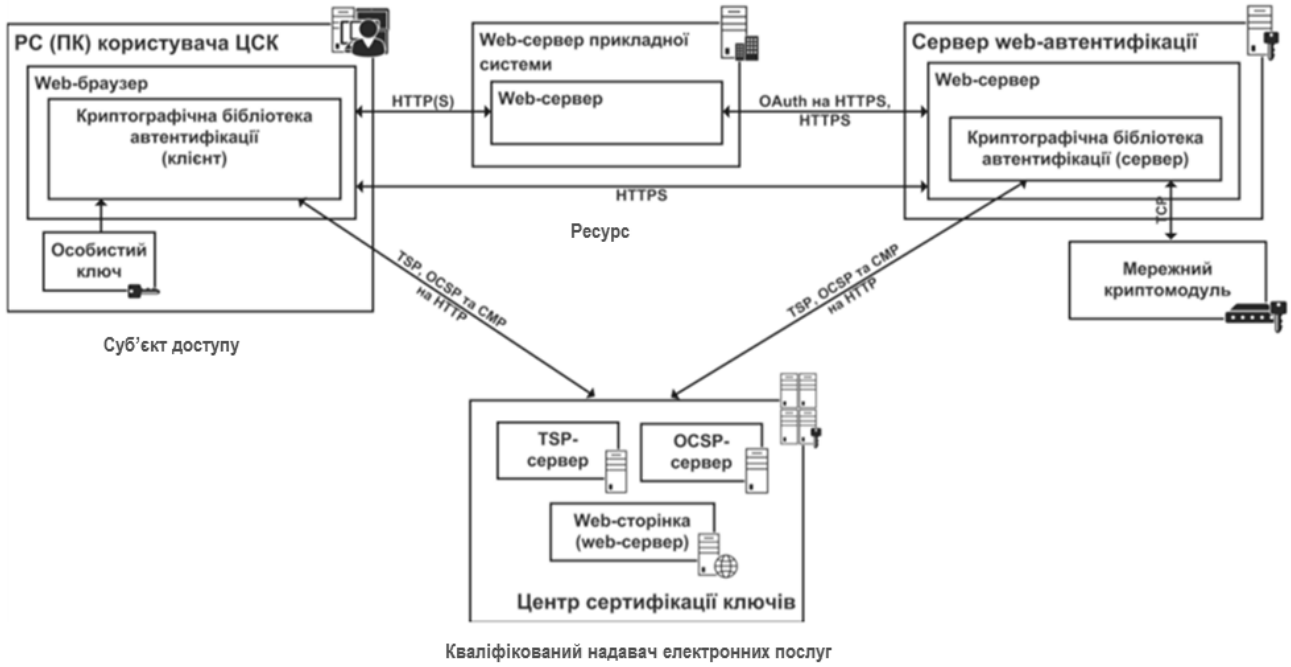


Рисунок 3.16 – Функціональна схема практичної реалізації вдосконаленої моделі автентифікації

Джерело: [93, 99] з уточненням автора

Практична реалізація забезпечена наступними компонентами:

– криптографічні бібліотеки (користувача ЦСК), зазначені в пп. 3,4 табл. 3.1;

– апаратні засоби КЗІ (табл. 3.2, табл. 3.3).

Програмні засоби КЗІ реалізують логіку роботи моделі та інтегровані безпосередньо у користувальницьку та серверну частини системи (користувача та сервер), через визначені інтерфейси.

Програмні засоби КЗІ в схемі можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі, мережні криптомодулі тощо.

До складу апаратних засобів комплексу можуть входити:

– електронний ключ «Кристал-1» («ІІТ Е. ключ Кристал-1») або будь-який аналог від іншого виробника (див. табл. 3.3);

– мережний криптомодуль «Гряда-301» («ІІТ МКМ Гряда-301») або будь-який аналог від іншого виробника.

Бібліотеки користувача центру сертифікації ключів (ЦСК) призначені для використання в якості базових засобів КЗІ та виконують наступні функції у їх складі:

– роботу з носіями ключової інформації (зчитування особистих ключів з носіїв);

– роботу з файловим сховищем сертифікатів та списків відкликаних сертифікатів (СВС), що включає:

– зчитування сертифікатів та списків відкликаних сертифікатів із файлового сховища;

– визначення статусу сертифіката за допомогою списків відкликаних сертифікатів;

– завантаження списків відкликаних сертифікатів з веб-сторінки ЦСК (з веб-серверу ЦСК);

– зашифрування та розшифрування даних;

– формування та перевірку ЕЦП від даних;

– захист сеансів передачі даних (захист з’єднань), що включає:

– реалізацію протоколу взаємної автентифікації сторін під час встановлення сеансу захищеної передачі даних (захищеного з’єднання);

– захист (шифрування та контроль цілісності) сегментів захищеної передачі даних (даних захищеного з’єднання);

– інтерактивну перевірку статусу сертифікатів у ЦСК за протоколом OCSP (через OCSP-сервер ЦСК);

– пошук сертифікатів у LDAP-каталозі ЦСК (на LDAP-сервері ЦСК);

– отримання позначок часу у ЦСК (через TSP-сервер ЦСК) тощо.

Бібліотеки користувача ЦСК інтегруються у прикладні системи або через власні програмні інтерфейси, реалізовані для ОС Microsoft Windows, Linux (Ubuntu/Debian/CentOS), UNIX (FreeBSD/IBM AIX/SunOS), Apple macOS/iOS, Google Android або через визначені інтерфейси (PKCS#11, GSS-API та ін.). Для всіх бібліотек існують приклади використання.

Електронний ключ призначений для апаратної реалізації криптографічних перетворень усередині пристрою у складі засобів користувача системи. В якості таких пристроїв, як захищених носіїв особистого ключа користувача, можливо використання аналогічних апаратних засобів КЗІ [103]. Найбільш поширені у використанні захищені носії особистих ключів представлені в табл. 3.3:

Таблиця 3.3 - Захищені носії особистих ключів

№ з/п	Найменування	Експертний висновок	
		на засіб КЗІ	на засіб КЕП
1	Електронний ключ «Кристал-1»	№ 04/02/03-171 від 19.01.2018	№ 04/05/02-998 від 14.04.2021
2	Електронний ключ «Алмаз-1К»	№ 04/05/02-995 від 14.04.2021	№ 04/05/02-996 від 14.04.2021
3	Електронний ключ «SecureToken-337»	№ 04/05/02-1380 від 12.05.2021	№ 04/05/02-1381 від 12.05.2021
4	Електронний ключ «Efit Key»	№ 04/05/02-992 від 14.04.2021	№ 04/05/02-1004 від 14.04.2021
5	Електронний ключ «AvestKey»	№ 04/05/02-383 від 10.02.2022	№ 04/05/02-384 від 10.02.2022

Мережний криптомодуль призначений для апаратної реалізації криптографічних перетворень у складі сервера системи.

На сервері системи встановлюються та використовуються наступні складові елементи:

– програмний комплекс захисту сервера, який включає бібліотеки користувача ЦСК (для відповідної серверної ОС);

– апаратний засіб КЗІ – мережний криптомодуль.

На засобах користувачів системи (робочих станціях чи персональних комп’ютерах - РС та ПК) встановлюються та використовуються наступні складові елементи:

– програмний комплекс захисту користувача, який включає бібліотеки користувача ЦСК (для відповідної ОС);

– апаратний засіб КЗІ – електронний ключ (захищений носій особистого ключа користувача) (див. табл. 3.3).

Процедуру формування сертифікатів відкритих ключів та списку відкликаних сертифікатів, що використовуються для механізму кваліфікованого електронного підпису, забезпечує незалежна третя сторона, якою виступає кваліфікований надавач електронних довірчих послуг, включений до Довірчого списку [62], що задовольняє вимоги, визначені в [44].

Практична реалізація моделей доступу та політики безпеки доступу. У відповідності до технічної документації виробника, ERP-система «IT-Enterprise» підтримує будь-яку рольову модель доступу сімейства RBAC.

На рівні системи «IT-Enterprise» доступ до даних та функцій роботи із даними надається користувачам на основі ролей. Для кожної групи користувачів (для кожної ролі) налаштовується перелік доступних для роботи модулів, а також функцій кожного модуля: тільки перегляд або модифікація, фільтрація даних, обмеження розрахункових режимів та інші. Якщо модуль та/або функція недоступна для користувача, модуль/функція не відображається в його головному меню.

Для користувачів та груп користувачів доступ до функцій надається за заданим розкладом. Для груп передбачена можливість створення спеціалізованих модулів, довільних меню, коригування існуючих меню, додавання та закриття функцій в меню.

Робота окремого користувача в системі також може бути параметризована: для різних користувачів задаються різні правила роботи, налаштовується доступ до тих чи інших можливостей системи, а також доступ до тих або інших даних (по

підрозділах, по групах ресурсів, по рахунках та іншим обраним параметрам). Для різних груп (ролей) налаштовується доступ та правила роботи.

Крім того, окремі правила роботи можуть бути задані в залежності від комп'ютера - робочого місця, з якого користувач працює з системою.

Тобто, обраний програмний продукт (п. 1 табл. 3.1) здатний реалізувати необхідність введення ієрархічної організації системи ролей *RH* та введення ієрархії запитів *RqH*, зазначені в підрозділі 2.3 даної роботи (що й потрібно для практичної реалізації вдосконаленої моделі доступу) та повноваженнями користувачів або привілеями (асоційованими з параметрами доступу), зазначеними в підрозділі 2.4 даної роботи (що й потрібно для практичної реалізації вдосконаленої моделі політики безпеки доступу користувачів до ресурсів).

Практична реалізація моделей здійснюється за допомогою інструментів та модулів ERP-системи «IT-Enterprise». Налаштування здійснюється виключно адміністратором системи в інтуїтивно зрозумілому інтерфейсі програми шляхом відмічання необхідних полів, які послідовно пропонує алгоритм налаштування.

Коротко цей процес відбувається в наступний спосіб. При реєстрації конкретного користувача в системі, йому обирається роль: адміністратора чи звичайного користувача. При виборі ролі звичайного користувача відкривається доступ для включення в загальні групи користувачів. Кожній такій групі користувачів встановлені відповідні дозволи: група з дозволом доступу до корпоративної електронної пошти, група з дозволом доступу до системи корпоративного електронного документообігу, група з дозволом доступу до певного архіву документів, та інші заздалегідь визначені та доступні групи.

Потім користувач включається в групи структурних підрозділів організації, що й відповідає його посаді. Таким групам в системі заздалегідь призначаються дозволи на доступ до різних ресурсів: баз даних, реєстрів, локалізованих архівів тощо.

Потім користувач включається в групи, що відповідають статусу його посади: група начальників відділів, група головних спеціалістів, група провідних спеціалістів тощо. Кожній такій групі в ієрархії ролей встановлена відповідна

ієрархія запитів, пов’язана з повноваженнями (або привілеями) в різних групах дозволу та групах функцій: тільки отримувати документи, надавати дозвіл на відправку документів, накладати резолюції, ставити завдання, здійснювати контроль, додавати документи до бази даних, знищувати документи в базі даних, відмічати статус документа в системі документообігу як «виконаний / в процесі виконання / на доопрацювання / в архів тощо», надавати дозвіл користувачу з групи ролей, нижчої за ієрархією, дозвіл на якийсь конкретний доступ до ресурсу або дію з ресурсом та тому подібне.

Тобто практична реалізація розроблених моделей доступу та політики безпеки доступу в реальній інфраструктурі цілком можлива із використанням можливостей програмних продуктів організації ERP-систем та SAP-систем.

Аналіз практичної реалізації моделей. Практична реалізація вдосконаленої моделі автентифікації, запропонованої та описаної в підрозділі 2.2, показала реальність її застосування при організації доступу користувачів до ресурсів в реальній інфраструктурі із використанням апаратних та програмних засобів (табл. 3.1, табл. 3.2) вітчизняного виробника, що повністю задовольняє вимоги, зазначені в підрозділі 1.4 даної роботи.

Практична реалізація вдосконаленої моделі доступ $RBAC_B$, опис якої здійснений в підрозділі 2.3, показала реальність та ефективність її застосування. Запит (*Rq*) являє собою набір інформації, яка пересилається між користувачем та сервером за протоколом HTTP(S). Модель враховує та забезпечує специфіку роботи веб-додатків та дозволяє розмежовувати доступ на основі шляхів запиту (URI).

Вдосконалена рольова модель доступу $RBAC_B$ допускає її впровадження в будь-яких інформаційних системах та дозволяє виконувати розмежування доступу на підставі параметрів запитів. Для множини запитів використовується правило бінарного відношення включення, яке дозволяє впорядкувати запити згідно з ієрархією запитів *RqH*. Для забезпечення бінарного відношення, для множини запитів *Rq* створюється ієрархія ролей *RH*, заснована на множині ролей *R* та обмеженні функцій *UA(U), roles(S), PA(R)*. Для автентифікації користувача

залишена багатофакторна автентифікація з використанням обох пар токену *Tk*: (ім'я, пароль) та (сертифікат відкритого ключа, особистий ключ).

Модулі ERP-системи «IT-Enterprise» підтримують процес зміненої в моделі рольового доступу $RBAC_B$ послідовності двоетапної організації системи розмежування доступу: спочатку створюються ролі та визначаються їх повноваження, а потім на визначені ролі призначаються конкретні користувачі системи.

Реалізоване введення ієрархічної організації системи ролей *RH* та введення ієрархії запитів *RqH* ефективне. Такий підхід віддзеркалює реальні організаційно-технологічні та організаційно-управлінські схеми на підприємствах та в організаціях: посади співробітників підприємств, організацій у більшості випадків утворюють ієрархічно підлеглі структури. Відповідно запропонована та реалізована модель доступу $RBAC_B$ легко впроваджується на основі «ролей-посад», «ролей-функцій», «ролей-повноважень» та ефективно вирішує проблеми реалізації у випадку складної ієрархічної структури посадових осіб (такої, як в органах місцевого самоврядування), особливо при організації колективного доступу до ресурсів в складних IT-системах з великою кількістю користувачів та великою кількістю ресурсів.

