МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

СТЕПАНЮК Олександр Володимирович

Модель багаторівневої системи контролю доступу / A Model of a Multilevel Access Control System

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
О.В. Степанюк

Науковий керівник
д.т.н., професор М.М.Касянчук

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2025 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2025

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь "магістр"
спеціальність:125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
"____"_____2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
СТЕПАНЮКУ Олександру Володимировичу
(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи
Модель багаторівневої системи контролю доступу / A Model of a Multilevel Access Control System
керівник роботи: д.т.н., професор М.М.Касянчук
затверджені наказом по університету від 29 листопада 2024 року № 938
2. Строк подання студентом закінченої кваліфікаційної роботи
5 грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити

– аналіз сучасних перспектив розвитку технологій контролю доступу;

– аналіз сучасних тенденцій розвитку SIEM-систем;

– формування політик захищеності доступу до обчислювальних комплексів;

– розробка концепції побудови моделей системи контролю доступу до інформаційних ресурсів;

– формування вимог та умов для проектування архітектури контролю доступу;

– розробка апаратного рівня архітектури моделі системи контролю доступу;

– опис тестового стенда з багаторівневим контролем доступу.

5. Перелік графічного матеріалу у роботі.

Матриця для дискреційної моделі доступу.

Модель Белла-Лападула.

Приклад захищеного обчислювального комплексу для доступу до сервісів.

Чотирьохрівнева архітектура системи КД, яка перебачає масштабування.

Апаратний рівень контролю доступу.

Розміщення віртуальних машин та програмного забезпечення.

Споживання ресурсів віртуальними машинами.

Споживання ресурсів процесора аналітичною віртуальною машиною.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання: 29 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Сучасні можливості вдосконалення технологій контролю доступу	12.2024 р. – 03.2025 р.	
2	Розробка багаторівневої масштабованої архітектури моделі контролю доступу	03.2025 р. – 06.2025 р.	
3	Реалізація та дослідження архітектури системи контролю доступу	06.2025 р. – 11.2025 р.	

Студент _____ Степанюк О.В.
(підпис)

Керівник роботи _____ д.т.н., проф. Касянчук М.М.
(підпис)

АНОТАЦІЯ

Степанюк О.В. Модель багаторівневої системи контролю доступу. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека та захист інформації», освітньо-професійна програма «Кібербезпека». – Західноукраїнський національний університет, Тернопіль, 2025.

Здійснено аналіз системних факторів впливу на процес контролю доступу, що дозволило визначити сучасні тенденції та перспективи розвитку технологій контролю доступу. На основі формування політик захищеності доступу до обчислювальних комплексів розроблено концепцію побудови моделі системи контролю доступу до інформаційних ресурсів. На основі формування вимог та умов для проектування архітектури контролю доступу розроблено чотирирівневу архітектуру для моделі системи контролю доступу. Розроблено модель багаторівневої системи контролю доступу, наведено опис тестового стенда з багаторівневим контролем доступу, що дозволило верифікувати отримані теоретичні результати.

Ключові слова: БАГАТОРІВНЕВА СИСТЕМА, КОНТРОЛЬ ДОСТУПУ, ДИСКРЕЦІЙНА МОДЕЛЬ, РОЛЬОВА МОДЕЛЬ, МАНДАТНА МОДЕЛЬ, ПОЛІТИКА БЕЗПЕКИ.

ABSTRACT

Stepaniuk O.V. A Model of a Multilevel Access Control System. – Manuscript.

Research for the degree of "Master" in specialty 125 "Cybersecurity and information protection", educational and professional program "Cybersecurity". – West Ukrainian National University, Ternopil, 2025.

An analysis of systemic factors influencing the access control process has been carried out, which allowed us to determine current trends and prospects for the development of access control technologies. Based on the formation of access security policies for computing complexes, a concept for constructing a model of an access control system for information resources has been developed. Based on the formation of requirements and conditions for designing an access control architecture, a four-level architecture for the access control system model has been developed. A model of a multi-level access control system has been developed, a description of a test bench with multi-level access control is provided, which allowed to verify the obtained theoretical results.

Keywords: MULTI-LEVEL SYSTEM, ACCESS CONTROL, DISCRETIONARY MODEL, ROLE MODEL, MANDATE MODEL, SECURITY POLICY.

ЗМІСТ

ВСТУП…….. 7
1 СУЧАСНІ МОЖЛИВОСТІ ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ КОНТРОЛЮ ДОСТУПУ ……... 10
1.1 Системні чинники, що впливають на процес контролю доступу 10
1.2 Сучасні напрямки восконалення реалізацій контролю доступу….... 13
1.3 Тенденції розвитку SIEM-систем ……... 23
2 РОЗРОБКА БАГАТОРІВНЕВОЇ МАСШТАБОВАНОЇ АРХІТЕКТУРИ МОДЕЛІ КОНТРОЛЮ ДОСТУПУ…… 27
2.1 Формування політик безпечного доступу до інформаційних систем ……..…….. 27
2.2 Концепція розробки системи контролю доступу до ресурсів інформаційних систем…..... 33
2.3 Моделі контролю доступу..... 36
3 РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ АРХІТЕКТУРИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ …… 48
3.1 Формування вимог та умов для проектування архітектури контролю доступу ……..... 48
3.2 Розробка чотирирівневої архітектури системи контролю доступу.. 53
3.3 Розробка апаратного рівня архітектури системи контролю доступу ……..... 55
3.4 Опис тестового стенда з багаторівневим контролем доступу …….. 57
ВИСНОВКИ……. 64
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 65
ДОДАТОК А Копії публікацій..... 69

ВСТУП

Сьогодні спостерігається тенденція до переведення державних, медичних, банківських, освітніх та багатьох інших послуг у цифровий формат [1]. Стрімкий розвиток цифрових технологій спричинив їхнє широке впровадження у різноманітні сфери суспільного життя [2, 3]. Економічна взаємодія та комунікація громадян з державними установами трансформується у процеси роботи з комп'ютерними сервісами через мережі [4, 5]. Ключовими інструментами цифрового простору стають веб-платформи (також відомі як електронні портали, обчислювальні системи (ОС)) або спеціалізоване програмне забезпечення з доступом до публічних мереж [6, 7].

У процесі створення ОС розробники стикаються з суперечливими вимогами: необхідно забезпечити максимальну доступність сервісу, його незалежність від платформ, зручність та простоту експлуатації (ідеально – мінімальну кількість дій для доступу); водночас сервіси оперують значними обсягами персональної, медичної, фінансової та іншої конфіденційної інформації, що вимагає посиленого контролю та ідентифікації користувачів. Для реалізації надійного контролю доступу (КД) застосовуються засоби інформаційної безпеки [8-10]. Інтеграція додаткових модулів у обчислювальну інфраструктуру ОС потребує ретельного планування ресурсів та визначення місць підключення компонентів КД.

Системи КД функціонують як складові інформаційних систем, що забезпечують роботу ОС, проте є автономними елементами з виділеною частиною інфраструктури, віртуальними та апаратними ресурсами, тобто система КД становить окремий об'єкт з власними завданнями розробки та налаштування [11-12]. Розвиток систем КД може відбуватися незалежно від технологій надання основних послуг ОС: можливе впровадження нових підходів до КД; оновлення програмних і апаратних компонентів без втручання у базовий функціонал ОС [13-15].

Все вищесказане робить актуальною задачу проведення теоретичних, експериментальних, структурних, програмно-апаратних досліджень з розробки принципів і рішень щодо побудови нових та вдосконалення існуючих засобів захищеного доступу до ОС на основі побудови масштабованої архітектури системи КД, що забезпечують функціонування багатокористувацьких обчислювальних комплексів.

Мета роботи. Метою даної роботи є розробка моделі багаторівневої системи контролю доступу.

Для вирішення поставленої мети вирішуються наступні **завдання**:

– аналіз сучасних перспектив розвитку технологій контролю доступу;

– аналіз сучасних тенденцій розвитку SIEM-систем;

– формування політик захищеності доступу до обчислювальних комплексів;

– розробка концепції побудови моделей системи контролю доступу до інформаційних ресурсів;

– формування вимог та умов для проектування архітектури контролю доступу;

– розробка апаратного рівня архітектури моделі системи контролю доступу;

– опис тестового стенда з багаторівневим контролем доступу.

Об’єкт дослідження. Процес контролю доступу до інформаційних ресурсів.

Предмет дослідження. Алгоритми та моделі контролю доступу до інформаційних ресурсів.

Методи дослідження. Математичні методи моделювання, методи контролю доступу, методи розробки архітектури інформаційних систем, метод тестування експериментальних стендів.

Наукова новизна одержаних результатів.

1. Здійснено аналіз системних факторів впливу на процес контролю доступу, що дозволило визначити сучасні тенденції та перспективи розвитку технологій контролю доступу.

2. На основі формування політик захищеності доступу до обчислювальних комплексів розроблено концепцію побудови моделі системи контролю доступу до інформаційних ресурсів.

3. На основі формування вимог та умов для проектування архітектури контролю доступу розроблено чотирирівневу архітектуру для моделі системи контролю доступу.

Практичне значення отриманих результатів.

Розроблено модель багаторівневої системи контролю доступу, наведено опис тестового стенда з багаторівневим контролем доступу, що дозволило верифікувати отримані теоретичні результати.

Публікації та апробація КР.

1. Степанюк О.В., Залізняк В.В., Касянчук М.М. Архітектура обчислювального комплексу з багаторівневим контролем доступу. Збірник матеріалів науково-практичного симпозіуму «Захист інформації’2025».Тернопіль, 2025. С.99-101 [16].

2. Степанюк О.В., Прончук Д.С. Сучасні перспективи автоматизованих систем контролю доступу. Збірник матеріалів науково-практичного симпозіуму «Технології Інтернету речей: системи та рішення» (TIP:CT-2025). Тернопіль, 2022. С.31-33 [17].

1 СУЧАСНІ МОЖЛИВОСТІ ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ КОНТРОЛЮ ДОСТУПУ

1.1 Системні чинники, що впливають на процес контролю доступу

Для забезпечення ефективної стратегії КД потрібно ідентифікувати весь спектр суттєвих ризиків та впливових чинників [18, 19]. Елементи, здатні впливати на КД, визначимо як впливові фактори.

Впливові чинники можна класифікувати за трьома категоріями:

1) чинники з прямим деструктивним впливом на КД – це потенційні ризики та їх реалізовані форми у вигляді атак;

2) чинники з непрямим деструктивним впливом на КД;

3) чинники, що сприяють покращенню процесу КД.

Необхідно скласти перелік потенційних впливів від кожного елемента всіх об'єктів та їхніх взаємодій, які задіяні у механізмі КД.

Суб'єкти доступу є джерелами найнебезпечніших і найбільш негативних масових впливів на процес КД; зокрема, вони є джерелами зловмисних дій – вважається, що не менше 70% атак реалізуються за участю персоналу об'єкта захисту [20]. Мається багато різних методик та переліків можливих загроз. Найбільш важливим та представницьким з подібних переліків є список загроз, пов'язаних із захистом персональних даних [21]. І хоча він прив'язаний до захисту персональних даних, цей список майже цілком може використовуватися і при аналізі загроз за вимогами, що виходять за межі захисту персональних даних. Більш того, цей перелік включає також загрози, що походять від інших компонентів.

Окрім ризиків безпеки, суб'єкти можуть чинити на КД такі впливи:

1) недбале або навіть зневажливе ставлення користувачів до заходів забезпечення ІБ;

2) систематичні намагання користувачів застосовувати на робочих станціях неавторизоване обладнання чи програми, посилаючись на виробничу необхідність;

3) пропозиції та ініціативи від користувачів щодо оптимізації механізмів КД;

4) фінансова чи інша форма підтримки користувачами систем обробки інформації на захищених об'єктах, включно з інфраструктурою ІБ та модулями КД.

Наступною складовою виступають об'єкти доступу – інформаційні платформи та технічні засоби, що становлять цінність для різних категорій користувачів, включаючи процеси опрацювання інформації. Вони також можуть генерувати негативні впливи, зокрема створювати ризики для ІБ [23]. Серед інших форм впливу від об'єктів доступу виділимо:

1) тривалий час опрацювання інформації на захищеному об'єкті;

2) неспроможність об'єкта доступу коректно реалізовувати призначені функції: відмови у роботі, програмні помилки, технічні несправності, недоліки архітектурних або програмно-технічних рішень;

3) підвищений рівень стійкості (відновлюваності) об'єкта доступу (програмної платформи чи технічного засобу), не задокументований у стандартній технічній документації;

4) розширені можливості програмної взаємодії об'єкта доступу з різноманітними додатками.