А підхід реалізації на основі «ролей-посад» та «ролей-повноважень» при колективному доступі до ресурсів при складній ієрархічній структурі посад та їх взаємодії в організації, можливий лише із застосуванням вдосконаленої моделі політики безпеки доступу $RBAC_B$, коли дерево ролей доповнюється (розширюється) повноваженнями або привілеями (або асоціативним поєднанням повноважень та привілеїв в залежності від мети застосування), що й показала практична реалізація в ERP-системі «IT-Enterprise».

Так як дослідження практичної реалізації проводилося на двох різних платформах, можливо провести порівняння. Практичний експеримент показав фактичну ідентичність виконання процесів автентифікації та доступу користувачів до ресурсів. Відмінність лише в тому, що програмний комплекс захисту «ІІТ Захист SAP-системи» використовується для підвищення

можливостей та безпеки застарілих SAP-систем, що знаходяться в експлуатації (в конкретному випадку - SAP R/3), до рівня сучасних ERP-систем, а ERP-система «IT-Enterprise» самодостатня. В обох випадках необхідно використання апаратних (табл. 3.2) та програмних засобів криптографічного захисту (п.п. 3, 4 табл. 3.1). При цьому при відсутності необхідності обов'язкового виконання вимог, визначених в підрозділі 1.4 даної роботи (наприклад, коли ресурси не відносяться до державних інформаційних ресурсів, або інформація, яка в них обробляється, не відноситься до інформації, вимога щодо захисту якої встановлена законом), можливо використання лише ERP-системи «IT-Enterprise» та файлу особистого ключа (з розширенням DAT або jks) користувача на звичайних флеш-носіях (або навіть, зберігання його на персональному комп'ютері користувача). Останній варіант з позицій інформаційної безпеки не рекомендується, проте за фактом, можливий.

Крім того, за аналізом практичної реалізації моделей, досліджено, що процедури та механізми, а також апаратні та програмні продукти вітчизняних виробників, які застосовані, фактично відповідають принципам архітектури нульової довіри, зазначеним в підрозділі 1.3 даної роботи, та при комплексному застосуванні із засобами антивірусного захисту (на ПК користувачів, серверах, мережевих екранах) та іншими відомими засобами, забезпечують ефективний захист на різних архітектурних рівнях інфраструктури:

- мережеву безпеку;
- безпеку баз даних;
- безпеку на рівні серверів застосувань з інстальованою СКБД;
- захист інформації на клієнтському комп'ютері користувачів тощо.

Що, в свою чергу, може підвищити ефективність захисту реальних інформаційних та кіберфізичних систем різного призначення та архітектури від складних, цільових та комплексних кібератак, описаних в підрозділі 1.2 даної роботи, та, відповідно, вирішує проблеми сучасного стану кіберзахисту, зазначені в підрозділі 1.1 розділу 1, з урахуванням виявлених причин та виокремлених факторів цих проблем.

Висновки до розділу 3

Здійснено пошук програмних засобів-аналогів вітчизняного виробництва. Пошук проведено із застосуванням методу вивчення аналога (прототипу) та методу еталонного оцінювання (benchmarking). Додатково до критеріїв функціональних можливостей, врахований критерій відповідності нормам чинного законодавства України у сферах захисту інформації, захисту державних інформаційних ресурсів, кіберзахисту об'єктів критичної інфраструктури, здійснення технічного та криптографічного захисту інформації, сфері електронних довірчих послуг, обов'язкові вимоги, якого визначені на попередніх етапах дослідження. Зазначено обґрунтування вибраних рішень.

Доведено наявність програмних та апаратних засобів вітчизняного виробництва, які відповідають обов'язковим вимогам законодавства та нормативно-правових актів в сфері технічного та криптографічного захисту інформації, придатних для практичного впровадження концепції архітектури нульової довіри.

Приведено опис інфраструктури, в якій здійснювалась практична реалізація розроблених моделей автентифікації, доступу до ресурсів та політики безпеки доступу (із застосуванням концепції архітектури нульової довіри) з метою перевірки їх працездатності та ефективності, зазначено умови впровадження.

Висвітлено хід та результати практичної реалізації розроблених моделей.

Доведено можливість практичної реалізації вдосконаленої моделі автентифікації користувачів при доступі до ресурсів та її ефективність.

Здійснено деталізоване вивчення реалізованого процесу автентифікації за допомогою співвідношення з описами, наведеними в технічній документації виробників програмних засобів [45, 93-101] та задокументованих в експертних висновках за результатами державної експертизи у сфері технічного або криптографічного захисту інформації [90-92, 102].

Доведено можливість практичної реалізації вдосконалених моделей доступу та політики доступу користувачів, їх ефективність, особливості застосування.

Проаналізовано результати практичної реалізації моделей, сформульовані відповідні висновки, зазначені: виявлені слабкі та сильні сторони, особливості, рекомендації.

Порівняно результати практичної реалізації моделей на двох різних платформах, наведено висновки та істотні особливості.

Продемонстровано можливість самостійного застосування вдосконаленої моделі автентифікації з використанням можливостей програмних та апаратних засобів криптографічного захисту інформації в будь-яких кіберфізичних системах, що використовують технології web-доступу до функцій або ресурсів.

З'ясовано особливість застосування вдосконаленої моделі доступу: її практична реалізація можлива тільки із використанням розробленої моделі політики безпеки доступу, та тільки в системах типу ERP та SAP. Проте, окремі можливості та особливості обох моделей можуть бути використані для модифікації застарілих моделей сімейства RBAC.

Запропоновано застосування вдосконалених моделей та програмного комплексу захисту «ІІТ Захист SAP-системи» для підвищення можливостей кіберзахисту та кібербезпеки застарілих SAP-систем, що знаходяться в експлуатації.

Доведено можливість застосування програмних та апаратних засобів вітчизняного виробництва, які відповідають обов'язковим вимогам законодавства та нормативно-правових актів в сфері технічного та криптографічного захисту інформації, для практичного впровадження концепції архітектури нульової довіри.

Продемонстровано здатність реалізованих підходів підвищити ефективність захисту реальних інформаційних та кіберфізичних систем різного призначення та архітектури від складних, цільових та комплексних кібератак, описаних в підрозділі 1.2 даної роботи, та, відповідно, вирішити проблеми сучасного стану кіберзахисту, озвучені в підрозділі 1.1 розділу 1, з урахуванням виявлених причин та виокремлених факторів цих проблем.

РОЗДІЛ 4
ЕКОНОМІЧНИЙ РОЗРАХУНОК ЗАПРОПОНОВАНИХ РІШЕНЬ

4.1 Розрахунок капітальних витрат на придбання

Методика та умови розрахунку:

Джерела даних: вхідні дані щодо ціноутворення та вартості для розрахунків обираються з оприлюднених договорів закупівлі, здійснених у відповідності до законодавства [104, 105].

Умови закупівлі: конкурентна процедура закупівлі (тендер) - здійснення конкурентного відбору, найбільш економічно вигідна тендерна пропозиція.

Код економічної класифікації [106]: КЕКВ 2240 за уточненням [107]: «придбання (постачання) програмного забезпечення (ліцензії на право користування програмним забезпеченням), на яке майнові права не передаються користувачу, при цьому майнові та авторські права на об'єкт інтелектуальної власності на зазначене програмне забезпечення залишаються у розробника (постачальника), а замовнику надається право користування цим програмним забезпеченням без права передачі самого програмного забезпечення та/або повноважень на його користування третім особам».

Коди продукції Національного класифікатора України Єдиного закупівельного словника ДК 021:2015 [108]:

- 48000000-8 Пакети програмного забезпечення та інформаційні системи;
- 48151000-1 Системи комп’ютерного керування;
- 48611000-4 Пакети програмного забезпечення для баз даних;
- 48612000-1 Системи керування базами даних;
- 48613000-8 Електронні системи управління даними;
- 48731000-1 Пакети програмного забезпечення для захисту файлів;
- 48514000-4 Пакети програмного забезпечення для роботи з віддаленим доступом;
- 48516000-8 Пакети програмного забезпечення для обміну інформацією;
- 48732000-8 Пакети програмного забезпечення для захисту даних;

- 48761000-0 Пакети антивірусного програмного забезпечення;

- 48781000-6 Пакети програмного забезпечення для управління системами;

- 48730000-4 Пакети програмного забезпечення для забезпечення безпеки.

Враховуємо особливості бухгалтерського обліку операцій з придбання програмного забезпечення [109, 110], а саме:

- ліцензійне програмне забезпечення закуповується на певних умовах, які зазначаються у договорі, оскільки такий об’єкт не може використовуватися, доки на нього не отримано відповідних майнових прав;

- виключні майнові права інтелектуальної власності не закуповуються;

- відповідно об’єкт закупівлі відноситься до нематеріальних активів.

Враховуємо, що пунктом 26-1 підрозділу 2 розділу XX Податкового кодексу Податкового кодексу України [111] визначено, що тимчасово, з 01.01.2013 року по 01.01.2023 року, звільняються від оподаткування податком на додану вартість операції з постачання програмної продукції, а також операції з програмною продукцією, плата за які не вважається роялті згідно з абзацами другим-сьомим підпункту 14.1.225 Податкового кодексу, у тому числі - криптографічні засоби захисту інформації.

Для розрахунку обрана кількість співробітників (користувачів) середнього підприємства [105, абз. 9 ч. 2 ст. 2]: 55 осіб.

При наявності вибору умов закупівлі ліцензії, обираються конкурентні ліцензії з терміном дії один рік (що значно оптимізує витрати на придбання), за наявності пропозиції надання безстрокової ліцензії, обирається остання.

Особливості коректності порівняння. Враховується, що конкурентні варіанти 1 та 2 подібні за функціональним призначенням (призначені для хмарних технологій), проте тільки варіант 2 відповідає вимогам законодавства, що визначені в підрозділі 1.4 даної роботи. Конкурентні варіанти 3 та 4 подібні за функціональним призначенням, проте мають відмінності: варіант 3 – самодостатній, варіант 4 – призначений для захисту застарілих SAP-систем, що знаходяться в експлуатації.

Результати розрахунку:

Визначена методика та умови дозволять розрахувати капітальні витрати на придбання за кількома конкурентними варіантами (табл. 4.1):

Таблиця 4.1 – Розрахунок капітальних витрат на придбання

№ з/п	Найменування	Одиниця виміру	К-ть	Ціна за од., грн.	Вартість, грн.	ПДВ, %	Всього, грн
Варіант 1							
1	Microsoft Azure AD	ліцензія	55	13495	742225	20	890670
2	F5 BIG-IP	од.	1	1275442	1275442	20	1530530
3	Lookout MES	ліцензія	55	564	6768	20	8121
4	ЕК Efit Key	од.	55	1250	68750	-	68750
Всього (разом з ПДВ):							2498071
Варіант 2							
5	IT-Enterprise Cloud	ліцензія	55	11044	607420	20	728904
6	ІІТ Користувач ЦСК-1	ліцензія	1(55)	35000	35000	-	35000
7	ІІТ Захист з’єднань-2	ліцензія	1(55)	30690	30690	-	30690
8	ЕК ІІТ Кристал-1	од.	55	1705	93775	-	93775
Всього (разом з ПДВ):							888369
Варіант 3							
9	IT-Enterprise	ліцензія	55	3909	214995	-	214995
10	ІІТ Користувач ЦСК-1	ліцензія	1(55)	35000	35000	-	35000
11	ІІТ Захист з’єднань-2	ліцензія	1(55)	30690	30690	-	30690
12	ЕК ІІТ Кристал-1	од.	55	1705	93775	-	93775
Всього (разом з ПДВ):							374460
Варіант 4							
13	ІІТ Захист SAP	ліцензія	1	125000	125000	-	125000
14	ІІТ Захист з’єднань-2	ліцензія	1(55)	30690	30690	-	30690
15	ЕК ІІТ Кристал-1	од.	55	1705	93775	-	93775
Всього (разом з ПДВ):							249465

4.2 Розрахунок витрат на щорічне утримання

Методика та умови розрахунку:

Джерела даних: вхідні дані щодо ціноутворення та вартості для розрахунків обираються з оприлюднених договорів закупівлі, здійснених у відповідності до у відповідності до законодавства [104, 105] або оприлюднених на офіційному сайті виробника (розробника), із опублікованих звітів замовника (покупця).

Умови закупівлі: конкурентна процедура закупівлі (тендер) - здійснення конкурентного відбору, найбільш економічно вигідна тендерна пропозиція.

Коди продукції Національного класифікатора України Єдиного закупівельного словника ДК 021:2015 [108]:

- 48000000-8 Пакети програмного забезпечення та інформаційні системи;
- 48730000-4 Пакети програмного забезпечення для забезпечення безпеки;
- 48760000-3 Пакети програмного забезпечення для захисту від вірусів.

Враховуємо особливості бухгалтерського обліку операцій з придбання програмного забезпечення [109, 110], а саме:

- ліцензійне програмне забезпечення закуповується на певних умовах, які зазначаються у договорі, оскільки такий об’єкт не може використовуватися, доки на нього не отримано відповідних майнових прав;
- виключні майнові права інтелектуальної власності не закуповуються;
- відповідно об’єкт закупівлі відноситься до нематеріальних активів.

Для розрахунку обрана кількість співробітників (користувачів) середнього підприємства [105, абз. 9 ч. 2 ст. 2]: 55 осіб.

При закупівлі ліцензій ураховується наявність вибору видів ліцензії:

- безстрокова (безумовно найкращий вибір);
- конкурентна ліцензія (з коефіцієнтом 1,5-2 до числа робочих місць);
- локальна ліцензія (одна ліцензія на одне робоче місце / користувача).

Вибір конкурентної ліцензії з терміном дії один рік, значно оптимізує витрати на її придбання.

Вартість локальної ліцензії визначається як 0,667 від вартості конкурентної ліцензії.

Якщо під час капітальних витрат на первинне придбання була закуплена безстрокова ліцензія, то вона не несе витрат на щорічне утримання.

Кваліфікований електронний підпис має максимальний термін дії два роки, проте в більшості випадків, отримання нового особистого ключа у кваліфікованого надавача електронних послуг - безкоштовна послуга.