Серед впливових факторів, що стосуються системи опрацювання даних, окрім ризиків, представлених у додатку, відзначимо такі чинники:

1) труднощі у взаємодії між різними інформаційними платформами або технічними засобами через їхню обмежену або низьку сумісність;

2) широкий асортимент програмного забезпечення, включаючи альтернативні рішення, що функціонує в системі опрацювання даних;

3) застосування перевірених та надійних програмно-технічних рішень у системі опрацювання даних;

4) суворе обмеження та мінімізація зв'язків системи опрацювання даних з зовнішніми платформами та об'єктами, особливо з недостатньо перевіреними.

Система захисту інформації, крім загроз безпеки, може зазнавати впливу таких чинників:

1) ротація персоналу, спричинена наявністю на ринку привабливіших пропозицій, передусім щодо винагороди;

2) обмежене фінансування для модернізації та оновлення захисних механізмів з урахуванням еволюції методів зловмисних втручань;

3) наявність сертифікаційних документів про відповідність системи захисту ІБ встановленим стандартам (зокрема, у сфері охорони персональної інформації);

4) ефективна співпраця зі службами кібербезпеки інших установ, які мають результативні системи захисту ІБ або високу експертизу у галузі ІБ.

Зовнішнє середовище становить одне з основних джерел загроз поряд із користувачами системи [24]. Як фактори непрямого впливу на процес КД виділимо такі:

1) підвищений рівень злочинності у місці розміщення захищеного об'єкта;

2) інтенсивний обмін даними захищеного об'єкта з зовнішніми мережами;

3) встановлені зв'язки та регулярні консультації з надійними та кваліфікованими онлайн-партнерами;

4) усвідомлення критичності питань ІБ на захищеному об'єкті та сприяння з боку регіональних адміністративних структур і правоохоронних органів.

Всі служби безпеки підпорядковані захищеному об'єкту, тобто керівництво об'єкта організовує роботу та здійснює нагляд за діяльністю систем безпеки. Захищений об'єкт, попри те, що всі заходи ІБ спрямовані на створення оптимальних умов його роботи, також може бути джерелом ризиків. Додатково виокремимо такі впливові чинники, пов'язані із захищеним об'єктом:

1) недостатня інформаційна інтеграція захищеного об'єкта з системою опрацювання даних та системою забезпечення ІБ;

2) наявність певних прогалин і вразливостей у політиці інформаційної безпеки, схвалених під впливом представників захищеного об'єкта з метою створення комфортніших умов його діяльності;

3) налагоджена координація систем забезпечення ІБ зі службою фізичної охорони об'єкта;

4) забезпечення адекватного фінансування системи ІБ з боку захищеного об'єкта.

Система КД також може становити джерело нестандартного впливу на процес КД:

1) недостатнє застосування технічних засобів КД, включаючи моніторинг пересування по території захищеного об'єкта;

2) застарівання засобів КД з плином часу та відсутність їх своєчасної модернізації;

3) недостатній нагляд за діяльністю працівників системи КД;

4) комплексна інтеграція системи КД з іншими підрозділами установи.

Отже, базу переліку впливових чинників формує список актуальних ризиків. Варто зазначити, що представлений перелік впливових факторів може коригуватися та доповнюватися в процесі дослідження конкретної установи, систем опрацювання даних та забезпечення ОС. Сформований перелік дає змогу підвищити результативність системи КД завдяки більш адекватному управлінню її процесами.

1.2 Сучасні напрямки вдосконалення реалізацій контролю доступу

Програмні рішення Security information and event management (SIEM) [25-27] – системи управління інформацією та подіями безпеки – з'явилися на ринку приблизно у 1997 році. Їхній функціонал був спрямований на

скорочення помилкових тривог систем виявлення мережевих атак (IDS - intrusion detection system), які становили серйозну проблему для IDS-платформ.

Подібно до багатьох інших технологій, SIEM-платформи виникли внаслідок розвитку та інтеграції систем Security Event Management (SEM) та Security Information Management (SIM). Програмні рішення SEM функціонують майже синхронно, виконуючи моніторинг, збирання та співставлення подій, генеруючи попереджувальні дані. Системи SIM аналізують накопичену інформацію з позицій статистичних закономірностей, аномалій тощо. Термін SIEM-системи застосовується, коли функціонал SEM та SIM інтегровано в єдиному програмному рішенні. З огляду на це, абревіатуру SIEM можна інтерпретувати як «система агрегації та співставлення подій». Важливо зауважити, що SIEM-платформи неможливо розглядати як автономне рішення (standalone), оскільки вони не здатні самостійно попередити інциденти інформаційної безпеки. Призначення SIEM-систем відображене в їхній назві – це обробка даних, отриманих з різноманітних джерел (IDS, DLP, фаєрволи, антивірусне ПЗ тощо), з наступним виявленням характерних відхилень від встановлених стандартів за попередньо визначеними параметрами [28, 29]. Водночас SIEM-системи мають численні переваги. Основною метою SIEM-платформ є акумуляція різнотипної заданої інформації та ідентифікація в ній сигналів про порушення інформаційної безпеки та критичні інциденти. Зазвичай для реалізації цих завдань застосовуються методи стандартизації, селекції, консолідації та співставлення подій. Але при збільшенні складності атак (наприклад, цільові атаки), об'єктів, що захищаються (в т. ч. кіберфізичних систем) і застосовуваних технологій, використовувані методи та підходи іноді не можуть забезпечити необхідний ступінь захищеності. На цю тенденцію негативно впливає також зростаючий обсяг даних, обробляти який все складніше. У SIEM-засобах захисту головна роль відводиться процесу кореляції даних [30], який спрямований, головним чином, на виявлення

причинно-наслідкових зв'язків між подіями, які поступають на обробку [31]. Процес кореляції даних дає можливість виявити шкідливі та аномальні активності, визначити джерело та цілі атаки, а також виявити багатокрокові атаки. В даний час час існує значна кількість методів та підходів, які застосовуються в процесі кореляції, однак найбільш широко використовується правило-орієнтований метод.

Програмний продукт Symantec Security Information Manager застосовує для виявлення загроз безпеки підхід, в рамках якого відбувається класифікація проблем та загроз безпечності і береться до уваги спосіб атаки, цільові ресурси та рівень впливу інциденту.

Аналітичний компонент продукту Symantec SIM базується на правилах, побудованих за принципом шаблонів. Правило може складатися з кількох елементарніших правил, що використовуються у типових сценаріях. Завдяки цьому процес створення та підтримки правил, здатних охоплювати множинні умови, значно спрощується. Така методологія забезпечує високошвидкісний аналіз - обробку до 30000 подій протягом однієї секунди.

Збирання та обробка подій відбувається синхронно із застосуванням встановлених правил через зіставлення потоку стандартизованих подій. У разі виявлення події/комплексу подій, що відповідають правилам кореляції, генерується висновок, який або створює новий інцидент, або автоматично приєднується до наявного інциденту. Висновки супроводжуються стислими поясненнями, що дозволяють оцінити ситуацію в системі без детального вивчення журналів. До запропонованих розробником (Symantec) описів конкретних заходів щодо усунення загрози можна долучити інструкції та методичні рекомендації, прийняті в конкретній організації [32].

Резюмуючи, можна констатувати, що програмне рішення Symantec SIM також ґрунтується на використанні правил кореляції, які, незважаючи на позиціонування як «інтелектуальні», не забезпечують детектування нових, раніше невідомих атак. Окрім того, ці технології знову орієнтовані на аналіз подій, що вже відбулися. Цей продукт можна умовно вважати краще

адаптованим завдяки тому, що компоненти збирання подій з моніторингових об'єктів (колектори) поділяються на дві категорії: ті, що функціонують на обладnанні Symantec SIM, та ті, що працюють на альтернативних комп'ютерах.

Програмне рішення MaxPatrol (виробник - Positive Technologies) характеризується такими особливостями:

1) симптоматика:

- відображення подій у зрозумілій для користувача формі;
- маркування подій тегами;
- доповнення метриками ризиків (включаючи інтегральну метрику ризику);
- категоризація подій за класами;

2) характеристики процесу кореляції подій:

- внутрішньосерійна кореляція;
- кореляція –на основі попередньо визначених правил;
- ретроспективний аналіз;
- функціональна обробка;
- симптоматичні блоки;
- користувацьке налаштування;

3) можливості роботи мережевого сенсора:

- виявлення загроз у трафіку – система здійснює глибоке інспектування мережевого трафіку для ідентифікації шкідливого програмного забезпечення, експлуатації вразливостей програмних компонентів та спроб несанкціонованого проникнення;
- протокольний аналіз включає виявлення використання нестандартних портів для обходу політик безпеки; моніторинг нетипових команд та їх параметрів; детектування тунельованих з'єднань; збір інформації про процеси автентифікації; аналіз протокольних обгорток та інкапсуляції;
- перехоплення файлів – система здатна витягувати файли безпосередньо з мережевого трафіку під час їх передачі, обчислювати

контрольні суми (MD5/SHA) та здійснювати захоплення пакетів (pcap) для подальшого дослідження;

– аналіз потоків з даними – формування та обробка заголовків мережевих потоків (flow headers) для побудови карти комунікаційних зв'язків між вузлами мережі;

– моніторинг SSL/TLS – відстеження та перевірка сертифікатів захищених з'єднань Secure Sockets Layer для виявлення підозрілих або скомпрометованих сертифікатів;

– розробка політик сегментації – формування та застосування правил міжзонної взаємодії для контролю трафіку між різними сегментами мережевої інфраструктури;

4) аналітичні можливості системи (забезпечують інтелектуальну обробку зібраної інформації через наступні механізми):

– вагові агрегати об'єктів – система присвоює та обчислює вагові коефіцієнти для різних об'єктів моніторингу: IP-адреси, імена користувачів (username), хости (Host), унікальні ідентифікатори (UID), мережеві порти тощо. Це дозволяє приорітизувати потенційні загрози;

– джерела даних для аналізу включають повні доменні імена (FQDN), криптографічні хеші файлів (MD5/SHA), IP-адреси, URL-адреси, електронні адреси;

– побудова графів залежностей – система створює візуалізацію та аналізує взаємозв'язки між окремими об'єктами інфраструктури, що допомагає виявляти складні ланцюжки атак;

– історична кореляція даних – використання накопиченої інформації для виявлення довгострокових трендів та латентних загроз, які не проявляються при аналізі окремих подій;

– формування контекстних зв'язків: зв'язок між процесом та користувачем, який його ініціював; асоціація користувача з конкретною

робочою станцією; відстеження множинних сесій входу одного користувача; аналіз поведінкових патернів користувачів;

– інтелектуальне виявлення загроз – використання накопиченої бази знань для ідентифікації підозрілої активності на основі історичних даних та встановлених базових показників;

– детектування аномалій включає виявлення нових контрольних сум процесів, які раніше не зустрічалися в системі; ідентифікацію унікальних ситуацій та нетипових комбінацій подій; сигналізацію про відхилення від встановлених поведінкових моделей; реєстрацію прецедентів, що не мають історичних аналогів;

– генерація звітності – автоматизоване формування аналітичних звітів різного рівня деталізації для різних категорій користувачів.

Центральне місце в архітектурі системи виявлення інцидентів займає механізм кореляції на основі правил. Важливою перевагою є можливість розширення стандартного набору правил власними доробками, що дозволяє адаптувати систему до унікальних потреб організації.

Особливий інтерес становить функція історичної кореляції, яка, ймовірно, реалізує механізм машинного навчання на основі минулих інцидентів. Це дозволяє системі поступово вдосконалювати процес виявлення загроз та формувати векторні моделі атак для збагачення бази знань.

Варто відзначити, що розглянуті програмні рішення приділяють значну увагу системі вагових коефіцієнтів та метрик для оцінки подій. Це дає підстави припускати наявність розширеної функціональності кореляції з використанням складних статистичних моделей та алгоритмів оцінки ризиків.

Побудова взаємозв'язків у системі орієнтована переважно на сутність користувача як центральний елемент аналізу. Система відстежує три основні види зв'язків: процес-користувач (хто ініціював яку діяльність), користувач-машина (з якими ресурсами взаємодіє користувач), користувач-логіни (як та коли користувач здійснює автентифікацію). Такий підхід дозволяє формувати

комплексний профіль поведінки користувача та ефективно виявляти інсайдерські загрози або скомпрометовані облікові записи.

Незважаючи на значні можливості, якими володіють представлені SIEM-продукти, їх масштабованість та гнучкість, вони не можуть гарантувати повністю забезпечення безпеки через такі особливості:

1) орієнтація на роботу з подіями, які описані правилами та зафіксовані у журналах;

2) застосування в якості основного інструменту методу кореляції з урахуванням заданих правил. Це рішення досить суб'єктивне та робить необхідним постійне доповнення переліку правил, що не завжди можливо у разі великомасштабних систем;

3) немає орієнтованості на специфіку поведінки користувачів.

Актуальні тенденції в галузі безпеки припускають концентрацію уваги на людині та її поведінці, оскільки саме людина - головне джерело порушень, загроз, інцидентів та ризиків. На зараз не існує уніфікованого найменування для рішень, що дозволяють аналізувати поведінку користувачів. Наприклад, компанія Gartner використовує назву User and Entity Behavior Analytics (UEBA). Схожі назви носять продукти компаній Gurucul, Forcepoint, Securonix та Fortscale. Розробники з Splunk, DNIF, HP ArcSight (HPE/MicroFocus), IBM та персонал IDC застосовують назву User Behavior Analytics (UBA) для своїх програмних продуктів.

Інші учасники ринку інформаційної безпеки акцентують увагу не лише на об'єктах дослідження, таких як сутності (Entity) чи користувачі (User), а й підкреслюють у своїх продуктах основні цілі та методології аналізу.

Microsoft та Exabeam послуговуються концепцією Advanced Threat Analytics (розширена аналітика загроз) або узагальненим терміном Advanced Analytics (розширена аналітика). Ця термінологія підкреслює фокус на виявленні складних, багатоступеневих загроз та використанні передових аналітичних методів для їх ідентифікації.

Аналітична компанія Forrester запровадила термін Security User Behavior Analytics (SUBA) – аналітика поведінки користувачів з точки зору безпеки. Цей термін позначає цілий клас рішень, призначених для поведінкового аналізу, при цьому особливий наголос робиться саме на аспектах забезпечення інформаційної безпеки організації. Таке формулювання чітко вказує на пріоритетність завдань захисту перед іншими можливими застосуваннями поведінкової аналітики.

На сучасному європейському ринку можна відзначити наявність продуктів класу UEBA/UBA/SUBA, які часто характеризуються змішаним підходом: система UBA (входить до DLP) від Zecurion; ProfileCenter від SearchInform; Prediction класу UEBA, пропонований компанією InfoWatch.

На початковому етапі розвитку технології User Behavior Analytics основний функціонал обмежувався двома ключовими напрямками:

– перший напрямок передбачав безперервне відстеження та глибокий аналіз дій користувачів у корпоративному середовищі. Система збирала інформацію про активність персоналу, формуючи комплексну картину їхньої взаємодії з інформаційними ресурсами;

– другий напрямок стосувався ідентифікації незвичайних патернів у діяльності користувачів та визначення їхньої критичності. Такий підхід давав можливість оперативно реагувати на найбільш суттєві та масштабні зміни в поведінкових моделях, ігноруючи малозначущі флуктуації.

З плином часу концептуальне розуміння того, яким має бути UBA-інструментарій, зазнало істотних трансформацій. До базового переліку функцій додалися нові, більш досконалі можливості:

– накопичення та збереження інформації;

– профілювання типової поведінки;

– виявлення аномалій та нестандартної активності;

– пріоретизація виявлених загроз.

Типовою проблемою багатьох систем забезпечення інформаційної безпеки є надмірна чутливість до найменших змін у середовищі. Це генерує

величезну кількість повідомлень та сповіщень, з якими команди безпеки фізично не можуть впоратися. Детальне розслідування кожного попередження стає неможливим через обмежені людські та часові ресурси.

UBA-технологія розв'язує цю проблему шляхом агрегації всіх попереджень, комплексної оцінки рівнів ризику та передачі спеціалістам з безпеки лише найбільш критичної інформації про відхилення, що потребують негайної уваги. Така інтелектуальна фільтрація призводить до значного підвищення ефективності роботи персоналу служби інформаційної безпеки, оскільки кількість помилкових спрацьовувань істотно скорочується, а фокус зміщується на реальні загрози (рисунок 1.1).

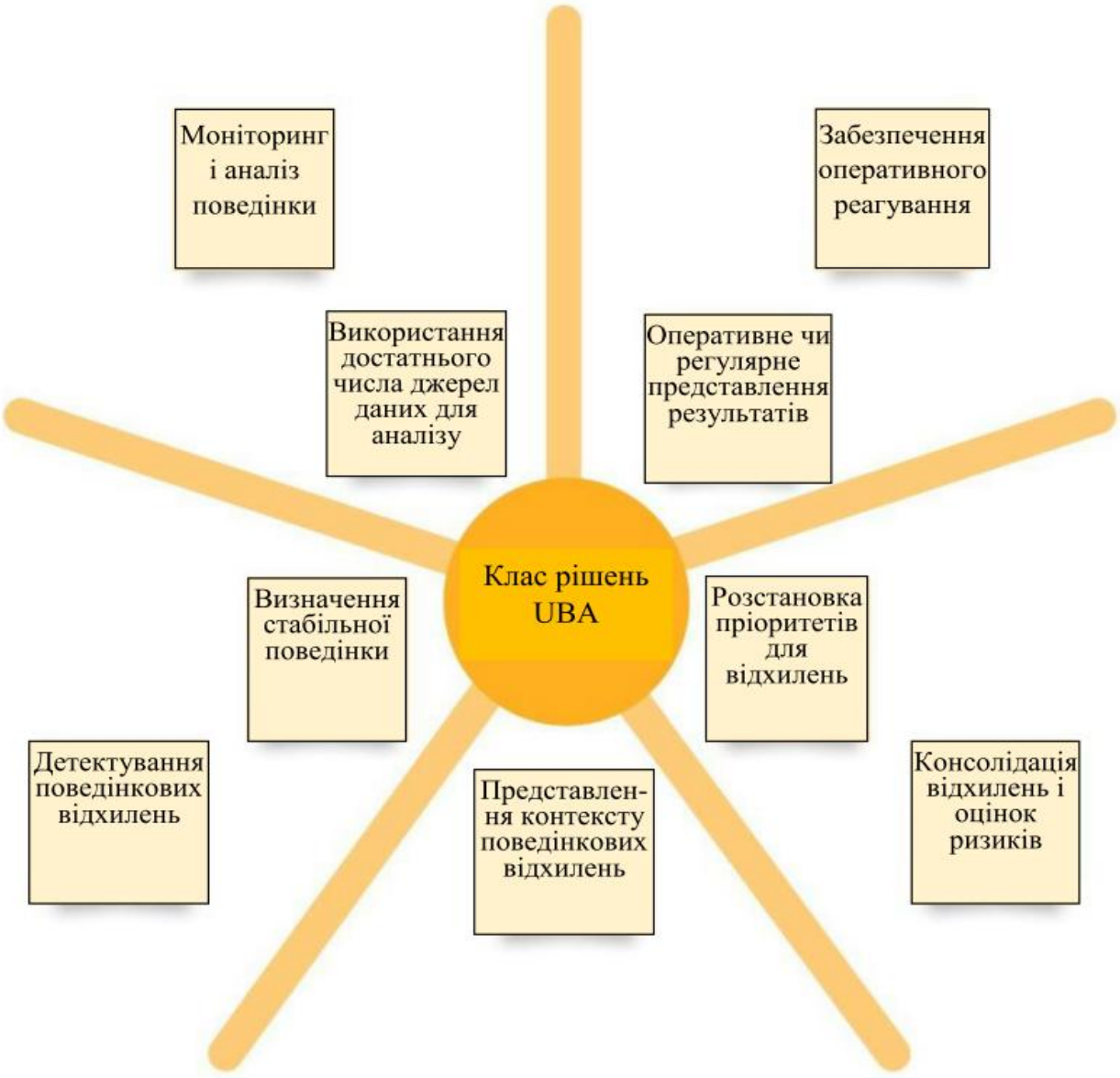

Рисунок 1.1 - Основні функції рішень класу UBA

Сучасні UBA-рішення часто включають додаткові корисні функціональні можливості:

- використання попередньо налаштованих шаблонів поведінки для різних об'єктів моніторингу;
- автоматичне сповіщення про виявлені аномалії в діях користувачів;
- гнучкі інструменти пошуку для проведення детальних розслідувань інцидентів;
- формування аналітичних звітів за результатами моніторингу;
- хронологічне відображення подій для аналізу динаміки поведінки в часі;
- аналіз історичних даних для виявлення аномалій, що відбулися в минулому.

Складні обчислювальні процеси такого масштабу стали можливими завдяки розвитку потужних технічних засобів та програмного забезпечення, які супроводжують користувача в цифровому середовищі.

Такі системи мають самостійно пристосовуватися до змін у контексті роботи та звичках користувачів, забезпечуючи стабільне функціонування при мінімальному ручному втручанні. Це вимагає здатності системи навчатися на основі спостережень за діями користувачів та аналізу вхідних даних. При цьому необхідна умова доступності для користувача призводить до вимог передбачуваності, здатності пояснення своїх дій та надання можливості користувачам розпізнавати та коригувати знання, отримані системою. Усе це приводить до методів, які використовують логічні правила при міркуваннях та поданні знань. При цьому необхідною буде певна статична попередня обробка інформації з датчиків, але незважаючи на це, такий підхід має помітні переваги при прийнятті базового логічного формалізму — простого та модульного виконання з використанням принципових уявлень часу та простору і структур політик.

Варто відзначити, що вивчення поведінкових патернів користувачів методом індуктивного аналізу створює певні виклики.

Система потребує безперервного навчання, оскільки дані про поведінку надходять постійно, що вимагає регулярного оновлення правил та накопичених знань. Також необхідно враховувати часові фактори для відстеження стабільності поведінки та її еволюції, включаючи випадки, що суперечать раніше встановленим закономірностям. У зв'язку з цим система має підтримувати немонотонну логіку міркувань.

Їй слід працювати з неповними даними, забезпечуючи при цьому ретельний контроль процесу аналізу. Це необхідно для дотримання принципів обмеження простору пошуку (зокрема, мінімізації модифікацій базової теоретичної моделі) та зручності взаємодії з користувачем.

1.3 Тенденції розвитку SIEM-систем

На основі аналізу експертних оцінок визначено найперспективніші напрями розвитку технологій кібербезпеки, що сприятимуть удосконаленню SIEM-систем:

- автоматизація реагування на інциденти інформаційної безпеки;
- підвищення кваліфікації фахівців з адміністрування систем;
- розширення можливостей SIEM шляхом інтеграції технологій аналізу поведінки користувачів (UBA);
- використання хмарних технологій для збору даних та надання сервісів за моделлю «as a service»;
- моніторинг активності на кінцевих пристроях та дослідження мережевого трафіку.

Впродовж останніх 15 років SIEM сприймається переважно як інструмент агрегації інформації з різноманітних джерел та її кореляційної обробки, при цьому аналіз зібраних даних обмежується лише кореляційними методами.

Для підвищення ефективності моніторингу подій безпеки потрібно чітко визначити:

- принципи нормалізації даних;
- набори правил для виявлення загроз;
- способи підключення джерел інформації;
- процедури введення джерел в експлуатацію;
- специфікацію правил детектування;
- інструкції з реагування при спрацюванні правил.

Наразі рівень охоплення SIEM-технологій становить 50-60%, а якість їх впровадження оцінюється на середньому рівні (3 бали).

Іншим трендом потенційного розвитку SIEM-рішень є автоматизація відповіді на інциденти. Виходячи з результатів опитування, проведеного Positive Technologies, одна четверта частина всіх опитаних спеціалістів у сфері ІБ працює в SIEM-системі щодня 2–4 години. Самими трудомісткими завданнями були названі: аналіз інцидентів (назвали 52% учасників опитування) та обробка хибних спрацьовувань - внесення змін до правил кореляції (58%). Налаштування джерел даних, а також моніторинг їх працездатності займають значну кількість часу на думку 30% фахівців. Така ситуація сприяє еволюції SIEM-рішень у бік програмних рішень Security orchestration and automated response (SOAR), які вирішують питання автоматичного реагування та оркестрації систем безпеки. Для цієї технології покриття приблизно дорівнює 60-70%, рівень якості реалізації, на думку експертів, дорівнює 3.