Результати розрахунку:

Визначена методика та умови дозволять розрахувати витрати на щорічне утримання конкурентних варіантів (табл. 4.2):

Таблиця 4.2 – Розрахунок витрат на щорічне утримання

№ з/п	Найменування	Одиниця виміру	К-ть	Ціна за од., грн.	Вартість, грн.	ПДВ, %	Всього, грн
Варіант 1							
1	Microsoft Azure AD	ліцензія	55	13495	742225	20	890670
2	F5 BIG-IP	ліцензія	1	122939	122939	20	147526
3	Lookout MES	ліцензія	55	564	6768	20	8121
4	Заміна особистого ключа	послуга	55	безкоштовна			0
Всього (разом з ПДВ):							1046317
Варіант 2							
5	IT-Enterprise Cloud	ліцензія	55	11044	607420	20	728904
6	ІІТ Користувач ЦСК-1	ліцензія	1(55)	безстрокова			0
7	ІІТ Захист з’єднань-2	ліцензія	1(55)	безстрокова			0
8	Заміна особистого ключа	послуга	55	безкоштовна			0
Всього (разом з ПДВ):							728904
Варіант 3							
9	IT-Enterprise	ліцензія	55	3909	214995	без	214995
10	ІІТ Користувач ЦСК-1	ліцензія	1(55)	безстрокова			0
11	ІІТ Захист з’єднань-2	ліцензія	1(55)	безстрокова			0
12	Заміна особистого ключа	послуга	55	безкоштовна			0
Всього (разом з ПДВ):							214995
Варіант 4							
13	ІІТ Захист SAP	ліцензія	1	безстрокова			0
14	ІІТ Захист з’єднань-2	ліцензія	1(55)	безстрокова			0
15	Заміна особистого ключа	послуга	55	безкоштовна			0
Всього (разом з ПДВ):							0

4.3 Визначення економічної ефективності

Методика та умови розрахунку:

Особливості бухгалтерського обліку операцій з придбання програмного забезпечення, а саме: ліцензійне програмне забезпечення закуповується на певних умовах, які зазначаються у договорі, оскільки такий об’єкт не може використовуватися, доки на нього не отримано відповідних майнових прав, а сам такий об’єкт закупівлі відноситься до нематеріальних активів з невизначеним строком корисного використання.

Із врахуванням вимог до фінансової звітності, що визначені [112-114], з уточненням, наданим в п. 2.5 [113], нематеріальні активи з невизначеним строком корисного використання амортизації не підлягають, а в п. 1.1 [113] зазначено, що бюджетні установи та підприємства, відповідно до законодавства застосовують міжнародні стандарти бухгалтерського обліку та фінансової звітності.

До групи міжнародних стандартів фінансової звітності, відноситься стандарт IAS 38 «Нематеріальні активи» [115], згідно якого враховуються капітальні витрати компанії за двома показниками:

- CAPEX (англ. *capital expenditures*) - капітальні витрати компанії на придбання та оновлення необоротних активів. Витрати компанії класифікуються як CAPEX у тому випадку, якщо йдеться про довгострокові нематеріальні активи з терміном дії понад один рік;

- OPEX (англ. *operational expenditure*) - операційні витрати компанії, пов'язані із забезпеченням поточної діяльності, а не із інвестиціями у майбутнє.

Відповідно, розрахунок капітальних витрат на придбання відноситься до фінансової звітності за показником CAPEX, розрахунок витрат на щорічне утримання відноситься до фінансової звітності за показником OPEX.

Розрахунок економічної ефективності того чи іншого варіанту визначається порівнянням конкурентних варіантів за цими показниками. Показник CAPEX розрахований в табл. 4.1, показник OPEX розрахований в табл. 4.2.

Порівняння конкурентних варіантів, що подібні за функціональним призначенням за показниками CAPEX та OPEX показано в таблиці 4.3 та таблиці 4.4 відповідно:

Таблиця 4.3 – Порівняння конкурентних варіантів 1 та 2

№ з/п	Аналоги за функціональним призначенням	CAPEX (капітальні витрати), грн.	OPEX (операційні витрати), грн./рік
1	Варіант 1	2498071	1046317
2	Варіант 2	888369	728904

Таблиця 4.4 – Порівняння конкурентних варіантів 3 та 4

№ з/п	Аналоги за функціональним призначенням	CAPEX (капітальні витрати), грн./рік	OPEX (операційні витрати), грн./рік
1	Варіант 3	374460	214995
2	Варіант 4	249465	0

Аналіз розрахунків. Програмні засоби відносяться до необоротних нематеріальних активів з невизначеним строком корисного використання.

При виборі конкурентних варіантів, близьких за показниками критеріїв інформаційної безпеки та подібних (аналогічних) за функціональним призначенням, слід ураховувати не тільки капітальні витрати на придбання CAPEX, а й послідуючі операційні витрати OPEX на їх щорічне утримання.

Витрати на щорічне утримання можуть як дорівнювати вартості капітальних витрат, так й досягати їх половинної вартості. З економічної точки зору перевагу слід віддавати варіантам з меншим показником OPEX.

Одна із складових операційних витрат на щорічне утримання – це закупівля (продовження терміну дії) ліцензій на використання програмних засобів. При наявності вибору видів ліцензії, з метою зменшення витрат необхідно обирати їх варіант: безстрокова (безумовно найкращий вибір), конкурентна ліцензія (з коефіцієнтом 1,5-2 до числа робочих місць), локальна ліцензія (одна ліцензія на одне робоче місце / користувача).

Висновки до розділу 4

Здійснено розрахунок капітальних витрат на придбання та витрат на щорічне утримання конкурентних між собою варіантів комплексу програмних засобів, розглянутих в попередніх розділах роботи.

З'ясовано, що: 1) програмне забезпечення згідно особливості бухгалтерського обліку операцій з придбання, відноситься до необоротних нематеріальних активів з невизначеним строком корисного використання; 2) ліцензійне програмне забезпечення закуповується на певних умовах, які зазначаються у договорі, оскільки такий об'єкт не може використовуватися, доки на нього не отримано відповідних майнових прав; 3) в більшості випадків, виключні майнові права інтелектуальної власності на програмні засоби не закуповуються; 4) нематеріальні активи з невизначеним строком корисного використання амортизації не підлягають; 5) згідно із статтею 26-1 Податкового кодексу, до 1 січня 2023 року звільняються від оподаткування податком на додану вартість операції з постачання програмної продукції, до якої відносяться криптографічні засоби захисту інформації; 6) при наявності вибору умов ліцензії, для зниження або оптимізації витрат на утримання програмних засобів, необхідно обирати наступні варіанти: безстрокова (за наявності, безумовно кращий вибір), конкурентна ліцензія (з коефіцієнтом 1,5-2 до числа робочих місць), локальна ліцензія (її вартість складає 0,667 від вартості конкурентної ліцензії); 7) отримання нового особистого ключа кваліфікованого електронного підпису, в більшості випадків, безкоштовна послуга.

Проведено визначення економічної ефективності шляхом порівняння конкурентних варіантів, що подібні за функціональним призначенням, за показниками капітальних витрат на придбання CAPEX та операційних витрат OPEX на їх щорічне утримання.

Продемонстровано, що витрати на щорічне утримання OPEX можуть як дорівнювати вартості витрат CAPEX, так й досягати їх половинної вартості.

Акцентовано увагу, що з економічної точки зору, перевагу слід віддавати варіантам з меншим показником OPEX.

ВИСНОВКИ

В кваліфікаційній роботі запропонований реально можливий практичний та концептуальний підхід підвищення кіберзахисту сучасних інформаційно-комунікаційних систем (різної конфігурації, структури, функціонального призначення) від складних та комплексних кібератак шляхом впровадження концепції архітектури нульової довіри на основі вдосконалених моделей доступу, автентифікації, політики безпеки, що здатні забезпечити практичну реалізацію цієї концепції з урахуванням вимог чинного законодавства в сферах кіберзахисту та захисту інформації.

В результаті проведеної роботи досягнута її мета та вирішені поставлені завдання, що дозволяє зробити узагальнені висновки:

1. Проаналізовано стан сучасного кіберзахисту. Розкрито сутність проблем кіберзахисту: появу системного глухого кута в галузі захисту інформації. Визначено основні проблеми сучасного стану кіберзахисту: 1) зростаюча динаміка кількості та видів шкідливого програмного забезпечення; 2) поява у вільному доступі так званих «конструкторів вірусів»; 3) низька ефективність антивірусних засобів та сумнівні перспективи їх розвитку; 4) наявність вразливостей «нульового дня», «люків», незадокументованих «входів» в системному та прикладному програмному забезпеченні; 5) відсутність національної системи верифікації іноземного програмного забезпечення на відсутність програмних та алгоритмічних закладок; 6) проблема необхідності проведення процедури оновлення та отримання оновлень програмного забезпечення через мережу Інтернет; 7) поява нових методів та способів зламу чи обходу криптографічного захисту інформації; 8) складність структури та технологій сучасних інформаційно-комунікаційних систем внаслідок розвитку інформаційних технологій, їх вразливість перед кіберзагрозами, відсутність дієвого захисту після подолання порушником периметру безпеки; 9) суттєва зміна тактики, сценаріїв, складності та інструментів проведення кібератак.

Виокремлено три основних фактори проблем кіберзахисту: 1) еволюцію кібератак та шкідливого програмного забезпечення; 2) цифрову трансформацію; 3) необхідність зміни парадигми кіберзахисту.

Встановлено, що дослідженню проблем кіберзахисту та заходам з їх вирішення приділяється достатня увага на всіх рівнях: науковому, законодавчому, технічному, організаційному тощо. Однак, незважаючи на значну кількість підходів до вирішення означених проблем, вони залишаються актуальними не тільки для України, але й для всієї світової спільноти в цілому.

2. Проаналізовано небезпеку еволюції шкідливого програмного забезпечення та кібератак. Встановлено їх взаємозв'язок. Опис результатів аналізу корисний в практичній діяльності для організації захисту від цільових кібератак, зокрема: 1) використанням моделей Cyber Kill Chain, Unified Kill Chain та їх модифікацій; 2) використанням бази знань ATT&CK, доступної на офіційному сайті некомерційної організації MITRE для аналізу існуючих та потенційних кіберзагроз, планування засобів управління захистом, пошуку загроз, виявлення та розслідування кіберінцидентів, інтеграції інструментів безпеки, обміну аналітичною та оперативною інформацією про атаки, джерела загроз або злочинні групи, для підвищення ефективності використання засобів управління захистом, тестування на проникнення та імітації цілеспрямованих кібератак з метою оцінки кібербезпеки систем та інфраструктури в цілому.

3. Систематизовано вимоги законодавства України у сферах захисту інформації в інформаційно-комунікаційних системах, захисту державних інформаційних ресурсів, кіберзахисту об'єктів критичної інфраструктури, здійснення технічного та криптографічного захисту інформації, сфері електронних довірчих послуг на предмет виокремлення обов'язкових вимог для урахування при впровадженні рішень, запропонованих в даній роботі.

4. З'ясовано, що перспективним рішенням (щодо реальності практичного впровадження) зміни парадигми кіберзахисту є архітектура нульової довіри. Приведено непрямі та прямі доводи такого факту: 1) результати досліджень провідних компаній Microsoft та Panda Security; 2) указ Президента США про

підвищення рівня національної кібербезпеки від 12.05.2021 року, в якому архітектура нульової довіри визнається «найкращим методом безпеки», а федеральному уряду та різним відомствам встановлюються завдання та терміни впровадження архітектура нульової довіри.

Акцентовано увагу на факт відсутності у вільному доступі наукових праць чи статей з дослідження практичного застосування концепції нульової довіри, що становить проблему для широкого застосування концепції архітектури нульової довіри.

Приведено достовірні джерела інформації про архітектуру нульової довіри: спеціальні публікації NIST 800-207 та NIST 1800-35B, зроблено їх короткий огляд на основі авторського технічного перекладу, виділено необхідні аспекти, висвітлено принципи архітектури нульової довіри та приклади практичної реалізації, необхідні для розуміння цієї концепції та її застосування.

Визначено інновацію архітектури нульової довіри в новому підході до принципів використання двох основних компонентів безпеки: процедур автентифікації та авторизації при наданні доступу до кожного ресурсу, та механізму надання доступу.

5. Побудовано формалізовані моделі обраного рішення організації процедур автентифікації, доступу та політики безпеки доступу користувачів до ресурсів, реалізованих на принципах нульової довіри, здійснено їх аналіз, запропоновано варіанти вдосконалення.

Продемонстровано можливість самостійного застосування вдосконаленої моделі автентифікації з використанням можливостей програмних та апаратних засобів криптографічного захисту інформації в будь-яких кіберфізичних системах, що використовують технології web-доступу до функцій або ресурсів.

З’ясовано особливість застосування вдосконаленої моделі доступу: практична реалізація можлива тільки із використанням розробленої моделі політики безпеки доступу, та тільки в системах типу ERP та SAP. Проте, окремі можливості та особливості цієї моделі можуть бути використані для модифікації існуючих в системах моделей сімейства RBAC.

Використані при моделюванні підходи, методики та напрацювання можуть знайти подальшого розвитку іншими дослідниками.

6. Проведено пошук програмних засобів вітчизняного виробництва для практичної реалізації процедур автентифікації, доступу та політики безпеки доступу.

Доведено, що при оцінюванні придатності засобів-аналогів, необхідно додатково до критеріїв функціональних можливостей, враховувати критерій відповідності нормам чинного національного законодавства.

Такий підхід та застосовані методи вивчення аналога (прототипу) та метод еталонного оцінювання можуть знайти подальшого розвитку іншими дослідниками.

7. Проведено експериментальне впровадження вдосконалених моделей автентифікації, доступу та політики безпеки доступу в реальній інфраструктурі (інформаційно-комунікаційній системах).

Здійснено деталізоване вивчення реалізованого процесу автентифікації за допомогою співвідношення з описами, наведеними в технічній документації виробників програмних засобів та задокументованими в експертних висновках за результатами державної експертизи у сфері технічного або криптографічного захисту інформації.

Проаналізовано результати практичної реалізації моделей, сформульовані відповідні висновки, зазначені виявлені слабкі та сильні сторони, особливості, рекомендації.

Порівняно результати практичної реалізації на двох різних платформах, наведено висновки та виявлені особливості.