Як третій напрямок для розвитку SIEM слід вказати взаємопроникнення технологій аналізу логів (SIEM-рішення), аналіз мережевого трафіку (Network Traffic Analysis, NTA-рішення), а також аналіз ситуації на кінцевих вузлах (Endpoint Detection & Response, EDR-рішення). За відсутності можливостей, що надаються EDR-системами та детального аналізу трафіку, моніторинг не можна вважати повним. Аналіз мережевого трафіку в найближчі роки буде обов'язковою процедурою при проведенні SIEM, аналіз ситуації на кінцевих

вузлах стане опціональною можливістю функціоналу. Для цієї технології частка покриття дорівнює 60-70%, а якість її реалізації експерти Positive Technologies вважають рівним 2 балам.

Четвертою тенденцією можна назвати додавання можливостей UEBA-рішень (механізмів аналізу поведінки об'єктів) до інструментів SIEM, що дасть можливість отримання повної картини ситуації в інфраструктурі на єдиному екрані. Принципова різниця між UEBA та SIEM полягає в тому, що кошти UEBA розробляють моделі поведінки, а SIEM-рішення є деяким конструктором, що збирає логи. В алгоритмах пошуку та вивчення інцидентів можуть використовуватись різні підходи: машинне навчання, глибоке навчання, статистичний аналіз тощо. Ці підходи дають оператору інформацію про те, які об'єкти ведуть себе нетиповим для них чином і чому така поведінка нехарактерна для них. Частка покриття цієї технології складає 70-80%. Уро-рівень якості реалізації відповідає 4 балам.

Наступний тренд у розвитку SIEM пов'язаний з використанням хмарних технологій. Дослідження, яке провела компанія Enterprise Strategy Group у 2019 р. на замовлення Intel Corp. і Dell Technologies, показало, що 64% організацій планували збільшення витрат на публічні хмарні платформи порівняно з попереднім роком. Ця тенденція стимулює вендорів до додавання найбільш широко використовуваних платформ (Google Cloud Platform, Microsoft Azure, Amazon Web Services) у перелік підтримуваних джерел SIEM. Крім того, вендори починають самі пропонувати системи SIEM за допомогою підходу «as a service», доповнюючи способи розгортання, налаштування та управління системою SIEM (хмарних, віртуальних пристроїв - virtual appliance). На думку експертів, покриття технології дорівнює 60-70%, якість реалізації дорівнює 3 бали.

Частина цих тенденцій уже знаходить практичне втілення (рисунок 1.2), решта набуде поширення протягом найближчих 1-3 років. Впровадження цих технологій підвищує ефективність роботи SIEM-систем та дозволяє зменшити

робоче навантаження на спеціалістів, які займаються моніторингом та відповіддю на інциденти безпеки.

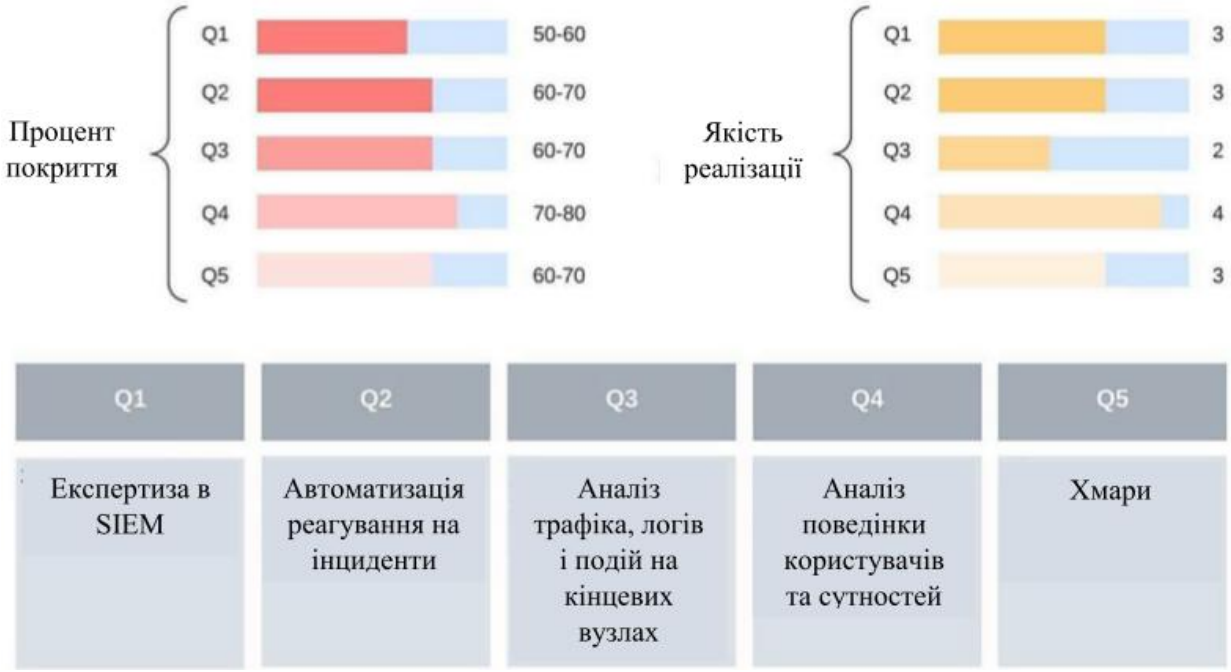

Рисунок 1.2 - Напрями еволюції SIEM-систем (шкала оцінювання якості впровадження: 1 - низька якість реалізації; 2 - якість нижче середньої; 3 - середня якість; 4 - якість вище середньої; 5 - висока якість реалізації)

Представлені дані базуються на експертному аналізі компанії Positive Technologies. Виявлені тенденції характерні для провідних постачальників SIEM-рішень на ринку (перелік лідерів сформовано на основі даних дослідницької компанії IDC).

2 РОЗРОБКА БАГАТОРІВНЕВОЇ МАСШТАБОВАНОЇ АРХІТЕКТУРИ МОДЕЛІ КОНТРОЛЮ ДОСТУПУ

2.1 Розробка політик безпечного доступу до інформаційних систем

Забезпечення безпечного доступу до конкретної інформаційної системи передбачає реалізацію декількох напрямів інформаційної безпеки, кожен з яких зараз оформлюється як окрема політика доступу (ПД). Політика забезпечення безпечного доступу являє собою структурований комплекс інструментів, методик та процедур, спрямований на вирішення завдань захисту доступу до операційної системи.

Сьогодні існує широкий спектр спеціалізованих політик. Сформуємо перелік ПД, що гарантують захищений контрольований доступ:

1) політика системи управління інформаційною безпекою;
2) політика надання прав доступу до ОС та їх контролю (політика керування доступом);
3) політика розмежування доступу;
4) політика чистого робочого місця та екрана;
5) політика щодо прихованого програмного забезпечення;
6) політика завантаження програмного забезпечення із зовнішніх або через зовнішні мережі;
7) політика використання мобільних пристроїв та даних (політика мобільного коду);
8) політика створення резервних копій;
9) політика міжорганізаційного обміну інформацією;
10) політика коректного використання електронних комунікацій;
11) політика зберігання записів (політика знищення даних);
12) політика експлуатації мережевих сервісів;
13) політика мобільних обчислень та комунікацій;
14) політика віддаленої роботи;

15) політика застосування криптографічного захисту (політика криптографічних засобів);

16) політика дотримання вимог;

17) політика ліцензування програмних продуктів;

18) політика обліку, зберігання та утилізації електронних і паперових носіїв (політика деінсталяції програмного забезпечення).

19) політика захисту і секретності даних;

20) політика протоколювання та аудиту;

21) політика контролю цілісності;

22) політика використання міжмережевих екранів;

23) політика аналізу вразливостей;

24) політика забезпечення стійкості до відмов;

25) політика безпечного відновлення системи;

26) політика створення захищених тунелів;

27) політика відновлення після збоїв;

28) політика фізичного захисту інформаційних систем;

29) політика адміністративного управління;

30) політика ідентифікації та перевірки автентичності;

31) політика роботи кінцевих користувачів;

32) політика антивірусного захисту;

33) політика здійснення ремонту, конфігурування та модернізації обладнання, що входить до складу автоматизованих систем обробки конфіденційних даних;

34) політика парольного захисту;

35) політика резервування та відновлення функціонування обладнання, програмного забезпечення та баз даних;

36) політика управління обліковими записами;

37) політика захисту автоматизованих робочих місць;

38) політика запобігання витоку інформації через технічні канали.

Залежно від специфічних вимог, перелік часткових політик доступу може бути деталізованим або скороченим. Зокрема, для захисту персональних даних поряд із загальною політикою доступу виокремлюють ключові види спеціалізованих політик (їх номери відповідають наведеному вище переліку), які підлягають перевірці під час атестації автоматизованих систем обробки конфіденційної інформації на відповідність вимогам безпеки персональних даних.

Серед усіх перелічених політик, політика контрольованого доступу посідає одне з найважливіших місць. Це зумовлено тим, що практично будь-яка зловмисна атака передбачає неавторизоване проникнення в захищену зону, де розміщений цільовий інформаційний ресурс, тобто включає несанкціоновані дії (НСД). Більше того, перший міжнародний стандарт інформаційної безпеки (відомий як «Помаранчева книга») базується на фундаментальній аксіомі безпеки [27]: «…what it really meanstocall a computer system "secure." …secure systems will control … access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information.» - «…що насправді означає називати комп’ютерну систему «безпечною». …захищені системи контролюватимуть … доступ до інформації таким чином, що тільки належним чином уповноважені особи або процеси, що працюють від їх імені, матимуть доступ читати, писати, створювати або видаляти інформацію.». Отже, згідно з концепцією «Помаранчевої книги», безпечна система — це система, що регулює доступ до інформації так, щоб лише уповноважені користувачі або процеси, що виконуються від їхнього імені, мали можливість читати, записувати, створювати та видаляти дані. Іншими словами, це положення стверджує, що всі питання забезпечення інформаційної безпеки зводяться до управління доступом суб'єктів до об'єктів.

Дане положення було прийнято більшістю провідних спеціалістів з інформаційної безпеки в усьому світі і повторено в стандартах та нормативних документах інших країн. У дійсності, це положення не є коректним, оскільки,

як видно знаведеного вище переліку 38 часткових політик безпеки, контроль доступу — це лише одна з приватних політик (хоч і найважливіша), і тому вона в принципі не може замінити всі інші види часткових політик; наприклад, проблеми, пов'язані з побічними електромагнітними випромінюваннями і наведеннями (ПЕМІН), не можуть бути природним чином укладені в рамки контролю доступу. Зазначимо, однак, що багато інших приватних політик справді націлені на підтримку політики управління доступом, і, насамперед, політика облікових записів, політика ідентифікації та аутентифікації, політика парольного захисту та ін.

Міжнародним еквівалентом Помаранчевої книги є стандарт ISO/IEC 15408, виданий у 2005 році, який ратифікували численні держави.

Проте, незважаючи на наведені доводи, питання контролю доступу (до інформаційних ресурсів, об'єктів та систем обробки інформації, інших елементів системи) залишається центральним у забезпеченні інформаційної безпеки, а більшість інших спеціалізованих політик значною мірою спрямовані на ефективну підтримку системи контролю та управління доступом.

У контексті інформаційного середовища замість терміну «контроль доступу» часто застосовується поняття «розмежування доступу». Проте для комплексного вирішення всіх питань, пов'язаних з доступом, в рамках єдиного підходу як до інформаційного, так і до фізичного середовища використовується формулювання «контроль та управління доступом» — цей термін найточніше відображає суть процедури доступу.

Зазначимо, що контроль доступу полягає у виконанні всіх дій та заходів, спрямованих на забезпечення доступу відповідно до встановленої політики КД, тоді як управління передбачає наявність механізмів адекватного реагування на ситуації, пов'язані з потенційними порушеннями процедури доступу, які не були передбачені обраною політикою КД. Наприклад, виникли нові загрози, які раніше не вважалися актуальними і тому не були враховані в політиці інформаційної безпеки.

Опишемо більш детально зміст політики контролю та управління доступом. Призначення: політика КД визначає правила представлення співробітникам доступу до ОС, що захищаються.

Ключові принципи політики контрольованого доступу є наступними. До роботи з інформаційними ресурсами обмеженого доступу допускаються користувачі, які ознайомлені з правилами роботи з цими ресурсами та несуть відповідальність за порушення встановлених правил. Кожному працівнику, який отримав дозвіл на роботу з певним інформаційним ресурсом, має бути присвоєно персональний унікальний ідентифікатор (обліковий запис користувача), під яким він здійснюватиме реєстрацію та роботу в інформаційній системі. За необхідності окремим працівникам може бути надано кілька унікальних ідентифікаторів (облікових записів). Спільне використання одного облікового запису кількома суб'єктами при роботі з операційною системою (колективного облікового запису) категорично забороняється.

Для повноти визначення необхідно описати основні дії (процедури), які можуть відбуватися з ОЗ. Основними є такі процедури:

1) створення ОЗ;

2) видалення ОЗ;

3) продовження ОЗ;

4) внесення змін до ОЗ;

5) зберігання документів, на основі яких були виконані певні дії з ОЗ.

Процес створення облікового запису, тобто реєстрації користувача, а також продовження строку дії облікового запису або внесення до нього змін ініціюється через подання заявки. Заявка має містити ідентифікаційні дані особи-заявника та обґрунтування для виконання відповідної операції з обліковим записом. Заявка підлягає затвердженню керівником структурного підрозділу, уповноваженого подавати такі заявки відповідно до чинної політики безпеки. Заявка узгоджується з адміністратором щодо регламентованих обмежень для даного облікового запису. Виконання заявки

здійснює системний адміністратор. Після завершення реєстрації облікового запису в заявці проставляється відмітка про виконання завдання із підписами відповідальних виконавців.

При настанні моменту припинення терміну дії повноважень користувача ОЗ має негайно блокуватися. У заявці поряд з ідентифікуючою інформацією наводиться основа, що породжує необхідність припинення терміну дії повноважень користувача. Заявка узгоджується із системою ІБ та передається на виконання системному адміністратору.

Усі оброблені заявки передаються відповідальному працівнику архіву згідно з встановленою процедурою та зберігаються в архіві впродовж терміну, визначеного політикою інформаційної безпеки. Копії опрацьованих заявок залишаються у системного адміністратора для здійснення необхідних дій у надзвичайних та нестандартних ситуаціях, а також з метою контролю.

Стосовно систем обробки даних проблема контролю доступу зводиться, перш за все, до контролю доступу до різних інформаційних систем: операційній системі, баз даних, системі електронного документообігу та ін., до технічних засобів обробки даних та інших об'єктів. Найбільш важливою з інформаційних систем з точки зору забезпечення ІБ є операційна система, встановлена на комп'ютерних системах об'єкта захисту, а також на інших корпоративних засобах зв'язку дя обробки даних — насамперед, на мобільних пристроях зв'язку.

В останні роки ця проблема значно загострилася через стрімкий розвиток інтернету, що спричинило появу численних нових типів загроз — мережевих. Ці загрози виявилися суттєво небезпечнішими, що зумовило бурхливий розвиток різноманітних засобів та механізмів мережевого захисту комп'ютерних систем. Політичні кола багатьох держав активно порушують питання про необхідність повного державного контролю над мережевим трафіком на національному рівні, створення власних апаратно-програмних засобів обробки інформації.

Отже, об'єктами доступу, які становлять інтерес для зловмисних дій, є інформаційні системи об'єкта захисту, технічне обладнання для обробки даних, а також безпосередньо самі процеси обробки інформації.

2.2 Концепція розробки системи контролю доступу до ресурсів інформаційних систем

Сучасні системи доступу містить широкий спектр засобів для контролю, ідентифікації і верифікації кожного користувача (рисунок 2.1).

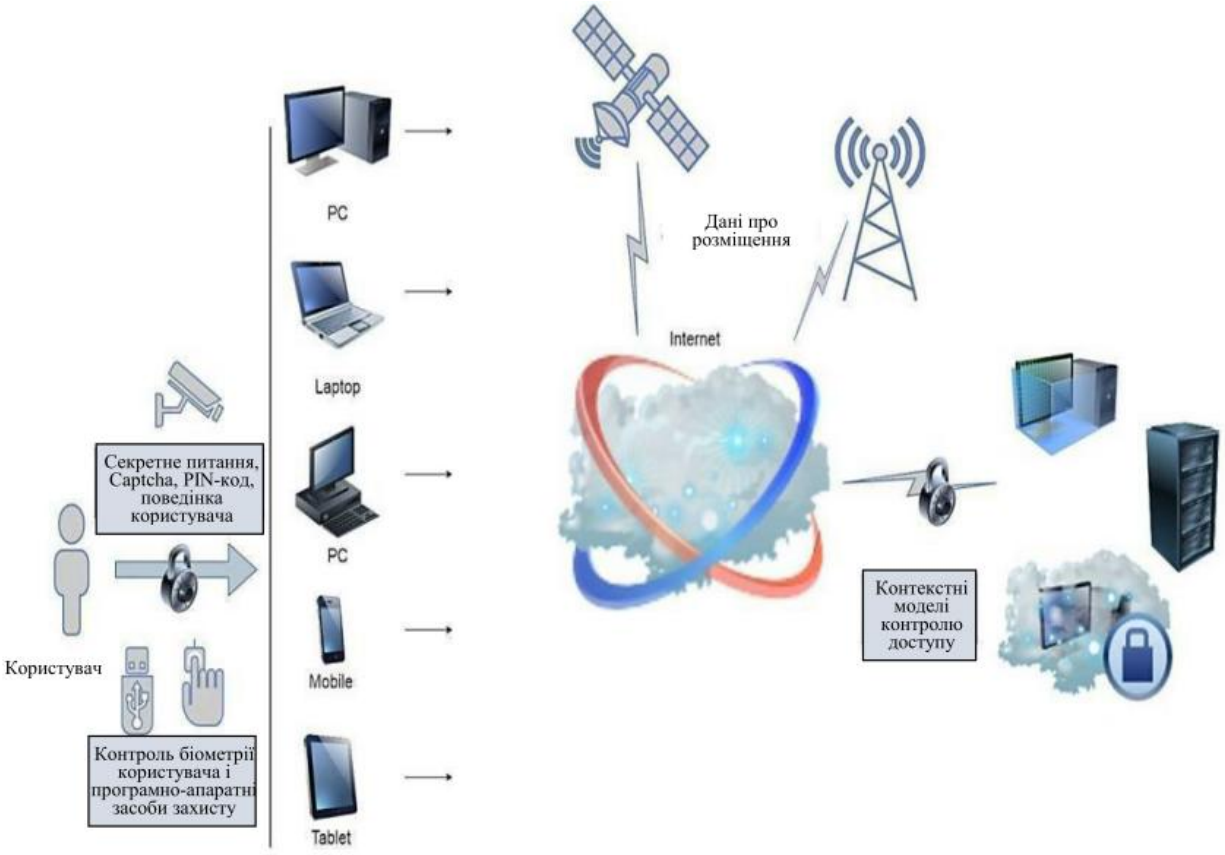

Рисунок 2.1 – Приклад архітектури обчислювального комплексу із багаторівневим КД

Вимоги до забезпечення контролю доступу та умови експлуатації можна сформулювати таким чином. Обчислювальний комплекс із системою захищеного контролю доступу до операційної системи через комп'ютерні

мережі надає можливість доступу з будь-якого пристрою користувача. При цьому здійснюється ідентифікація користувача із застосуванням різноманітних біометричних методів (наприклад, сканування відбитка пальця, вбудовані або зовнішні камери), у процесі доступу застосовуються програмні засоби верифікації (контрольне питання, PIN-коди, Captcha). Наразі активно розвиваються системи аналізу поведінки користувачів (наприклад, реакція користувачів на запити доступу або поведінкові патерни). Складовою контролю доступу є визначення місцезнаходження користувача, ці відомості можуть бути зіставлені з інформацією у профілі користувача. Для доступу до сервісів існує рівень контролю доступу, що забезпечується контекстними моделями. Такими моделями можуть бути політики, побудова моделей на основі журналів подій, відповідних груп користувачів, а також спеціалізовані методики, характерні для предметної області сервісу — медичні, банківські, освітні, які мають власні спеціалізовані протоколи та особливості доступу. На рівні обчислювальних ресурсів — серверів, віртуальних машин, баз даних — реалізується апаратний контроль доступу.

Таким чином, за змістом процес доступу до операційної системи описується відношенням певної групи суб'єктів до визначеної сукупності ресурсів, до яких ці суб'єкти прагнуть отримати доступ.

Для опису, формалізації, аналізу чи синтезу системи контрольованого доступу необхідно передусім описати три основні його складові:

- суб'єктів, що беруть участь у системі КД;
- ресурси;
- об'єкти, які становлять інтерес для суб'єктів.

Зауважимо, що в процесі контрольованого доступу ставиться завдання забезпечення безпеки усіх необхідних характеристик даних, для яких обмежено доступ.

Під суб'єктом розуміється не лише фізична чи юридична особа, яка бажає скористатися певним програмно-апаратним чи інформаційним ресурсом в інформаційній системі, а також інформаційні процеси, програмно-

апаратні засоби, які можуть отримати доступ до ОС. Таким чином, під суб'єктом розуміється будь-який об'єкт або процес, який може здійснити певну дію в інформаційній системі з використанням процесорних пристроїв системи. Приклади суб'єктів програмно-апаратного типу:

- операційна система;

- антивірусні та мережеві засоби;

-інформаційні системи конкретного призначення (редактори, СУБД, системи електронного документообігу, системи для обслуговування бізнес-процесів, зокрема, 1С тощо).

Під об'єктом, що здійснює доступ, розуміються будь-які поіменовані елементи інформаційної системи, до яких може отримати доступ хоча б один з процесорних пристроїв: інформаційні системи:

- периферійне та мережеве обладнання;

- файли;

- носії інформації;

- зовнішні пристрої різного призначення.

Більше того, одні об'єкти доступу можуть бути частиною інших об'єктів (якщо вони поіменовані та доступні для процесорів); наприклад, флешка та файли, записані на ній є об'єктами доступу, такими ж є база даних і окремі записи, що містяться в ній, міжмережевий екран та окремі його параметри, доступні для процесорів.

Доступ описує безпосередньо набір тих дій, які може здійснювати даний суб'єкт над цим об'єктом. Таким чином, доступ прив'язаний до пари «суб'єкт-об'єкт» і являє собою набір дозволених (санкціонованих) дій, які може вчиняти суб'єкт над об'єктом. Основними видами доступів є читання та запис даних. Багато інших видів дій з даними можуть з деяким ступенем умовності зведені до цих видів доступу. Наприклад, видалення файлу може розглядатися як запис порожніх даних у файл – у цьому випадку порожній файл ототожнюється з віддаленим файлом, що в цілому не завжди коректно. Далі, додавання даних у файл ототожнено із записом даних. Однак, якщо дані

структуровані (наприклад, у базах даних), то подібне додавання вимагає попереднього формування структурного скелета нового запису, що вже не вкладається у схему просто запису даних у файл. Тому до перерахованих видів дій, які можуть входити в доступ, додаються також видалення об'єкта (файлу, пристрою з переліку тощо), додавання об'єкта (записи, пристрої), активації об'єкта (запуску програми, включення технічного пристрою), модифікація (заміна), блокування, контроль права власності (включаючи авторизацію, підтвердження авторства чи авторських прав). До складу можливих видів доступу можуть бути включені інші більш специфічні дії.

2.3 Моделі контролю доступу

Процес встановлення та реалізації прав доступу для пари «суб'єкт-об'єкт» із визначених переліків суб'єктів і об'єктів та механізм зміни прав під час роботи інформаційної системи становить основну суть політики доступу. На сьогодні виділяється три основні підходи до побудови системи контрольованого доступу: 1) дискреційний; 2) мандатний; 3) рольовий. Розглянемо детальніше кожен із зазначених підходів.

Дискреційне управління доступом (Discretionary Access Control, DAC), чи розмежувальна політика доступу (РПД) — це політика, за якої процедура надання/відмови у доступі базується на характеристиках самих об'єктів доступу. Кожен об'єкт доступу має низку характеристик, насамперед, рівень конфіденційності та його цінність — навіть за однакових рівнів конфіденційності цінність об'єкта, включаючи його вартість та можливі збитки від порушення його безпеки, можуть відрізнятися. Значення зазначених характеристик зазвичай визначаються власником об'єкта. Тобто спочатку передбачається, що кожний об'єкт має власника. Власник володіє всіма правами доступу до об'єкту, включаючи, як правило, право передавати частково або повністю свої права на цей об'єкт (технічний засіб, програмну

систему, інформаційну базу тощо) іншим суб'єктам, зокрема, надавати в оренду, продавати або разово використовувати.