Запропоновано застосування вдосконалених моделей та програмного комплексу захисту «ІІТ Захист SAP-системи» для підвищення можливостей та безпеки застарілих SAP-систем, що знаходяться в експлуатації для організації.

8. Здійснено розрахунок капітальних витрат на придбання та витрат на щорічне утримання конкурентних між собою варіантів комплексу програмних засобів, розглянутих в даній роботі.

Проведено визначення економічної ефективності шляхом порівняння конкурентних варіантів (що подібні за функціональним призначенням) за показниками капітальних витрат на придбання CAPEX та операційних витрат OPEX на їх щорічне утримання.

Продемонстровано, що витрати на щорічне утримання OPEX можуть досягати половинної вартості капітальних витрат CAPEX.

Акцентовано увагу, що з економічної точки зору, перевагу слід віддавати варіантам з меншим показником OPEX, що надає можливість оптимальних витрат бюджетних коштів та уникнення проблем з фінансуванням щорічного утримання програмних продуктів.

Отримані результати дозволяють виокремити два важливих аспекти дослідження:

1. Доведено можливість використання програмних та апаратних засобів вітчизняного виробництва, які відповідають обов’язковим вимогам законодавства та нормативно-правових актів в сфері технічного та криптографічного захисту інформації, для практичного впровадження концепції архітектури нульової довіри.

2. Продемонстровано здатність реалізованого підходу підвищити ефективність захисту реальних інформаційних та кіберфізичних систем різного призначення та архітектури від складних, цільових та комплексних кібератак, та, відповідно, вирішити більшість проблем сучасного стану кіберзахисту, наведених в роботі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Killing the Computer to Save It / The New York Times, Oct. 29, 2012. https://www.nytimes.com/2012/10/30/science/rethinking-the-computer-at-80.html

2. Robert NM Watson. Computers: It's Time to Start Over / IEEE Spectrum, 26 Dec. 2012. https://spectrum.ieee.org/computers-its-time-to-start-over

3. Robert NM Watson. Reflections on decade of operating system access control extensibility / Communications of the ACM 56(2), January 2013.

4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2021.– №11 (листопад). – 327 с.

5. Андреев Н.О. Перспективы развития антивирусных продуктов / Прикладная информатика. Информационная безопасность. Инструментальные средства. № 1(19) 2019. С. 75-79.

6. Горобец А.А., Куницкий А.В., Парфентий, А.Н., Чувило О.А. Проблемы антивирусной индустрии, методы борьбы с компьютерными угрозами и ближайшие перспективы развития / РИ, 2006, № 4. С. 38-43.

7. Захарченко А.А., Хажмурадов М.А. Динаміка мережевих епидемій та эфективність систем захисту / АСУ и приборы автоматики. Харків. 2008. Вип. 144. С. 189-193.

8. Гребенькова Ю.А., Лопатин Д.В. Современное антивирусное программное обеспечение / Психолого-педагогический журнал «Гаудеамус». 2010. №2 (16). С. 1-2.

9. Петренко В.И., Требуева Ф.Б, Анзоров А.Р., Стручков И.В. Метод защиты системы машинного обучения от вредоносных программ / Caspian journal: Control and High Technologies. 2022. № 1 (57). С. 113-127.

10. Bolum, Wang, Yuanshum, Yao, Shawn, Shan, Huiying, Li.Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks. Conference: 2019 IEEE Symposium on Security and Privacy, 2019.

11. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2021.– №6 (червень) . – 261 с.

12. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2022.– №9 (вересень). – 311 с.

13. Офіційний документ. Executive Order on Improving the Nation's Cybersecurity. The White House. May 12, 2021.

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

14. Андреев А.Г., Казаков Г.В., Корянов В.В. Методический подход к выявлению программных закладок в специальном программном обеспечении систем критических приложений / Инженерный журнал: наука и инновации. Вып. 7.·2021. С. 1-14.

15. Вареница В.В., Марков А.С., Савченко В.В., Цирлов В.Л. Практические аспекты выявления уязвимостей при проведении сертификационных испытаний программных средств защиты информации / Вопросы кибербезопасности. 2021. № 5(45). С. 36-44.

16. Логінов І. Кіберзагрози, пов'язані з використанням іноземного програмного забезпечення, і досвід окремих держав з їх попередження / Global Cyber Security Forum: збірник матеріалів Першого міжнародного науково-практичного форуму, 14-16 листопада 2019 р. / М-во освіти і науки України, Харків. Нац. ун-т радіоелектроніки. Харків: ХНУРЕ. 2019. С. 61-63.

17. Закон України «Про основні засади забезпечення кібербезпеки України» Відомості Верховної Ради, 2017, № 45, ст.403.

18. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ: НАУ, 2013. 432 с.

19. Козюра В.Д., Хорошко В.О. Як протистояти реальним кіберзагрозам об'єктам критичної інфраструктури України. Кібербезпека в Україні: правові та організаційні питання: матеріали Всеукр. наук.-практ. конф., м. Одеса, 17 листопада 2017 р. Одеса: ОДУВС, 2017. С. 79–80.

20. Бараненко Р.В. Кібератаки як одна із форм кібертероризму / Вчені записки Таврійського національного університету ім. В.І. Вернадського, Серія: Технічні науки, Т.32(71), №1,Ч.1, 2021, С.45-50.

21. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка.- К.: ДУТ, 2015.- 288 с.

22. Яковів І.Б. Кібернетична модель APT атаки / Information Technology and Security. 2018. Vol. 6, Iss. 1. С. 46-58.

23. Котенко А.М., Ясько М.С. Забезпечення кіберзахисту комп'ютерної мережі об'єкта інформаційної діяльності / Сучасний захист інформації №4(48). 2021. С. 64-68.

24. Скирда А.В. Дослідження застосування кіберзброї проти України. // Матеріали Всеукраїнської науково-практичної інтернет-конференції. Молодь в науці: дослідження, проблеми, перспективи (МН-2022). – 2022.

URL: https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/16284/13708

25. Bahrami P.N. et al. Cyber kill chain-based taxonomy of advanced persistent threat actors: analogy of tactics, techniques, and procedures / P.N.Bahrami, A.Dehghantanha, T.Dargahi, R.M.Parizi, K.K.R.Choo, H.H.Javadi / Journal of information processing systems. 2019. Vol. 15. No.4. P.865-889.

26. Kim H., Kwon H.J., Kim K.K. Modified cyber kill chain model for multimedia service environments / Multimedia Tools and Applications. 2019. Vol.78. No.3. P. 3153-3170.

27. Bhatt P., Yano E.T., Gustavsson P. Towards a framework to detect multi–stage advanced persistent threats attacks / 2014 IEEE 8 international symposium on service-oriented system engineering. - IEEE, 2014.

28. Siddiqi M.A., Ghani N. Critical analysis on advanced persistent threats / International Journal of Computer Applications. 2016. Vol.141. No.13. P.46-50.

29. Hahn A. et al. A multi-layered and kill-chain based security analysis framework for cyber-physical systems / International Journal of Critical Infrastructure Protection. 2015. Vol.11. P.39-50.

30. Yadav T., Rao A.M. Technical aspects of cyber kill chain / International Symposium on Security in Computing and Communication. (SSCC 2015). Springer, Cham, 2015. Vol.536. P.438-452.

31. Case D.U. Analysis of the cyber attack on the Ukrainian power grid / Electricity Information Sharing and Analysis Center (E- ISAC). 2016. Vol.388. P.1-29.

32. Dargahi T. et al. A cyber- kill- chain based taxonomy of crypto ransomware features / Journal of Computer Virology and Hacking Techniques. 2019. Vol.15. No.4. P.277– 305.

33. PandaLabs Panda Security. Понимание кибер-атак. Часть I. Cyber-Kill Chain. https://www.cloudav.ru/upload/iblock/08c/PAD_PADCyber-Kill20Chain.pdf

34. ATT&CK Enterprise Matrix [Електронний ресурс] - Режим доступу до ресурсу: https://attack.mitre.org/matrices/enterprise/

35. Finding Cyber Threats with ATT&CK-Based Analytics [Текст] / Blake E. Strom Joseph A. Battaglia Michael S. Kemmerer William Kupersanin Douglas P. Miller Craig Wampler Sean M. Whitley Ross D. Wolf - 2017 The MITRE Corporation - 53 с.

36. Куренная В.О. Искусственный интеллект в информационной безопасности / Научно-образовательный журнал для студентов и преподавателей «StudNet» №6. 2022. С. 7202-7208.

37. Ocheredko Andrey R. Research of IRP-systems based on the analysis of mechanisms of response to information security incidents / Caspian journal: Control and High Technologies. № 1 (53). 2021. P. 63-74.

38. Отчет Panda Security «Понимание угроз 2020». Режим доступу: https://iitd.com.ua/wp-content/uploads/2020/05/pandalabs-threat-insights-2020.pdf

39. Microsoft Security. Zero Trust Adoption Report. 2021. Режим доступу: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWGWha

40. Швыряев П.С. Утечки конфиденциальных данных: главный враг внутри / Вестник государственного управление. Выпуск № 91. Апрель 2022. С. 226-241.

41. NIST Special Publication 800-207 Zero Trust Architecture.

42. NIST Special publication 1800-35B Implementing a Zero Trust Architecture.

43. Закон України «Про захист інформації в інформаційно-комунікаційних системах». Відомості Верховної Ради України, 1994, № 31, ст.286

44. Закон України «Про електронні довірчі послуги». Відомості Верховної Ради, 2017, № 45, ст.400.

45. Технічний документ. Інтегрована система електронної ідентифікації. Порядок обробки інформації у системі ЄААД.468244.209 Д7.01.

46. Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затверджений постановою Кабінету Міністрів України від 19.09.2018 № 749.

47. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518.

48. Перелік стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.10.2020 № 687.

49. ДСТУ ISO/IEC 9798-3:2014 «Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3. Механізми з використанням методу цифрового підпису».

50. ДСТУ ETSI TS 119 312:2015 «Електронні підписи й інфраструктури (ESI). Криптографічні комплекти».

51. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння».

52. ITU-T Recommendation X.805. Security architecture for end-to-end communications.

53. Девянин П.Н. Обзорные лекции по моделям безопасности компьютерных систем / Прикладная дискретная математика, приложение к № 2. Изд. Института криптографии, связи и информатики: М. 2009. С. 151–190.

54. Медведев Н.В. Концепция открых систем и задача аутентификации в локальных сетях / Вестник МГТУ им. М.Э. Баумана. Сер. «Приборостроение». №1 2005. С. 52-62.

55. Марков А.С., Цирлов В.Л. Безопасность доступа: подготовка к CISSP Вопросы кибербезопасности № 2(10). 2015. С. 60-68.

56. Вишняков В.А., Гондаг-Саз М.М. Модели и средства аутентификации пользователей в корпоративных системах управления и облачных вычислениях/ Доклады БГУИР № 3 (97). 2016. С. 111-114.

57. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : моногр. / Ю.І. Горбенко, І.Д. Горбенко. М-во освіти і науки України, Харків. Нац. ун-т радіоелектроніки – Харків : Форт, 2010. – 608 с.

58. Шляхтина Е.А., Гамаюнов Д.Ю. Схема групповой аутентификации на основе доказательства с нулевым разглашением / Математические основы компьютерной безопасности № 51. 2021. С. 68-84.

59. Рацеев С.М., Ростов М.А. О протоколах аутентификации с нулевым разглашением знания / Изв. Сарат. ун-та. Сер. Математика. Механика. Информатика. Т. 19, вып. 1. 2019. С. 114-121.

60. Бондаренко О.В., Карпінець В.В. Двофакторна аутентифікація в системах контролю і управління доступом / Тези доповідей Всеукраїнської науково-практичної Інтернет-конференції студентів, аспірантів та молодих

науковців «Молодь в науці: дослідження, проблеми, перспективи» (МН-2020), м. Вінниця, 18-29 травня 2020 р. 2020.

61. Маницький В.Є. REVERSE-SHELL як інструмент отримання несанкціонованого доступу / Сучасний захист інформації №1(49), 2022. С. 34-37.

62. Порядок ведення Довірчого списку, затверджений наказом Міністерства цифрової трансформації України від 08.07.2020 № 104.

63. ITU-T Recommendation X.509. Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

64. Белим С.В., Богаченко Н.Ф. Применение метода анализа иерархий для оценки рисков утечки полномочий в системах с ролевым разграничением доступа / Защита информации № 6. 2013. С. 67-72.

65. Белим С.В., Белим С.Ю, Богаченко Н.Ф. Теоретико-графовый анализ ролевой политики безопасности / Математические структуры и моделирование. Вып. 19. 2009. С. 85-96.

66. Салієва О.В., Яремчук Я.Ю. Порівняння моделей інформаційної безпеки за характеристиками суб`єктів / Матеріали 23-го міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті»: конференція «Управління знаннями та конкурентна розвідка», 16-18 квітня 2019 р. Харків, 2019. С. 67-68.

67. Девянин П.Н. Формирование словаря терминов теории моделирования безопасности управления доступом и информационными потоками в компьютерных системах / Прикладная дискретная математика. № 2. 2011. С. 17-39.

68. Волинець О.Ю., Куліш Д.В., Приймак А.В., Яремчук Я.Ю. Удосконалення моделі керування доступом на основі ролей у приватних хмарних середовищах / Реєстрація, зберігання і обробка даних. 2019. Т. 21, № 4. С. 49-57.

69. Девянин П.Н. Базовая ролевая ДП-модель / Прикладная дискретная математика. № 1. 2018. С. 64-70.

70. Колегов Д.Н. Построение иерархического ролевого управления доступом / Прикладная дискретная математика. № 3(17). 2012. С. 70-76.

71. Колегов Д.Н. О построении иерархического ролевого управления доступом / Прикладная дискретная математика. Прил. к № 4. 2012. С. 69-71.

72. Armando A., Ranise S. Scalable automated symbolic analysis of administrative role-based access control policies by SMT solving / J. of Computer Security. 2012. Vol. 20. № 4. P. 309–352.

73. Kuhn D. R., Coyne E. J., and Weil T. R. Adding attributes to role-based access control / IEEE Computer. 2010. №. 43(6). P. 79–81.

74. Кузнецов О.О., Король О.Г., Босько В.В., Євсеєв С.П. Методика дослідження колізійних властивостей кодів автентифікації повідомлень / Військово-технічний збірник. № 2 (25). 2011. С. 23-30.