При РПД об'єктами контролю, на основі аналізу яких і приймаються управлінські рішення, є безпосередньо об'єкти роботи даних. Тому, найпростіший спосіб задання РПД полягає у перерахуванні для кожної пари «суб'єкт-об'єкт» надані права доступу із супутніми умовами та обмеженнями. Це перечислення може бути представлене у вигляді матриці, рядки якої відповідають суб'єктам системи, а стовпці - об'єктам доступу; на перетині перераховуються дозволені види доступів із супутніми обмеженнями. Описана матриця називається матрицею доступу. На рисунку 2.2 наведено приклад матриці для дискреційної моделі доступу.

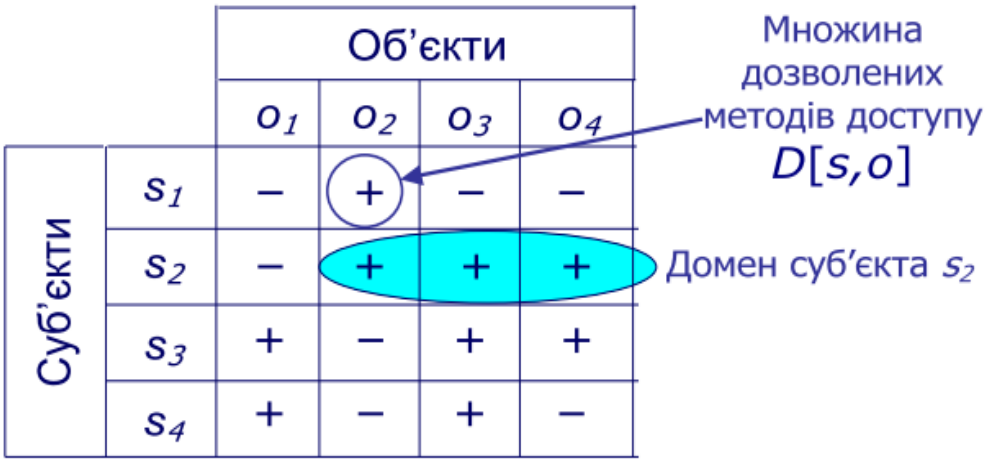

Рисунок 2.2 - Приклад матриці для дискреційної моделі доступу

Таким чином, будь-яка РПД задається матрицею доступу, яка однозначно визначає конкретну РПД, і принцип доступу, що лежить в основі РПД може бути сформульований наступним чином: дозволено тільки те, що записано у матриці доступу. Ця процедура доступу реалізує заборонний принцип доступу, коли дозволено тільки те, що записано, а все інше заборонено — на відміну від дозвільного принципу доступу, коли перераховується все, що заборонено, а все інше - дозволено.

Концепція розмежувальної політики доступу (РПД), яка за своєю суттю має понад двотисячолітню історію як елемент систем фізичної охорони та захисту об'єктів, при застосуванні до систем обробки інформації демонструє низку суттєвих вад. Насамперед, ця політика контрольованого доступу, навіть за умови найсуворішого дотримання всіх вимог політики інформаційної безпеки, загалом не гарантує безпеку в перспективі — існують конкретні випадки РПД, для яких математично доведено неможливість забезпечення гарантій безпеки.

Другою суттєвою вадою цієї політики, особливо критичною, є беззахисність перед атаками за допомогою шкідливих закладок типу троянських програм. Проілюструємо це твердження на прикладі. Припустимо, у системі присутні два користувачі U_1 і U_2, при цьому U_2 є зловмисником. До об'єктів захисту належать три інформаційно-програмні елементи O_1, O_2 і O_3, де:

- елемент O_1 містить конфіденційні дані, які заборонені для користувача U_2;
- елемент O_2 містить інформацію обмеженого використання, доступну обом користувачам, причому рівень конфіденційності елемента O_2 не поступається рівню конфіденційності O_1;
- елемент O_3 є загальнодоступним.

Для неавторизованого отримання інформації з елемента O_1 користувач U_2 може діяти наступним способом. Запустивши елемент O_3 зі своїми обліковими даними, користувач U_2 може впровадити в нього троянську програму, яка дозволить реалізувати такий сценарій: O_3 під час паралельної роботи з O_2 (яку також може ініціювати U_2) впроваджує в O_2 програму, призначену для копіювання певної інформації з O_1 до O_2 в момент, коли обидві програми функціонуватимуть одночасно (будуть активовані користувачем U_1), що на практиці рано чи пізно неминуче станеться. Після цього троянська програма скопіює ці дані з O_1 в O_2, звідки зловмисник U_2 зможе їх отримати. Варто наголосити, що витік інформації відбувся без формального порушення

встановлених правил доступу. Практична імплементація такого каналу витоку на базі троянської програми потребує додаткової деталізації.

У підсумку можна зазначити, що класична дискреційна політика доступу, попри свою структурну простоту, легкість реалізації та надзвичайно широке поширення (оскільки переважна більшість програмних систем ґрунтується саме на принципах РПД), має низку суттєвих вад. Ці недоліки не дозволяють беззастережно використовувати її як достатню та самодостатню основу для побудови сучасних механізмів контролю доступу. Водночас повна відмова від дискреційного підходу також є неможливою, адже специфіка його роботи зумовлює те, що елементи дискреційності так чи інакше інтегровані навіть у більш суворі та структуровані моделі, такі як мандатна політика чи рольове управління доступом. Обидві ці моделі містять механізми, що допускають або передбачають певну свободу прийняття рішень щодо доступу, тобто фактично використовують окремі елементи РПД.

У зв’язку з цим постає завдання не відмови від дискреційної політики, а удосконалення її механізмів так, щоб мінімізувати її слабкі сторони й значною мірою нейтралізувати негативні наслідки, властиві цьому підходу. Водночас слід розуміти, що досягнення абсолютної безпеки неможливе. Проведений аналіз показує, що гарантувати повну й безумовну захищеність у майбутньому в принципі не можна, оскільки об’єкти, щодо яких здійснюється контроль доступу, постійно змінюються, оновлюються й піддаються впливу зовнішніх факторів. Це робить недосяжною вимогу повної передбачуваності поведінки системи захисту для будь-якого можливого сценарію.

Саме тому до дискреційної політики доступу зазвичай не висувають вимоги забезпечити абсолютну гарантію захищеності на перспективу. Натомість метою стає досягнення певного гарантованого рівня безпеки з ймовірністю, що не опускається нижче встановленої межі. Такий підхід відповідає концепції гарантованої якості функціонування (Quality-of-Service, QoS), що дозволяє контролювати та кількісно оцінювати ступінь надійності

механізмів доступу й забезпечувати прийнятний рівень захисту в умовах неможливості отримання повної гарантії.

Мандатне управління доступом (MandatoryAccessControl - MAC), або повноважна політика доступу (ППД) - політика КД, при якій процедура надання/ненадання доступу спирається на характеристики не об'єктів доступу, а інформаційних потоків, які виникають між об'єктами та суб'єктами системи. Іншими словами, при здійсненні доступу відбувається переміщення інформації між суб'єктом і об'єктом доступу - це переміщення називається інформаційним потоком. Всім об'єктам і всім суб'єктам приписуються мітки, що позначають їхній рівень секретності або рівень доступу відповідно. Тоді принцип доступу в рамках ППД може бути сформульований наступним чином: дозволені тільки ті потоки, які не приводять до інформаційного потоку від більш секретного об'єкта або суб'єкта до менш секретного об'єкта чи суб'єкта; при рівних рівнях секретності всі потоки дозволені. Таким чином, мандатне управління доступом спирається на заборонний принцип доступу, на відміну від дискреційного управління доступом.

Розглянемо тепер більш детально, в чому полягає різниця між цими двома політиками КД. Спочатку розглянемо два базові види доступу: читання та запис. Під час читання інформаційний потік спрямований від об'єкта до суб'єкта; тому потік буде дозволеним, якщо рівень секретності об'єкта не нижче рівня доступу об'єкта, що збігається з правилом дозволеного доступу до РПД. Таким чином, стосовно читання правила доступу для обох політик (РПД і ППД) збігаються. При реалізації доступу «запис» інформаційний потік спрямований від суб'єкта до об'єкту; тому рівень доступу суб'єкта повинен бути не нижче рівня таємності об'єкта. Проте за дискреційної політики, якщо рівень доступу суб'єкта нижче рівня таємності об'єкта, то доступ до запису також заборонений. Таким чином, стосовно доступу «запис» правила доступу в РПД і в ППД протилежні. До дій типу «запис» зводяться й інші важливі види доступу: додавання даних, зміна, знищення. Таким чином, у всіх перерахованих доступах правила доступу в РПД та ППД протилежні.

Описане правило запобігає утворенню каналу витоку інформації, який був розглянутий раніше під час аналізу недоліків дискреційної моделі доступу. Суть його полягає в тому, що в політиці примусової (мандатної) безпеки для того, щоб троянська програма, розміщена в об'єкті O_2, могла прочитати конфіденційні дані з об'єкта O_1 і передати їх назад у O_2, необхідно, щоб обидва об'єкти мали однаковий поточний рівень секретності. Лише за цієї умови виконання операції читання та подальшого запису було б можливим.

Однак, якщо користувач U_2 має право читати дані з O_2, то згідно з правилами мандатної політики його рівень доступу за операцією читання має бути не нижчим за рівень секретності O_2, а отже — і O_1. За таких умов користувач U_2 здатний отримати інформацію безпосередньо з O_1, не звертаючись до O_2. Отже, U_2 у цьому випадку не може мати права читання для O_2, і вся схема організації витоку за допомогою O_2 втрачає сенс — вона не дозволяє користувачу отримати доступ до потрібних даних.

Разом із тим, застосування мандатної політики доступу породжує низку труднощів. Розглянемо дві ключові. По-перше, згідно з правилом запису, якщо рівень секретності суб'єкта перевищує рівень секретності об'єкта, то суб'єкт не має права записувати дані в цей об'єкт. Це створює практичні обмеження: наприклад, керівник, який має вищий рівень доступу, ніж його підлеглий, технічно не може передати жодної інформації співробітникові, адже запис у «менш секретний» об'єкт для нього заборонений. Така ситуація очевидно суперечить реальній логіці управління персоналом.

Щоб усунути цю проблему, у мандатній моделі вводиться поняття поточного рівня секретності об'єкта та поточного права доступу. Якщо потрібно передати інформацію від об'єкта з вищим рівнем секретності до об'єкта з нижчим, перед записом обидва об'єкти тимчасово переводять на однаковий проміжний рівень секретності — так званий поточний рівень. Після такого «вирівнювання» операція запису стає можливою та не порушує вимог політики безпеки.

Ще одна проблема в ППД: політика мандатного управління, як видно з наведеного опису, складніша за політику дискреційного керування доступом. Якщо відбудеться збій роботи самої системи мандатного управління доступом, то буде заблокована вся система обробки даних. Щоб уникнути подібної ситуації в ППД для вузької категорії користувачів, що включає адміністраторів інформаційної безпеки, вводиться можливість прямого втручання у процедуру управління доступом, що є, по суті, дискреційним управлінням доступом. Таким чином, при реалізації ППД не вдалося поки що позбутися РПД.

Однією з найвідоміших і найпоширеніших моделей, що реалізує принципи політики доступу, є модель Белла—Лападули (рисунок 2.2). Вона вперше була представлена в «Помаранчевій книзі» — офіційному стандарті *Trusted Computer System Evaluation Criteria* (TCSEC), розробленому Міністерством оборони США у 1983 році. Цей документ, який встановлював вимоги до захищених комп'ютерних систем, набув широкого розповсюдження під неформальною саме назвою «Помаранчева книга».

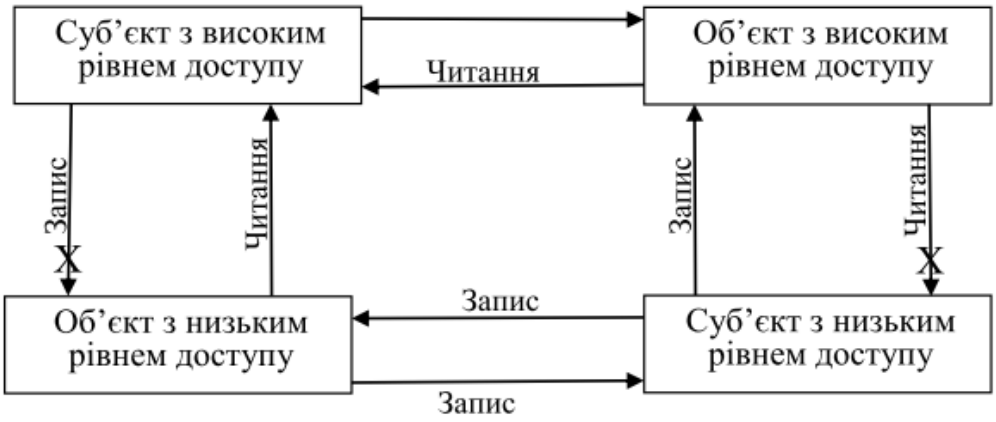

Рисунок 2.3 – Модель Белла-Лападула

У межах моделі Белла—Лападули реалізовано всі основні механізми примусового управління доступом, згадані вище. Для цієї моделі математично доведено, що якщо всі правила мандатної безпеки дотримуються протягом як

завгодно тривалого часу, то в майбутньому система залишатиметься захищеною від несанкціонованого доступу. Тобто модель гарантує неможливість зловмисного проникнення за умови коректного виконання її вимог. Це забезпечує рівень безпеки, що є принциповою перевагою повноважної політики над дискреційною, яка таких строгих гарантій забезпечити не може.

У дискреційній політиці доступу об’єктами контролю виступають не лише самі суб’єкти та об’єкти, а й інформаційні потоки, які виникають між ними. Насамперед враховуються напрямки цих потоків, оскільки саме вони визначають можливість передавання даних від одного елемента системи до іншого. Тому для опису мандатної політики доступу застосовують функції секретності для об’єктів та функції доступу для суб’єктів. Вони фіксують поточні характеристики кожного суб’єкта й об’єкта, а процедура реалізації ППД зводиться до порівняння значень цих функцій для кожної пари «суб’єкт—об’єкт» з урахуванням конкретної операції доступу.

Мандатне управління доступом забезпечує можливість строгого дотримання політики безпеки та гарантує захищеність у перспективі. Проте воно має і суттєві недоліки. Насамперед це структурна обмеженість існуючих моделей, які реалізують ППД: часто вони не дозволяють повністю врахувати всі вимоги до безпеки в реальних, складних інформаційних системах. Крім того, у разі масштабних ІТ-систем обсяг робіт із призначення та контролю прав доступу настільки великий, що виконання всіх необхідних операцій вручну стає вкрай складним або практично нереальним.

Таким чином, хоча мандатна політика вирішує одну з ключових проблем інформаційної безпеки — проблему гарантованого захисту в майбутньому, її практичне застосування поки що менш поширене, ніж використання дискреційної моделі. Причина полягає в тому, що формальні моделі ППД надто спрощені та не враховують низку специфічних вимог, характерних для реальних систем. Тому на практиці мандатна політика зазвичай використовується як доповнення до РПД. Наприклад, у поширених СУБД

основний механізм доступу заснований на дискреційному підході, а мандатні можливості додаються як окремий пакет розширень.

Рольова політика доступу (РлПД) ґрунтується на тому, що всім суб'єктам призначають певні ролі, які визначають межі допустимих дій користувача. Роль являє собою набір дозволів і заборон, формований як на основі принципів дискреційної політики, так і з урахуванням елементів мандатної моделі. Ба більше, сучасні системи рольового доступу реалізують підхід, у межах якого ролі можуть змінювати свій набір дозволених дій залежно від поточного стану інформаційної системи чи параметрів безпеки. Це дозволяє динамічно розширювати або звужувати повноваження користувача й робить рольову модель особливо гнучкою.

У межах РлПД об'єктами контролю виступають саме ролі, а не індивідуальні суб'єкти чи окремі об'єкти. Далі доцільно розглянути основні переваги та недоліки рольової політики порівняно з дискреційною (РПД) і мандатною (ППД), починаючи з визначення її сильних сторін.

Роль може динамічно змінюватися, дозволятися чи заборонятися в залежності від поточного стану системи, що дозволяє значно підвищити ефективність управління доступом і тим самим, ефективність забезпечення ІБ. Приклад однієї із схем РлПД навеений на рисунку 2.4.

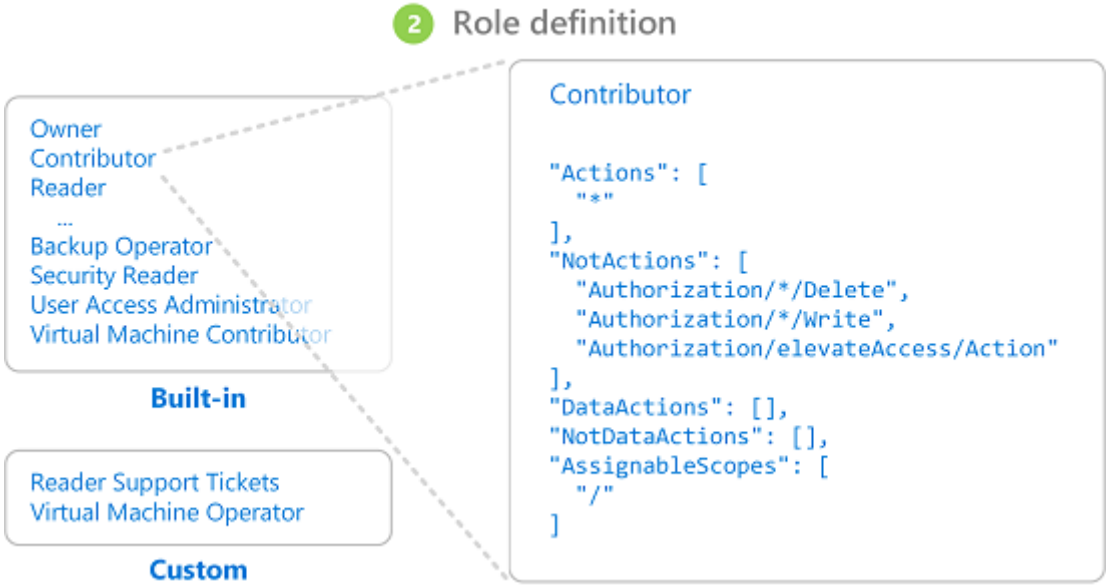

Рисунок 2.4 - Схема РлПД

Однією з серйозних проблем при практичній реалізації РПД та ППД, особливо для великих систем, є складність завдання та контролю прав доступу кожної пари «суб'єкт-об'єкт». Для вирішення цієї проблеми в рамках РПД та ППД часто створюють групи користувачів, наділяючи правами групу та приписуючи кожного користувача до деякої групи. Однак при цьому взаємодія всередині груп потребує окремої уваги, оскільки користувачі одного рівня прав можуть мати індивідуальні вимоги щодо доступу. У рольовій політиці доступу вибирається чи формується типовий набір ролей, у яких всі можливі проблеми взаємодії максимально усунуті. Задання політики управління доступом на основі ролей в цілому вимагає суттєво менших зусиль, ніж задання прав доступу на основі РПД та ППД.

Організація процесу управління доступом на основі ролей дозволяє формувати різні сценарії процесу забезпечення ІБ, в яких може бути зафіксована певна послідовність активізації ролей, допустиме поєднання ролей (у сенсі спільної реалізації їх в той самий момент), у тому числі з урахуванням запущених додатків.

Рольова модель управління доступом широко використовується в багатьох критично важливих сферах, зокрема в системах керування базами даних та електронного документообігу. Завдяки цьому інтеграція РлПД на рівні операційної системи є логічним та природним доповненням до рольових механізмів, що застосовуються в цих прикладних системах. Такий підхід забезпечує більш комплексне охоплення всіх можливих варіантів взаємодії користувачів із ресурсами системи та сприяє узгодженості політики доступу на різних рівнях.

Використання наборів ролей дозволяє значно точніше, ніж у випадку дискреційної чи мандатної політики, відобразити специфіку роботи сучасних систем обробки даних та задовольнити численні вимоги до безпеки. Ролі дають змогу враховувати як структурні особливості системи, так і функціональні обов’язки користувачів, забезпечуючи гнучкість та адаптивність налаштування прав доступу.

Разом із тим, рольова політика має і свій суттєвий недолік — відсутність строгого математичного доведення гарантованого виконання вимог безпеки в майбутньому. Це зумовлено високою складністю формальних моделей, на яких базується РлПД. Через значну багатовимірність та динамічність таких моделей їх повноцінний аналіз у ручному режимі майже неможливий, що ускладнює побудову формальних доказів гарантованості.

На жаль, існуючі методи автоматичного аналізу подібних моделей поки що малоефективні. Прикладом автоматичного аналізу подібних моделей є підхід, заснований на використанні методів темпоральної логіки.

Для проведення аналізу розглянемо три найпоширеніші моделі контролю доступу, надавши їм узагальнену характеристику та визначивши їх сильні й слабкі сторони. У результаті з’ясовано, що найвживанішою є дискреційна політика доступу. Її важливість зумовлена тим, що дві інші моделі частково базуються на принципах РПД і фактично містять окремі елементи дискреційного підходу.

Разом із тим РПД має низку істотних вад, які створюють підґрунтя для потенційних загроз та можуть бути використані зловмисниками. Саме тому виникає необхідність удосконалення дискреційної системи шляхом додавання нових механізмів, покликаних підвищити її рівень захищеності без порушення базових принципів. Далі наведемо кілька можливих напрямів підвищення ефективності.

Перш за все, доцільно застосовувати всі три політики доступу у поєднанні. Дискреційна (РПД) та мандатна (ППД) політики можуть функціонувати одночасно, причому операція доступу дозволяється лише тоді, коли вона не суперечить жодній із них. Найбільші труднощі при інтеграції цих політик виникають щодо операцій запису та операцій, що мають аналогічну логіку, оскільки правила доступу для запису в РПД і ППД мають протилежний характер.

Для подолання цієї проблеми аналіз доступу при виконанні операції запису слід здійснювати з урахуванням поточних рівнів секретності об’єктів і

поточних рівнів доступу суб’єктів. У такому випадку конфліктів між двома політиками не виникає, оскільки при "вирівнюванні" рівнів секретності допустимим є лише зниження або незмінність рівня доступу суб’єкта — його підвищення не допускається. За цієї умови паралельне використання РПД і ППД стає можливим і коректним.

Що стосується рольової політики (РлПД), то в межах кожної ролі можуть одночасно застосовуватися як дискреційні, так і мандатні механізми, а також їх комбінації. Це дозволяє створювати гнучкі, багатоетапні моделі доступу, які точніше враховують вимоги конкретної системи.

Таким чином, одночасне використання РПД, ППД та РлПД створює умови для значного підвищення рівня захищеності обчислювальних комплексів, забезпечуючи більш комплексний і багатовимірний підхід до контролю доступу.

3 РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ АРХІТЕКТУРИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1 Формування вимог та умов для проектування архітектури контролю доступу

Аналіз конфігурації інформаційних комплексів показує, що підвищення ефективності функціонування може бути досягнуто за рахунок використання в їх архітектурі систем КД на усіх елементах передачі даних. Використання певних зовнішніх систем та контурів КД не гарантує захист від витоку даних за межами вбудованого контуру на апаратному чи програмному рівнях. Такі системи вимагає великих ресурсів в зв’язку з додатковими програмними модулями та їх стикуваннями з програмно-апаратним забезпеченням ОС.

Наприклад, в архітектурі обчислювальних комплексів, що реалізує багаторівневий КД на основі концепції SIEM, необхідно реалізувати збір та зберігання подій. Відомості про стан різних елементів доступу до сервісів та управління подіями фіксуються обробниками подій, розподіленими по мережі на всіх рівнях. Кожен з обробників подій безпосередньо підключений до одного або кількох джерел. Кожен із обробників подій має набір правил. При обробці подій від локально підключених джерел застосовується набір правил. При виявленні порушення КД безпеки працівник подій видає попередження системи безпеки.

У найзагальнішому вигляді архітектуру SIEM-технології можна подати таким чином. Її функціонування забезпечується обчислювальним комплексом, що працює як сукупність веб-сервісів і має доступ до глобальної мережі. У межах цього підходу система контролю доступу передбачає перетворення правил SIEM у формалізовані структури.

З програмної точки зору необхідно організувати обробку даних про доступ та виконати трансформацію правил управління подіями в їх формальне подання, яке може бути використане під час розгортання у мережі вузлів-обробників подій. У самій мережі обробників подій реалізується механізм

впровадження та використання оптимізованих SIEM-правил, що дозволяє підвищити ефективність виявлення та реагування на події безпеки.