75. National Institute of Standards and Technology. Role Based Access Control (RBAC) and Role Based Security.

76. Ferraiolo D.F., Kuhn D.R. Role-Based Access Control / 15th National Computer Security Conference. 1992. P. 554–563.

77. Богаченко Н.Ф., Филиппова А.В. Ранжирование полномочий на основе анализа иерархии ролей в моделях разграничения доступа / Математические структуры и моделирование. 2019. № 1(49). С. 89–96.

78. Салієва О.В., Яремчук Я.Ю. Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури / Безпека інформації. 2020. Т. 26, № 2. С. 64-73.

79. Девянин П.Н., Кулямин В.В., Петренко А.К., Хорошилов А.В., Щепетков И.В. Интеграция мандатного и ролевого управления доступом и мандатного контроля целостности в верифицированной иерархической модели безопасности операционной системы / Труды ИСП РАН. Том 32. Вып. 1, 2020. С. 7-26.

80. Булдакова Т.И., Коршунов А.В. Обеспечение информационной безопасности ERP-систем / Вопросы кибербезопасности. №5(13). Специальный выпуск. 2015. С. 41-44.

81. Егорова Г.В., Шляпкин А.В. Информационная безопасность ERP-систем / Информационные системы и технологии: управление и безопасность. 2013. №2. С. 202-211.

82. Титов А.В., Скиба В.Ю., Силенко А.В., Рыжов Ю.Н. Модели и методы описания политик безопасности для управления доступом в распределительных информационных системах / Математическое моделирование: методы, алгоритмы, технологии / Научно-технические ведомости. СПб. ГПУ. № 4. 2009. С. 176-182.

83. Усов С.В. О представлении некоторых ролевых моделей разграничения доступа объектно-ориентированной моделью HRU / Математические структуры и моделирование. 2018. № 4(48). С. 128-138

84. Belim S.V., Belim S.Y., Bogachenko N.F., Kabanov A.N. User Authorization in a System with a Role-Based Access Control on the Basis of the Analytic Hierarchy Process / IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics). 14-16 Nov., 2017. P. 1-5.

85. Сенцова А.Ю., Машкина И.В. Разработка частной политики информационной безопасности системы облачных вычислений / Вестник УГАГУ. Т. 20, № 2(72). 2016. С. 134–142.

86. Харитонов Д.А. Алгоритм поиска аналога и прототипа / Вестник ОГУ. 2015. № 3 (178). С. 249 -257.

87. Петрова И.Ю., Пучкова А.А. Методика проведения патентного анализа с целью поиска аналогов и прототипов полученных технических решений / Mordovia university bulletin. Том. 26. №. 1. 2016. С. 50-

88. Radauer A., Walter L. Elements of good practice for providers of publicly funded patent information services for SMEs – Selected and amended results of a benchmarking exercise / World Patent Information. 2010. Vol. 32. Issue 3. P. 237-245.

89. Farhadzadeh E.M., Muradaliyev A.Z., Tagiyeva D.E. Operative Benchmarking Same Type Technical Objects / RT&A. 2020. № 2. Vol. 15, P. 50-53.

90. Експертний висновок у сфері технічного захисту інформації на «Комплекс засобів захисту Комп’ютерної програми (системи управління

підприємством) «IT-Enterprise» («IT-Підприємство», «IT-Предприятие»), розробки ТОВ НВП «Інформаційні технології», зареєстрований в Адміністрації Держспецзв'язку за № 31Е, дійсний з 31.08.2022 до кінця воєнного стану.

91. Експертний висновок у сфері криптографічного захисту інформації на «Комплекс програмний користувача центру сертифікації ключів «ІІТ Користувач ЦСК-1»», розроблений ПрАТ «Інститут інформаційних технології», зареєстрований в Адміністрації Держспецзв'язку за № 04/05/02-1277 від 29.04.2021, дійсний до 29.04.2026.

92. Експертний висновок у сфері криптографічного захисту інформації на «Комплекс програмний захисту мережних з’єднань «ІІТ Захист з’єднань-2. Клієнт захисту з’єднань», розроблений ПрАТ «Інститут інформаційних технології», зареєстрований в Адміністрації Держспецзв'язку за № 04/03/02-1188 від 15.05.2020, дійсний до 15.05.2025.

93. Технічний документ. Комплекс користувача ЦСК. Загальний опис системи. ЄААД.468244.021 ПД.02.

94. Технічний документ. Програмний комплекс користувача ЦСК. Бібліотека підпису користувача ЦСК. Версія 1.3.1. ЄААД.21107-13 13 01-1.

95. Технічний документ. Програмний комплекс користувача ЦСК. Бібліотека користувача ЦСК (ОС Microsoft Windows). Версія 1.3.1. Опис програми. Настанова програміста. Настанова системного програміста. ЄААД.21107-13 13/32/33 01-1.

96. Технічний документ. Програмний комплекс користувача ЦСК. Бібліотека користувача ЦСК (java-аплет). Версія 1.3.1. Опис програми. Настанова програміста. Настанова системного програміста. ЄААД.21107-13 13/32/33 09-1.

97. Технічний документ. Програмний комплекс користувача ЦСК. Web-бібліотеки підпису користувача ЦСК. Версія 1.3.1. Настанова оператора. ЄААД.21118-13 34 01-1.

98. Технічний документ. Комплекс захисту SAP-системи. Загальний опис системи. ЄААД.468244.081 ПД.

99. Технічний документ. Засоби автентифікації користувачів ЦСК (OAuth). Загальний опис системи. ЄААД.468244.206 ПД.

100. Технічний документ. Комплекс захисту мережних з'єднань (TCP/IP). Загальний опис системи. ЄААД.468244.094 ПД.

101. Технічний документ. Електронний ключ «Кристал-1» Настанова з експлуатації ЄААД.469535.040 РЭ.

102. Експертний висновок у сфері криптографічного захисту інформації на «Електронний ключ «Кристал-1», зареєстрований в Адміністрації Держспецзв'язку за № 04/05/02-998 від 14.04.2021, дійсний до 18.01.2023.

103. Скирда А.В. Дослідження необхідності та номенклатури захищених носіїв особистих ключів в Україні // Матеріали Всеукраїнської науково-практичної інтернет-конференції. Молодь в науці: дослідження, проблеми, перспективи (МН-2022). – 2022.

URL: https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/14264/12091

104. Закон України «Про публічні закупівлі». Відомості Верховної Ради, 2016, № 9, ст.89.

105. Загальні вимоги до програмних продуктів, які закуповуються та створюються на замовлення державних органів, затверджені постановою Кабінету Міністрів України від 12.08.2009 № 869.

106. Економічна класифікація видатків бюджету, затверджена наказом Міністерства фінансів України від 14.01.2011 № 11 (у редакції наказу Міністерства фінансів України від 26.12.2011 № 1738).

107. Інструкція щодо застосування економічної класифікації видатків бюджету, затверджена наказ Міністерства фінансів України 12.03.2012 № 333 (у редакції наказу Міністерства фінансів України 21.06.2012 № 754).

108. Національний класифікатор України. Єдиний закупівельний словник ДК 021:2015, введений в дію наказом Міністерства економічного розвитку України від 23.12.2015 № 1749 (із змінами та доповненнями, введеними в дію наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 24.04.2020 № 783).

109. Закон України «Про бухгалтерський облік та фінансову звітність в Україні. Відомості Верховної Ради України, 1999, № 40, ст.365.

110. Положення, про порядок бухгалтерського обліку окремих активів та операцій підприємств державного, комунального секторів економіки і господарських організацій, які володіють та/або користуються об'єктами державної, комунальної власності, затверджене наказом Міністерства фінансів України від 19.12.2006 № 1213 (із змінами та доповненнями, введеними в дію наказом Міністерства фінансів України від 09.07.2021 № 385).

111. Податковий кодекс України. Відомості Верховної Ради України, 2011, № 13-14, № 15-16, № 17, ст.112).

112. Національне положення (стандарт) бухгалтерського обліку 1 «Загальні вимоги до фінансової звітності», затверджене наказом Міністерства фінансів України від 07.02.2013 № 73.

113. Методичні рекомендацій щодо облікової політики підприємства, затверджених наказом Міністерства фінансів України від 27.06.2013 № 635.

114. Порядок подання фінансової звітності, затверджений постановою Кабінету Міністрів України від 28.02.2000 № 419.

115. Міжнародні стандарти фінансової звітності. IAS 38 «Нематеріальні активи». Переклади, актуалізовані та погоджені. Офіційний сайт Міністерства фінансів України. [Електронний ресурс] Режим доступу: https://mof.gov.ua/uk/msfz

Додаток А

Технічне завдання

Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ
Голова секції «Управління інформаційною безпекою» кафедри МБІС
д.т.н., професор
_____ Юрій ЯРЕМЧУК
«24» вересня 2022 року

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

«Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки»

08-72.МКР.009.00.000.ТЗ

Керівник магістерської кваліфікаційної роботи
д.т.н., професор каф. МБІС
_____ Ю.Є. Яремчук

Вінниця – 2022 р.

1. Найменування та область застосування

Підвищення кіберзахисту від складних та комплексних кібератак шляхом впровадження концепції архітектури нульової довіри на основі вдосконалених моделей доступу, автентифікації, політики безпеки, що здатні забезпечити практичну реалізацію цієї концепції з урахуванням вимог чинного законодавства в сферах кіберзахисту та захисту інформації. Область застосування: кіберзахист.

2.Підстава для проведення робіт

Робота виконується на основі наказу ректора ВНТУ № 203 від 14. 09. 2022 р.

3. Мета та призначення МКР

3.1 Мета: дослідження практичних та концептуальних підходів підвищення кіберзахисту сучасних інформаційно-комунікаційних систем (різної конфігурації, структури, функціонального призначення) від складних та комплексних кібератак шляхом впровадження концепції архітектури нульової довіри на основі вдосконалених моделей доступу, автентифікації, політики безпеки, що здатні забезпечити практичну реалізацію цієї концепції з урахуванням вимог чинного законодавства в сферах кіберзахисту та захисту інформації.

3.2 Призначення: підвищення ефективності кіберзахисту інфраструктури, вирішення основних проблем сучасного стану кіберзахисту.

4. Джерела розробки

4.1. Method of user authentication by keyboard handwriting based on neural networks and genetic algorithm / Andrii Pryimak, Yurii Yaremchuk, Olha Salieva, Vasyl Karpinets, Nataliia Kunanets // Proceedings of the International Workshop of IT-professionals on Artificial Intelligence (ProfIT AI 2021). – Kharkiv, Ukraine, September 20-21, 2021, P. 141-149..

4.2. Бондаренко О.В., Карпінець В.В. Двофакторна аутентифікація в системах контролю і управління доступом / Тези доповідей Всеукраїнської науково-практичної Інтернет-конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи» (МН-2020), м. Вінниця, 18-29 травня 2020 р. 2020.

4.3. Волинець О.Ю., Куліш Д.В., Приймак А.В., Яремчук Я.Ю. Удосконалення моделі керування доступом на основі ролей у приватних хмарних середовищах / Реєстрація, зберігання і обробка даних. 2019. Т. 21, № 4. С. 49-57.

4.4. NIST Special Publication 800-207 Zero Trust Architecture.

4.5. NIST Special publication 1800-35B Implementing a Zero Trust Architecture.

4.6. Законодавство України у сферах захисту інформації в інформаційно-комунікаційних системах, захисту державних інформаційних ресурсів, кіберзахисту об’єктів критичної інфраструктури, здійснення технічного та криптографічного захисту інформації, сфері електронних довірчих послуг.

5. Вимоги до виконання МКР

Для досягнення мети необхідно вирішити наступні завдання:

- провести пошук, збір, систематизацію та аналіз інформації для вивчення сучасного стану кіберзахисту, виявити тенденції його розвитку, основні проблеми, виокремити причини та фактори проблем, запропонувати можливий концептуальний варіант підвищення ефективності кіберзахисту від складних та комплексних кібератак;

- проаналізувати еволюцію шкідливого програмного забезпечення та кібератак, сценарії реалізації складних та комплексних кібератак;

- систематизувати вимоги законодавства України з кіберзахисту, виокремити вимоги, необхідні для врахування при опрацюванні окремих завдань дослідження;

- урахувати іноземний досвід впровадження концепції архітектури нульової довіри, виокремити основні принципи, аспекти, складності застосування, інновації в підході до процедур автентифікації та доступу, навести приклад достовірної практичної реалізації, оцінено можливість подібної реалізації із використанням апаратних, програмних засобів вітчизняного виробництва та з урахуванням вимог чинного законодавства;

- побудувати формалізовані моделі обраного рішення організації процедур автентифікації, доступу та політики безпеки доступу користувачів до ресурсів,

реалізованих на принципах нульової довіри, здійснити їх аналіз, запропонувати варіант вдосконалення;

- провести пошук програмних та апаратних засобів вітчизняного виробництва для практичної реалізації процедур автентифікації, доступу та політики безпеки доступу;

- здійснити практичне впровадження вдосконалених моделей автентифікації, доступу та політики безпеки доступу в реальній інфраструктурі (інформаційно-комунікаційній системах), проаналізувати отримані результати;

- провести економічний розрахунок запропонованих рішень, порівняти конкурентні варіанти, оцінити економічну ефективність.

6. Вимоги до розроблення документації

Оформлення МКР повинно відповідати вимогам державних стандартів України, зокрема ДСТУ 3008:2015, ДСТУ 8302:2015.

7. Техніко-економічні показники

7.1 Цінність результатів використання даного проекту повинна перевищувати витрати на його реалізацію.

7.2 Обрані рішення та можливість їх практичної реалізації повинні бути орієнтовані на широкий загал.

8. Стадії та етапи розробки

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання теми	01.09.2022	15.09.2022
2	Аналіз предметної області обраної теми	15.09.2022	20.09.2022
3	Апробація отриманих результатів	20.09.2022	30.09.2022
4	Розробка алгоритму роботи	01.10.2022	10.10.2022
5	Написання магістерської роботи на основі розробленої теми	01.10.2022	20.11.2022
6	Розробка економічної частини	15.11.2022	20.11.2022
7	Попередній захист магістерської кваліфікаційної роботи	24.11.2022	25.11.2022
8	Перевірка магістерської кваліфікаційної роботи на наявність плагіату	28.11.2022	30.11.2022
9	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	01.12.2022	10.12.2022
10	Захист магістерської кваліфікаційної роботи	19.12.2022	21.12.2022

9. Вимоги до захисту інформації з обмеженим доступом

Для використання в роботі інформації з обмеженим доступом, що отримана під час переддипломної практики, необхідно отримання письмового дозволу та умов оприлюднення від власника (володільця) такої інформації. В такому випадку оформлення МКР здійснюється у відповідності до вимог законодавства із захисту інформації з обмеженим доступом.

10. Порядок контролю та прийому

Для приймання магістерської кваліфікаційної роботи надається:

- ПЗ до магістерської кваліфікаційної роботи;
- довідки про впровадження результатів;
- презентація;
- відгук керівника роботи;
- відгук опонента

Технічне завдання до виконання прийняв _____ **А.В.Скирда**

Додаток Б

Довідки про практичне впровадження результатів

ВІННИЦЬКА МІСЬКА РАДА
ДЕПАРТАМЕНТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Україна, 21050, Вінницька обл., Вінницький район, м. Вінниця, вулиця Соборна, 59
тел. (0432) 59-50-13, 59-51-50, 59-51-53, e-mail it@vmr.gov.ua

01.11.2022 № 13/00/019/163804

ДОВІДКА
про практичне впровадження результатів дослідження в рамках магістерської кваліфікаційної роботи Скирда Антона Вячеславовича на тему: «Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки»

Цією довідкою посвідчується, що практичні результати дослідження отримані студентом Вінницького національного технічного університету Скирда Антоном Вячеславовичем під час проходження переддипломної практики в період з 01.09.2022 по 28.10.2022 року в департаменті інформаційних технологій Вінницької міської ради.

Практична реалізація розроблених в рамках кваліфікаційної роботи моделей доступу, автентифікації та політики безпеки здійснювалась на кількох реальних інформаційно-комунікаційних системах, об'єднаних ERP-системою «IT-Enterprise». Для порівняння можливостей була створена альтернативна експериментальна платформа: на реальну локалізовану систему SAP R/3 встановлений програмний комплекс захисту «ІІТ Захист SAP-системи».

Отримані результати визнані такими, що заслуговують на увагу та мають потенціал практичного застосування з метою підвищення ефективності кіберзахисту реальних кіберфізичних систем різної архітектури та функціонального призначення.

Зокрема, налаштовану конфігурацію безпеки локалізованої системи SAP R/3 із встановленим програмним комплексом захисту «ІІТ Захист SAP-системи», після тестування системи захисту, залишено в подальшій експлуатації, що підвищує захищеність об'єкту критичної інфраструктури та дозволяє без додаткових фінансових витрат виконати в повному обсязі Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518.

Реалізація вдосконалених моделей доступу та політики безпеки в ERP-системі та відповідні налаштування теж залишені для практичного використання, модель автентифікації буде прийнята після забезпечення всіх користувачів захищеними носіями особистого ключа (за виявленою в ході експерименту особливістю, програмний продукт «IT-Enterprise» застосовує варіант автентифікації з формуванням параметру «Вхід по ключу електронного підпису» одразу для всіх без виключення груп користувачів, що ускладнює швидке впровадження).

Корисне значення має економічний розділ кваліфікаційної роботи, який повністю розкриває особливості закупівлі програмних засобів, продовження ліцензій на використання та розрахунок витрат на щорічне утримання. Результати прийняті до уваги при плануванні щорічних витрат.

Окремі практичні результати дослідження також ураховані в підпорядкованих департаменту комунальних підприємствах: «Вінницький інформаційний центр» та «Вінницякартсервіс».

Директор департаменту **Володимир РОМАНЕНКО**

КОМУНАЛЬНЕ ПІДПРИЄМСТВО
«ВІННИЦЯКАРТСЕРВІС»

21050, м. Вінниця, вул. Соборна, 36; Тел.: (0432) 65 51 55, Код ЄДРПОУ 39547113

26.10.2022 р. № 105/1

За місцем вимоги

ДОВІДКА
про впровадження результатів

Видана студенту Вінницького національного технічного університету Скирда Антону Вячеславовичу про те, що його ідеї та окремі результати дослідження, проведені в рамках опрацювання магістерської кваліфікаційної роботи на тему: «Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки» використані комунальним підприємством «Вінницякартсервіс».

Зокрема використано окремі можливості, що надають вдосконалена модель доступу та політика безпеки доступу:

- при доступі користувачів до інформаційної бази даних автоматизованої системи обліку оплати проїзду в громадському транспорті;
- при організації доступу технічних адміністраторів до кінцевих пристроїв системи автоматичного визначення місцезнаходження транспорту.

Довідка видана без фінансових зобов'язань перед автором та підтверджує передачу усіх майнових прав набувачеві КП «Вінницякартсервіс».

Директор **Катерина БАБІНА**

М.П.

КОМУНАЛЬНЕ ПІДПРИЄМСТВО "ВІННИЦЯКАРТСЕРВІС" Ідент. код 39547113 Україна м.Вінниця

КОМУНАЛЬНЕ ПІДПРИЄМСТВО

«ВІННИЦЬКИЙ ІНФОРМАЦІЙНИЙ ЦЕНТР»

ЄДРПОУ 36365026, Р/р UA 863204780000026008212002919 в ПАТ АБ "УКРГАЗБАНК", м. КИЇВ
ІПН 363650202287, № свід. ПДВ 100306819 Україна, 21050, м. Вінниця, вул. Соборна, 64, тел. 59-53-77

27.10.2022 № 194/2/15

ДОВІДКА
про використання результатів кваліфікаційної роботи

Довідка видана студенту групи УБ-21м Вінницького національного технічного університету СКИРДА Антону Вячеславовичу про те, що результати його дослідження, проведені в рамках магістерської кваліфікаційної роботи на тему: «Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки» використані комунальним підприємством «Вінницький інформаційний центр» в модулі забезпечення безпеки доступу до встановлених камер системи відеоспостереження, створеної в рамках програми «Безпечне місто»:

- скоригована встановлена політика доступу до камер системи відеоспостереження, що значно підвищило ефективність організаційно-технічних заходів із запобігання несанкціонованого доступу до камер відеоспостереження;
- введено двофакторну автентифікацію користувачів на основі особистих ключів та сертифікатів відкритих ключів кваліфікованого електронного підпису при доступі до бази даних зберігання архівних записів із використанням програмного комплексу користувача центру сертифікації ключів «ІІТ Користувач ЦСК-1» та програмного комплексу клієнта захисту мережних з'єднань «ІІТ Захист з'єднань-2. Клієнт захисту з'єднань» та персональних захищених носіїв особистого ключа.

Окремі ідеї та пропозиції планується використати при розробці Технічного завдання модернізації системи відеоспостереження «Безпечне місто» в 2023 році.

Довідка видана без фінансових та будь-яких інших зобов'язань перед автором.

Директор Сергій БРИГАДИР

Додаток В

Лістинги програмного коду

В.1 Ділянку (мова програмування C#), що приведена нижче:

```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Security.Cryptography.X509Certificates;
using Microsoft.IdentityModel.Tokens;

(...)

X509Certificate2 cert = new X509Certificate2("THE_X509_PEM_FILE_PATH");
RsaSecurityKey rsaSecurityKey = new RsaSecurityKey(cert.GetRSAPublicKey());
```

для читання особистого ключа в PKCS#1 необхідно змінити на:

```
using System;
using System.IO;
using System.Security.Cryptography;
using Microsoft.IdentityModel.Tokens;

(...)

string privateKeyPem = File.ReadAllText("THE_PEM_ENCODED_FILE_PATH");
// keeping only the payload of the key
privateKeyPem = privateKeyPem.Replace("-----BEGIN RSA PRIVATE KEY-----", "");
privateKeyPem = privateKeyPem.Replace("-----END RSA PRIVATE KEY-----", "");
byte[] privateKeyRaw = Convert.FromBase64String(privateKeyPem);
// creating the RSA key

RSACryptoServiceProvider provider = new RSACryptoServiceProvider();
provider.ImportRSAPrivateKey(new ReadOnlySpan<byte>(privateKeyRaw), out _);
RsaSecurityKey rsaSecurityKey = new RsaSecurityKey(provider);
```

В.2 Ділянка коду (мова програмування C#) для варіанту реалізації державних алгоритмів та протоколів повинна бути налаштована (необхідно встановити значення 1 та виправити EU на UA) таким чином:

```
public static int GeneratePrivateKeySilently
      EU_KEY_MEDIA keyMedia,            // Вхідний. Параметри носія
                                        // особистого ключа.
      int UAKeysType,                   // Вхідний. Тип ключа для державних
                                        // криптографічних алгоритмів та
                                        // протоколів
      int UADSKeysSpec,                 // Вхідний. Параметри ключа ЕЦП
                                        // для державних криптографічних
                                        // алгоритмів та протоколів
      int UAKEPKeysSpec,                // Вхідний. Параметри ключа
                                        // протоколу розподілу ключів
                                        // для державних криптографічних
                                        // алгоритмів та протоколів.
      string UAParamsPath,              // Вхідний. Каталог чи носій з
                                        // параметрами ЕЦП та протоколу
                                        // розподілу ключів для державних
                                        // криптографічних алгоритмів та
                                        // протоколів
ref byte[1] privKeyInfo,                // Вихідний. Інформація про
                                        // особистий ключ у вигляді
                                        // масиву байт (якщо null інформація
                                        // не повертається)
      ref byte[1] UARequest,            // Вихідний. Запит на сертифікат у
                                        // вигляді масиву байт для державних
                                        // криптографічних алгоритмів та
                                        // протоколів. Якщо генерується
                                        // ключ для міжнародних
                                        // криптографічних алгоритмів та
                                        // протоколів повинен дорівнювати
                                        // null
      ref string UAReqFileName,         // Вихідний. Ім’я файлу за
                                        // замовчуванням для запиту на
                                        // сертифікат для державних
                                        // криптографічних алгоритмів та
                                        // протоколів
```

```
        ref byte[1] UAKEPRequest,       // Вихідний. Запит на
                                        // сертифікат особистого ключа
                                        // протоколу розподілу ключів у
                                        // вигляді масиву байт для державних
                                        // криптографічних алгоритмів та
                                        // протоколів. Якщо генерується
                                        // ключ для міжнародних
                                        // криптографічних алгоритмів та
                                        // протоколів або якщо не потрібен
                                        // окремий ключ для протоколу
                                        // розподілу ключів повинен
                                        // дорівнювати null
    ref string UAKEPReqFileName,        // Вихідний. Ім'я файлу за
                                        // замовчуванням для запиту на
                                        // сертифікат особистого ключа
                                        // протоколу розподілу ключів для
                                        // державних криптографічних
                                        // алгоритмів та протоколів
        ref byte[1] privKeyInfo,        // Вихідний. Інформація про
                                        // особистий ключ у вигляді
                                        // масиву байт (якщо null інформація
                                        // не повертається)
        ref byte[1] UARequest,          // Вихідний. Запит на сертифікат у
                                        // вигляді масиву байт для державних
                                        // криптографічних алгоритмів та
                                        // протоколів. Якщо генерується
                                        // ключ для міжнародних
                                        // криптографічних алгоритмів та
                                        // протоколів повинен дорівнювати
                                        // null
        ref string UAReqFileName,       // Вихідний. Ім'я файлу за
                                        // замовчуванням для запиту на
                                        // сертифікат для державних
                                        // криптографічних алгоритмів та
                                        // протоколів
```

Додаток Г

Ілюстративний матеріал (презентація)

Магістерська кваліфікаційна робота

на тему:

Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки

Виконав: Скирда Антон Вячеславович

Керівник: Яремчук Юрій Євгенович

Актуальність

Поширення кіберзагроз на всі сфери життєдіяльності суспільства та держави в цілому, вдосконалення інструментарію реалізації кіберзагроз зумовлює необхідність перегляду стратегії та тактики протидії ним, пошук шляхів підвищення ефективності кіберзахисту від складних, комплексних та цільових кібератак. Що, в свою чергу, відповідає пріоритетам забезпечення кібербезпеки нашої держави та стратегічним цілям, визначеним Стратегією кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 № 447/2021.

Мета роботи

Вдосконалення моделей доступу, автентифікації, політики безпеки, що здатні забезпечити практичну реалізацію концепції архітектури нульової довіри з урахуванням вимог чинного законодавства в сферах кіберзахисту та захисту інформації

Завдання

1

Проведено пошук, збір, систематизацію та аналіз інформації для вивчення сучасного стану кіберзахисту, виявлено тенденції його розвитку, основні проблеми, виокремлено причини та фактори проблем, запропоновано можливий концептуальний варіант підвищення ефективності кіберзахисту від складних та комплексних кібератак

Проблеми кіберзахисту:

1. Зростаюча динаміка кількості та видів шкідливого програмного забезпечення.
2. Поява у вільному доступі «конструкторів вірусів».
3. Низька ефективність антивірусних засобів та сумнівні перспективи їх розвитку.
4. Наявність вразливостей «нульового дня» (від англ. zero day, 0-day), «люків» (від англ. trapdoor), незадокументованих входів» (англ. back door) в системному та прикладному програмному забезпеченні.
5. Відсутність національної системи верифікації іноземного програмного забезпечення на відсутність алгоритмічних закладок.
6. Процедура оновлення (update) та отримання оновлень програмного забезпечення здійснюються через мережу Інтернет.
7. Поява нових методів та способів зламу чи обходу криптографічного захисту інформації.
8. Складність структури та технологій сучасних інформаційно-комунікаційних систем внаслідок розвитку інформаційних технологій, їх вразливість перед кіберзагрозами. Відсутність дієвого захисту після подолання порушником периметру безпеки.
9. Суттєва зміна тактики, сценаріїв, складності та інструментів проведення кібератак, у тому числі як наслідок проблем 1-8.

Основні фактори проблем:

1. Еволюція кібератак.
2. Цифрова трансформація.
3. Необхідність зміни парадигми кіберзахисту.

Завдання

2

Проаналізовано еволюцію шкідливого програмного забезпечення та кібератак, сценарії реалізації складних та комплексних кібератак

Зростання кількості записів вірусних сигнатур в продуктах Zillya!:

Щоденно вірусна база поповнюється на 10-50 тисяч записів, а станом на 01.03.2013 року вірусна колекція Zillya! займала більш ніж 12 ТБ.

Технології конструктора вірусів:

У звіті IDG Research (DARK Reading) «State of Enterprise Secure Access» за 2019 рік зазначено, що 18% нових шкідливих програм залишаються непоміченими протягом перших 24 годин, а 2% загроз можуть залишатися непоміченими навіть протягом 3 місяців після зараження.

За даними Verizon Data Breach Investigations Report, у 99% зразків шкідливого коду життєвий цикл складає не більше 58 секунд.

Сценарії реалізації складних та комплексних кібератак:

Модель Cyber Kill Chain:

Модель Unified Kill Chain:

Модель Cyber Kill Chain компанії Panda Security:

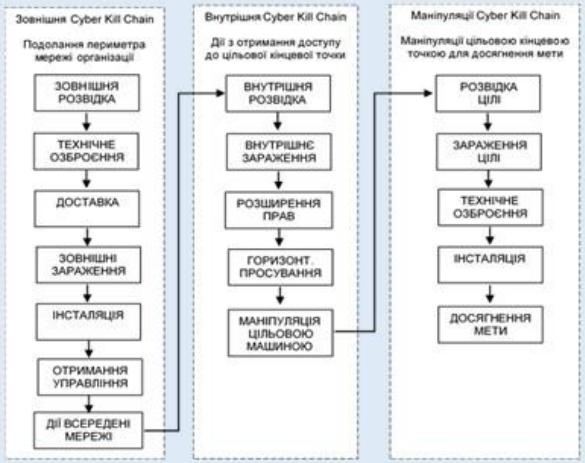


Схема кібератаки із використанням вірусу Win32/ Stuxnet:

Завдання

3

Систематизовано вимоги законодавства України з кіберзахисту, виокремлено вимоги, необхідні для врахування при опрацюванні окремих завдань дослідження

Зокрема:

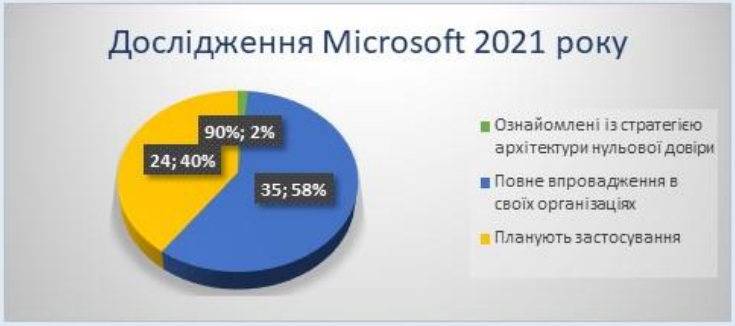
- Закон України «Про основні засади забезпечення кібербезпеки України»;
- Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
- Закон України «Про електронні довірчі послуги»;
- Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затверджений постановою Кабінету Міністрів України від 19.09.2018 № 749;
- Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518;
- Перелік стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 27.10.2020 № 687.

Виокремлено 15 обов'язкових вимог

Завдання

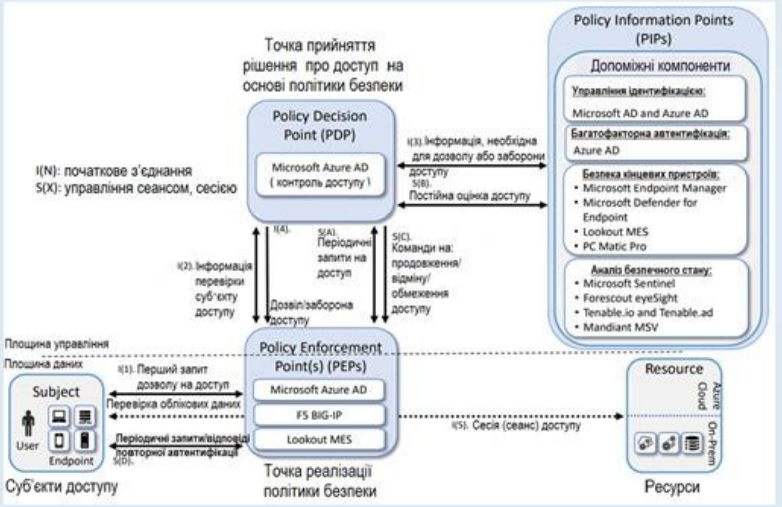
4

Висвітлено іноземний досвід впровадження концепції архітектури нульової довіри, виокремлено основні принципи, аспекти, складності застосування, інновації в підході до процедур автентифікації та доступу, наведено приклад достовірної практичної реалізації, оцінено можливість подібної реалізації із використанням апаратних, програмних засобів вітчизняного виробництва та з урахуванням вимог чинного законодавства



Абстрактна модель доступу з нульовою довірою:

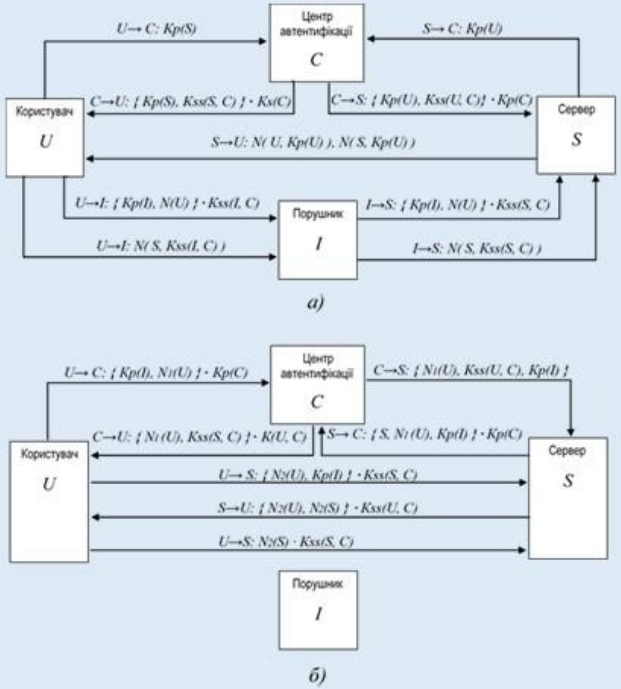
Приклад реалізованої моделі доступу з нульовою довірою:



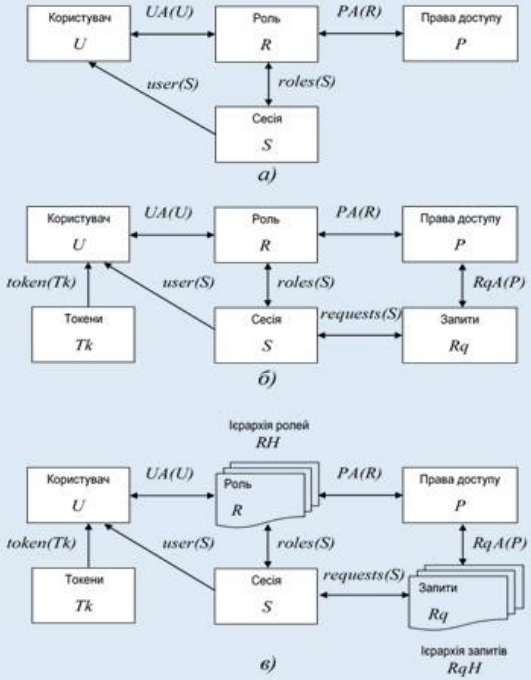
Завдання

5

Побудовано формалізовані моделі обраного рішення організації процедур автентифікації, доступу та політики безпеки доступу користувачів до ресурсів, реалізованих на принципах нульової довіри, здійснено їх аналіз, запропоновано варіанти вдосконалення



Порівняння моделей автентифікації:
а - базової , б - вдосконаленої



Порівняння моделей доступу RBAC:
а - базової , б - Azure AD, б – вдосконаленої

Ієрархія ролей *RH*:

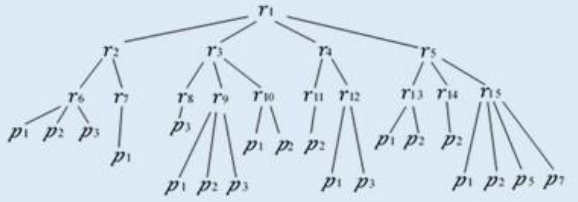
R – множина ролей
P – множина повноважень
RP: $R \rightarrow 2^P$ – призначення повноважень ролям
RR: $R \rightarrow 2^P$ – авторизація ролей повноважень ролям

Рольовий граф *G=(R, E, RP)*:

R – множина вершин графа
P – множина дуг графа
E – множина дуг в антисиметричному, транзитивному відображені *RP*
RR: $R \rightarrow 2^P$ – мітки вершин графу

Теоретико-графове представлення ієрархії ролей

Побудова дерева ролей



Розширене повноваженнями дерево ролей

Завдання

6

Проведено пошук програмних та апаратних засобів вітчизняного виробництва для практичної реалізації процедур автентифікації, доступу та політики безпеки доступу

№ з/п	Найменування програмного засобу	Виробник
1	Комп'ютерна програма системи управління підприємством «IT-Enterprise»	НВП «Інформаційні технології» (м. Київ, Україна)
2	Комплекс програмний захисту SAP-системи «ІІТ Захист SAP-системи»	ПрАТ «Інститут інформаційних технологій» (м. Харків, Україна)
3	Комплекс програмний користувача центру сертифікації ключів «ІІТ Користувач ЦСК-1»	ПрАТ «Інститут інформаційних технологій» (м. Харків, Україна)
4	Комплекс програмний клієнта захисту мережних з'єднань «ІІТ Захист з'єднань-2. Клієнт захисту з'єднань»	ПрАТ «Інститут інформаційних технологій» (м. Харків, Україна)

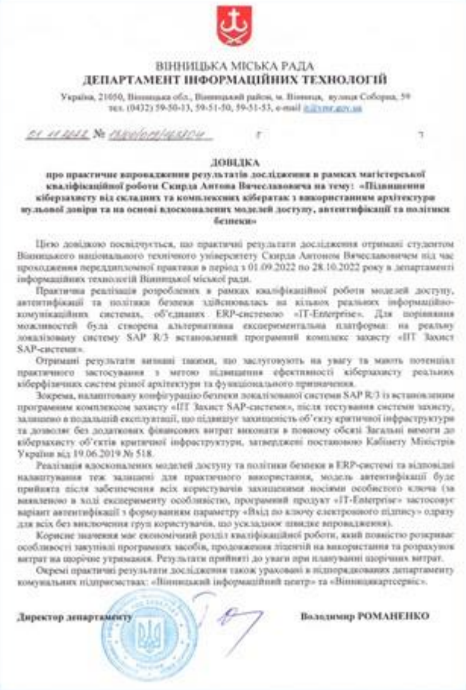
№ з/п	Найменування апаратних засобів криптографічного захисту інформації	Примітка
1	Мережний криптомодуль (наприклад, «ІІТ МКМ Гряда-301») або аналогічний	Один на ERP (SAP) - систему
2	Захищений носій особистих ключів (наприклад, «ІІТ Е. ключ «Кристал-1») або аналогічний	Персональний, у кожного користувача

№ з/п	Найменування	Експертний висновок	
		на засіб КЗІ	на засіб КЕП
1	Електронний ключ «Кристал-1»	№ 04/02/03-171 від 19.01.2018	№ 04/05/02-998 від 14.04.2021
2	Електронний ключ «Алмаз-1К»	№ 04/05/02-995 від 14.04.2021	№ 04/05/02-996 від 14.04.2021
3	Електронний ключ «SecureToken-337»	№ 04/05/02-1380 від 12.05.2021	№ 04/05/02-1381 від 12.05.2021
4	Електронний ключ «Efit Key»	№ 04/05/02-992 від 14.04.2021	№ 04/05/02-1004 від 14.04.2021
5	Електронний ключ «AvestKey»	№ 04/05/02-383 від 10.02.2022	№ 04/05/02-384 від 10.02.2022

Завдання

7

Здійснено практичне впровадження вдосконалених моделей автентифікації, доступу та політики безпеки доступу в реальній інфраструктурі (інформаційно-комунікаційній системах)



ВІННИЦЬКА МІСЬКА РАДА
ДЕПАРТАМЕНТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОВІДКА
про практичне впровадження результатів дослідження в рамках магістерської кваліфікаційної роботи Скирда Антона Вячеславовича на тему: «Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки»

Цією довідкою посвідчується, що практичні результати дослідження отримані студентом Вінницького національного технічного університету Скирда Антоном Вячеславовичем під час проходження переддипломної практики в період з 01.09.2022 по 28.10.2022 року в департаменті інформаційних технологій Вінницької міської ради.

Практична реалізація розроблених в рамках кваліфікаційної роботи моделей доступу, автентифікації та політики безпеки здійснювалась на кількох реальних інформаційно-комунікаційних системах, об'єднаних ERP-системою «IT-Enterprise». Для порівняння можливостей була створена альтернативна експериментальна платформа: на реальну локалізовану систему SAP R/3 встановлений програмний комплекс захисту «ІІТ Захист SAP-системи».

Отримані результати визнані такими, що заслуговують на увагу та мають потенціал практичного застосування з метою підвищення ефективності кіберзахисту реальних кіберфізичних систем різної архітектури та функціонального призначення.

Зокрема, налаштовану конфігурацію безпеки локалізованої системи SAP R/3 із встановленим програмним комплексом захисту «ІІТ Захист SAP-системи», після тестування системи захисту, залишено в подальшій експлуатації, що підвищує захищеність об'єкту критичної інфраструктури та дозволяє без додаткових фінансових витрат виконати в повному обсязі Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518.

Реалізація вдосконалених моделей доступу та політики безпеки в ERP-системі та відповідні налаштування теж залишені для практичного використання, модель автентифікації буде прийнята після забезпечення всіх користувачів захищеними носіями особистого ключа (за виявленою в ході експерименту особливістю, програмний продукт «IT-Enterprise» застосовує варіант автентифікації з формуванням параметру «Вхід по ключу електронного підпису» одразу для всіх без виключення груп користувачів, що ускладнює швидке впровадження).

Корисне значення має економічний розділ кваліфікаційної роботи, який повністю розкриває особливості закупівлі програмних засобів, продовження ліцензій на використання та розрахунок витрат на щорічне утримання. Результати прийняті до уваги при плануванні щорічних витрат.

Окремі практичні результати дослідження також враховані в підпорядкованих департаменту комунальних підприємствах: «Вінницький інформаційний центр» та «Вінницякартсервіс».

Директор департаменту **Володимир РОМАНЕНКО**

КОМУНАЛЬНЕ ПІДПРИЄМСТВО
«ВІННИЦЯКАРТСЕРВІС»
21050, м. Вінниця, вул. Соборна, 36; Тел.: (0432) 65 51 55, Код ЄДРПОУ 39547113

26.10.2022 р. № 105/1

За місцем вимоги

ДОВІДКА
про впровадження результатів

Видана студенту Вінницького національного технічного університету Скирда Антону Вячеславовичу про те, що його ідеї та окремі результати дослідження, проведені в рамках опрацювання магістерської кваліфікаційної роботи на тему: «Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки» використані комунальним підприємством «Вінницякартсервіс».

Зокрема використано окремі можливості, що надають вдосконалена модель доступу та політика безпеки доступу:

- при доступі користувачів до інформаційної бази даних автоматизованої системи обліку оплати проїзду в громадському транспорті;
- при організації доступу технічних адміністраторів до кінцевих пристроїв системи автоматичного визначення місцезнаходження транспорту.

Довідка видана без фінансових зобов'язань перед автором та підтверджує передачу усіх майнових прав набувачеві КП «Вінницякартсервіс».

Директор **Катерина БАБІНА**
М.П.

КОМУНАЛЬНЕ ПІДПРИЄМСТВО
«ВІННИЦЬКИЙ ІНФОРМАЦІЙНИЙ ЦЕНТР»

27.10.2022 № 184/2/15

ДОВІДКА
про використання результатів кваліфікаційної роботи

Довідка видана студенту групи УБ-21м Вінницького національного технічного університету СКИРДА Антону Вячеславовичу про те, що результати його дослідження, проведені в рамках магістерської кваліфікаційної роботи на тему: «Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки» використані комунальним підприємством «Вінницький інформаційний центр» в модулі забезпечення безпеки доступу до встановлених камер системи відеоспостереження, створеної в рамках програми «Безпечне місто»:

- скоригована встановлена політика доступу до камер системи відеоспостереження, що значно підвищило ефективність організаційно-технічних заходів із запобігання несанкціонованого доступу до камер відеоспостереження;
- введено двофакторну автентифікацію користувачів на основі особистих ключів та сертифікатів відкритих ключів кваліфікованого електронного підпису при доступі до бази даних зберігання архівних записів із використанням програмного комплексу користувача центру сертифікації ключів «ІІТ Користувач ЦСК-1» та програмного комплексу клієнта захисту мережних з'єднань «ІІТ Захист з'єднань-2. Клієнт захисту з'єднань» та персональних захищених носіїв особистого ключа.

Окремі ідеї та пропозиції плануються використати при розробці Технічного завдання модернізації системи відеоспостереження «Безпечне місто» в 2023 році.

Довідка видана без фінансових та будь-яких інших зобов'язань перед автором.

Директор Сергій БРИГАДИР

Завдання

8

Проведено економічний розрахунок запропонованих рішень, проведено порівняння конкурентних варіантів, оцінено економічну ефективність

Розрахунок капітальних витрат на придбання (CAPEX):

№ з/п	Найменування	Одиниця виміру	К-ть	Ціна за од., грн.	Вартість, грн.	ПДВ, %	Всього, грн
Варіант 1							
1	Microsoft Azure AD	ліцензія	55	13495	742225	20	890670
2	F5 BIG-IP	од.	1	1275442	1275442	20	1530530
3	Lookout MES	ліцензія	55	564	6768	20	8121
4	ЕК Efit Key	од.	55	1250	68750	-	68750
Всього (разом з ПДВ):							2498071
Варіант 2							
5	IT-Enterprise Cloud	ліцензія	55	11044	607420	20	728904
6	ІІТ Користувач ЦСК-1	ліцензія	1(55)	35000	35000	-	35000
7	ІІТ Захист з'єднань-2	ліцензія	1(55)	30690	30690	-	30690
8	ЕК ІІТ Кристал-1	од.	55	1705	93775	-	93775
Всього (разом з ПДВ):							888369
Варіант 3							
9	IT-Enterprise	ліцензія	55	3909	214995	-	214995
10	ІІТ Користувач ЦСК-1	ліцензія	1(55)	35000	35000	-	35000
11	ІІТ Захист з'єднань-2	ліцензія	1(55)	30690	30690	-	30690
12	ЕК ІІТ Кристал-1	од.	55	1705	93775	-	93775
Всього (разом з ПДВ):							374460
Варіант 4							
13	ІІТ Захист SAP	ліцензія	1	125000	125000	-	125000
14	ІІТ Захист з'єднань-2	ліцензія	1(55)	30690	30690	-	30690
15	ЕК ІІТ Кристал-1	од.	55	1705	93775	-	93775
Всього (разом з ПДВ):							249465

Розрахунок витрат на щорічне утримання (OPEX) :

№ з/п	Найменування	Одиниця виміру	К-ть	Ціна за од., грн.	Вартість, грн.	ПДВ, %	Всього, грн
Варіант 1							
1	Microsoft Azure AD	ліцензія	55	13495	742225	20	890670
2	F5 BIG-IP	ліцензія	1	122939	122939	20	147526
3	Lookout MES	ліцензія	55	564	6768	20	8121
4	Заміна особистого ключа	послуга	55	безкоштовна			0
Всього (разом з ПДВ):							1046317
Варіант 2							
5	IT-Enterprise Cloud	ліцензія	55	11044	607420	20	728904
6	ІІТ Користувач ЦСК-1	ліцензія	1(55)	безстрокова			0
7	ІІТ Захист з'єднань-2	ліцензія	1(55)	безстрокова			0
8	Заміна особистого ключа	послуга	55	безкоштовна			0
Всього (разом з ПДВ):							728904
Варіант 3							
9	IT-Enterprise	ліцензія	55	3909	214995	без	214995
10	ІІТ Користувач ЦСК-1	ліцензія	1(55)	безстрокова			0
11	ІІТ Захист з'єднань-2	ліцензія	1(55)	безстрокова			0
12	Заміна особистого ключа	послуга	55	безкоштовна			0
Всього (разом з ПДВ):							214995
Варіант 4							
13	ІІТ Захист SAP	ліцензія	1	безстрокова			0
14	ІІТ Захист з'єднань-2	ліцензія	1(55)	безстрокова			0
15	Заміна особистого ключа	послуга	55	безкоштовна			0
Всього (разом з ПДВ):							0

Порівняння конкурентних варіантів:

№ з/п	Аналоги за функціональним призначенням	CAPEX (капітальні витрати), грн.	OPEX (операційні витрати), грн./рік
1	Варіант 1	2498071	1046317
2	Варіант 2	888369	728904

№ з/п	Аналоги за функціональним призначенням	CAPEX (капітальні витрати), грн.	OPEX (операційні витрати), грн./рік
1	Варіант 3	374460	214995
2	Варіант 4	249465	0

Застосована методика та отримані висновки розрахунків мають практичне значення

Об'єктом дослідження є:

кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем

Предметом дослідження є:

підвищення кіберзахисту з використанням архітектури нульової довіри на основі вдосконалених моделей доступу, автентифікації та політики безпеки

Методи дослідження

Для реалізації визначеної мети та вирішення поставлених завдань використано комплекс взаємодоповнюючих загальнонаукових та спеціальних методів дослідження та аналізу, зокрема:

- **системний аналіз та синтез (у всіх розділах роботи);**
- **методи інформаційно-аналітичного дослідження (розділ 1);**
- **моделювання (підрозділи 2.2 - 2.4);**
- **методи вивчення аналога (прототипу) та метод еталонного оцінювання (підрозділи 2.1, 3.1);**
- **експеримент (підрозділ 3.3);**
- **метод аналізу ієрархій та метод побудови рольового дерева розмежування доступу, методика теоретико-графового представлення (підрозділ 2.4);**
- **методи визначення та оцінки економічної ефективності (розділ 4).**

Новизна одержаних результатів

- **вперше запропоновано, досліджено та доведено можливість застосування концепції архітектури нульової довіри для підвищення ефективності кіберзахисту об'єктів критичної інфраструктури, захисту державних інформаційних ресурсів та інформаційно-комунікаційних систем, з урахуванням вимог та обмежень, регламентованих законодавчими та нормативно-правовими актами в цих сферах;**

- **вперше здійснено технічний переклад NIST 1800-35B (дата публікації: липень 2022 року) та його аналіз, на основі якого висвітлено невідомі до цього достовірні приклади практичної реалізації інновацій архітектури нульової довіри, що дозволяє: 1) більш глибоке розуміння концепції архітектури нульової довіри, абстрактний опис принципів якої зазначений в NIST 800-207 (дата публікації: серпень 2020 року); 2) стимулює подальші дослідження парадигми архітектури нульової довіри, як найбільш перспективного варіанту вирішення проблем кіберзахисту; 3) надає можливість практичного використання: як наведених в NIST 1800-35B програмних продуктів для реалізації архітектури нульової довіри, так й вітчизняних аналогів, що в свою чергу: 4) дозволяє знизити капітальні витрати на придбання та утримання засобів кіберзахисту;**

- **вперше використано положення стандарту IAS 38 «Нематеріальні активи» для демонстрації економічної ефективності впровадження конкурентних між собою програмних засобів захисту, що надає можливість оптимальних витрат бюджетних коштів та уникнення проблем з фінансуванням щорічного утримання програмних продуктів.**

- **дістало подальшого розвитку використання напрацювань та запропонованих раніше методик в процесах створення та дослідження формалізованих моделей;**

- **дістала подальшого розвитку раніше запропонована ідея поєднання двох відомих методів (аналізу ієрархій та побудови рольового дерева розмежування доступу) при моделюванні на основі теоретико-графового представлення ієрархії ролей, що розширює можливості вдосконалення практичних рольових моделей доступу.**

Практичне значення одержаних результатів:

- продемонстровано можливість застосування програмних та апаратних засобів вітчизняного виробництва, які відповідають обов'язковим вимогам законодавства та нормативно-правових актів в сфері технічного та криптографічного захисту інформації, для практичного впровадження концепції архітектури нульової довіри;
- доведено, що реалізовані рішення здатні підвищити ефективність захисту реальних інформаційних та кіберфізичних систем різного призначення та архітектури від складних, цільових та комплексних кібератак, та, відповідно, вирішувати проблеми сучасного стану кіберзахисту.

Апробація результатів роботи:

- окремі результати досліджень, використані в роботі, оприлюднені на Всеукраїнській науково-практичній інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2022)» (м. Вінниця, 16 – 17 червня 2022 року).

Публікації:

- Скирда А.В. Дослідження застосування кіберзброї проти України. // Матеріали Всеукраїнської науково-практичної інтернет-конференції. Молодь в науці: дослідження, проблеми, перспективи (МН-2022). – 2022.
- Скирда А.В. Дослідження необхідності та номенклатури захищених носіїв особистих ключів в Україні // Матеріали Всеукраїнської науково-практичної інтернет-конференції. Молодь в науці: дослідження, проблеми, перспективи (МН-2022). – 2022.

Результати дослідження використано:

- департаментом інформаційних технологій Вінницької міської ради практичною реалізацією вдосконалених моделей на кількох реальних інформаційно-комунікаційних системах, об'єднаних ERP-системою «IT-Enterprise» та в реальній локалізованій системі SAP R/3, шляхом відповідних налаштувань програмного комплексу захисту «ІІТ Захист SAP-системи» (довідка від 01.11.2022 № 13/00/019/163804);
- комунальним підприємством «Вінницькартсервіс» в автоматизованій системі обліку оплати проїзду в громадському транспорті та системі автоматичного визначення місцезнаходження транспорту (довідка від 26.10.2022 № 105/1);
- комунальним підприємством «Вінницький інформаційний центр» в системі відеоспостереження «Безпечне місто» (довідка від 27.10.2022 № 194/2/15).

Висновки

В кваліфікаційній роботі запропонований реально можливий практичний та концептуальний підхід підвищення кіберзахисту сучасних інформаційно-комунікаційних систем (різної конфігурації, структури, функціонального призначення) від складних та комплексних кібератак шляхом впровадження концепції архітектури нульової довіри на основі вдосконалених моделей доступу, автентифікації, політики безпеки, що здатні забезпечити практичну реалізацію цієї концепції з урахуванням вимог чинного законодавства в сферах кіберзахисту та захисту інформації

Отримані результати дозволяють виокремити два важливих аспекти дослідження:

Доведено можливість

використання програмних та апаратних засобів вітчизняного виробництва, які відповідають обов'язковим вимогам законодавства та нормативно-правових актів в сфері технічного та криптографічного захисту інформації, для практичного впровадження концепції архітектури нульової довіри

Продемонстровано здатність

реалізованого підходу підвищити ефективність захисту реальних інформаційних та кіберфізичних систем різного призначення та архітектури від складних, цільових та комплексних кібератак, та, відповідно, вирішити більшість проблем сучасного стану кіберзахисту

Поставлені завдання дослідження виконані в повному обсязі

Дякую за увагу !

Додаток Д

Протокол перевірки на наявність ознак академічного плагіату

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ
ЗАПОЗИЧЕНЬ

Назва роботи: Підвищення кіберзахисту від складних та комплексних кібератак з використанням архітектури нульової довіри та на основі вдосконалених моделей доступу, автентифікації та політики безпеки

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ: Кафедра менеджменту та безпеки інформаційних систем
Факультет менеджменту та інформаційної безпеки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 94% Схожість 6%

Аналіз звіту подібності (відмітити потрібне):

1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ (підпис) Коваль Н.П. (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ (підпис) Скирда А.В. (прізвище, ініціали)

Керівник роботи _____ (підпис) Яремчук Ю.Є. (прізвище, ініціали)