З розглянутих прикладів видно, що системи КД є частиною обчислювальних комплексів, що забезпечує комп'ютерні послуги. Водночас КД є також окремими компонентами, а під управління КД виділяються частина інфраструктури, віртуальні та фізичні ресурси. Це дозволяє розглядати архітектуру КД як самостійний об'єкт, хоч він і є частиною всього обчислювального комплексу, але зі своїми завданнями конфігурування та проектування. Системи КД розвиватися можуть окремо власне від технологій, що забезпечать надання ОС, можуть доповнювати реалізацію нових концепцій КД, оновлюватись та змінювати апаратне, програмне забезпечення, не змінюючи основних функціональних можливостей ОС. Водночас КД не можна розглядати поза контекстом всього обчислювального комплексу — системні зв'язки між усім ним та підсистемою КД мають бути враховані на рівні техніко-економічних характеристик та функціональних можливостей, що реалізуються ОС у цифровому середовищі.

Отже, можна визначити загальну концепцію створення архітектури системи КД так: її розроблення є окремою, самостійною інженерною задачею, яка не залежить безпосередньо від основних функцій чи методів, що застосовуються в базовому обчислювальному комплексі, який представляє інформаційну систему у цифровому середовищі. Інакше кажучи, хоча система КД інтегрована в обчислювальний комплекс, що забезпечує надання основних сервісів, вона виконує власний набір функцій. Вона отримує дані про доступ від тих самих користувачів і пристроїв, працює через ті ж канали передачі й задіює ті самі обчислювальні ресурси, однак використовує їх для збору, передачі, аналізу та зберігання саме інформації про події доступу, яка не належить до основної діяльності із надання сервісів системи.

Перехід до нових технологій обробки даних або оновлення інфраструктури не змінюють ключових функцій сервісів у цифровому середовищі, однак система КД при цьому повинна відповідати визначеним

технічним та економічним вимогам. Такий підхід дозволяє розглядати розроблення архітектури КД як одну з критично важливих задач у сфері побудови обчислювальних комплексів, інформаційних систем і комп'ютерних мереж.

Завдання формування архітектури КД можна визначити як проектування автономної підсистеми всередині обчислювального комплексу, яка має чітко окреслені функції — збір, передавання, зберігання та обробка даних про дії користувачів. Її методи роботи, набори ресурсів та технологічні підходи мають бути незалежними від тих, що застосовуються для функціонування основних сервісів системи, але вимагають власних обчислювальних ресурсів у складі обчислювального комплексу, причому потрібно дотримуватися техніко-економічних вимог.

Запропонований підхід дозволяє сформулювати ряд завдань, які являються типовими для класу об'єктів, що розглядається: визначити систему збору даних, сформувати віртуальну інфраструктуру для обробки даних КД, визначити склад і техніко-економічні вимоги до обчислювальних ресурсів, необхідних для вирішення завдань КД, визначити склад та необхідні ресурси для компонентів аналізу даних КД.

Аналіз технічних вимог і робочих умов дає змогу окреслити узагальнену модель підсистеми контролю доступу (КД). Її апаратна частина охоплює віртуальні машини, сервери, систему зберігання даних, а також мережеве обладнання, що забезпечує підключення клієнтів до основних сервісів (ОС). Програмні компоненти, інтегровані в інформаційну інфраструктуру сервісів, засоби управління доступом і модулі обробки даних, реалізують такі ключові функції: реєстрацію подій доступу користувачів, передавання та збереження отриманих даних; формування правил і прогнозування (оцінювання можливих значень) поведінкових маркерів користувачів відповідно до встановлених політик захищеного доступу; зіставлення фактичних показників із заданими персоналізованими шаблонами. Схематичний приклад реалізації КД для ОС представлено на рисунку 3.1.

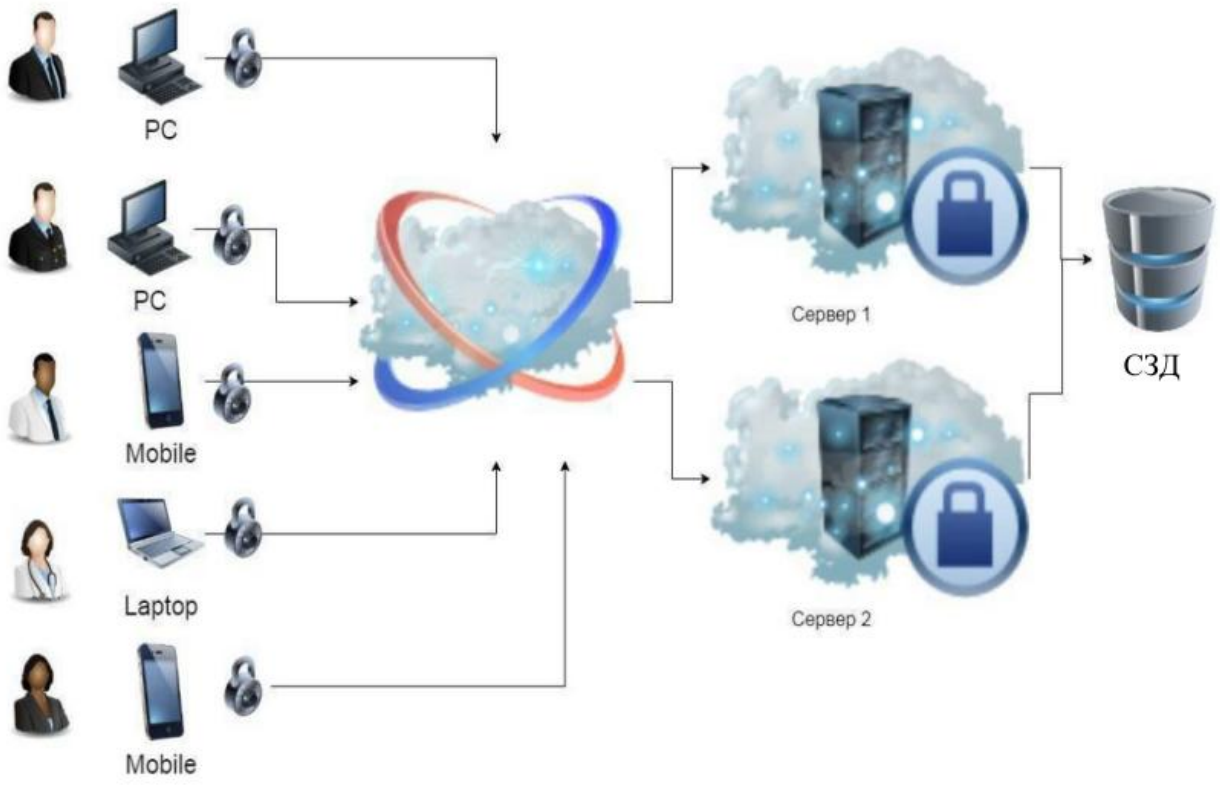

Рисунок 3.1 — Приклад захищеного обчислювального комплексу для доступу до сервісів

У продемонстрованій на рисунку 3.1 структурі сервери разом із системою зберігання даних (СЗД) інтегровані в єдину мережеву інфраструктуру. Кожен із серверів може забезпечувати клієнтам одну або декілька послуг — наприклад фінансові, банківські, державні, освітні, ігрові, служби бронювання, сервіси передавання потокових даних, пошукові системи тощо. Крім цього, кожен сервер оснащено модулем безпеки та диспетчером подій. Диспетчер подій відповідає за моніторинг, фіксацію та агрегування всіх релевантних відомостей про події, що виникають під час надання обчислювальних послуг. Зібрані дані є основою для виявлення нетипових ситуацій та своєчасного реагування на потенційні загрози.

Обчислювальна система представляє собою об'єднання взаємопов'язаних комп'ютерів, засобів обробки інформації та додаткового обладнання. Для роботи з мережевими даними така система використовує комунікаційну інфраструктуру, яка забезпечує передачу інформації між усіма

складовими елементами. Ця інфраструктура може базуватися на різних типах з'єднань: дротових кабельних лініях, технологіях бездротової передачі даних або волоконно-оптичних каналах зв'язку.

У випадку, коли модуль моніторингу подій ідентифікує ознаки можливого порушення безпеки, система автоматично створює сповіщення про інцидент. Це сповіщення формується на підставі проведеного аналізу та містить інструкції для інших компонентів системи захисту, спрямовані на блокування підозрілої діяльності, пов'язаної з певною операційною службою.

Модуль моніторингу подій працює на основі алгоритмів статистичного зіставлення, які дозволяють виявляти закономірності та взаємозв'язки між різними записами в журналах безпеки. Крім того, цей модуль може містити додаткові функціональні блоки для аналізу дій користувачів та адміністративного керування системою.

Сервера можуть відправляти інциденти безпеки на хмарні ресурси для подальшого аналізу додатком когнітивного машинного навчання на основі ідентифікованих характеристик інцидентів безпеки, виявлених під час локального аналізу за допомогою інформації безпеки та диспетчера подій. Ідентифікованими характеристиками можуть бути: подія, що спостерігається, пов'язана з інцидентом безпеки; подія, що спостерігається, має оцінку ризику безпеки, вищу граничного значення; подія, що спостерігається, визначається антивірусами як шкідливе ПЗ.

Диспетчер подій ідентифікує ризики та загрози безпеці, наприклад, несанкціоновані доступи до серверів та СЗД. База інцидентів безпеки повинна містити інциденти неправомірного використання конфіденційною інформацією, що зберігається на серверах обчислювальних комплексів. Це може бути конфіденційна інформація, така як номери кредитних карток, номери банківських рахунків, фінансові записи, медичні записи — будь-яка інформація, що включає конфіденційні або персональні дані. Для доступу до веб-служб через публічні мережі користувачі можуть застосовувати різноманітні клієнтські пристрої: стаціонарні та ноутбуки, планшети, мобільні

телефони, смарт-годинники, телевізори з функцією Smart TV, ігрові консолі та інше обладнання. При цьому власник такого пристрою може здійснювати шкідливі дії стосовно серверних служб як ненавмисно (через помилку), так і цілеспрямовано (зі зловмисним наміром).

СЗД являє собою мережеве сховище інформації, призначене для роботи з різнотипними даними незалежно від їх структурування. Зокрема, така система може містити один або декілька репозиторіїв інцидентів інформаційної безпеки з детальною інформацією про кожен випадок, включаючи характеристики джерел загроз, оцінки їх критичності та інші параметри. Також СЗД призначена для зберігання різноманітної службової інформації, зокрема даних для ідентифікації користувачів: логінів, паролів, біометричних параметрів адміністраторів системи та фахівців з інформаційної безпеки.

Структура мережевої обчислювальної платформи може бути розширена довільною кількістю додаткових серверних вузлів, клієнтських терміналів, накопичувачів інформації та іншого обладнання. Програмне забезпечення, що функціонує в такій системі, може передаватися на комп'ютери чи інші обчислювальні пристрої для роботи під керуванням операційної системи. Зокрема, програмний код може зберігатися на серверному вузлі та передаватися клієнтському пристрою через мережу для виконання у веб-браузері користувача.

3.2 Розробка чотирирівневої архітектури системи контролю доступу

На рисунку 3.2 зображено рівні системи КД до даних обчислювального комплексу, що надає ОС по мережах.

Програмно-апаратний рівень обчислювального комплексу включає: апаратні компоненти (у т. ч.: мейнфрейми, сервери, блейд-сервери, пристрої зберігання, мережеві компоненти); системне та програмне забезпечення обчислювального комплексу, а також програмно-апаратне забезпечення

клієнтського додатку та веб-сервіси, доступні через браузери клієнтських пристроїв.

Рисунок 3.2 — Чотирьохрівнева архітектура системи КД, яка перебачає масштабування

Рівень віртуальної обчислювальної інфраструктури забезпечує взаємодію віртуальних серверів, віртуальної пам'яті, віртуальних мереж, віртуальних додатків та операційних систем, віртуальних клієнтів; управління мережевою взаємодією клієнтських запитів з ОК.

Рівень фізичних ресурсів включає: розподіл обчислювальних ресурсів ОК, які використовуються для виконання завдань КД в хмарному середовищі; спеціалізоване ПЗ; доступ до середовища користувачів та системних адміністраторів; а також управління системою зберігання даних.

Рівень компонентів аналізу даних КД включає конкретне програмно-математичне забезпечення, яке реалізує обробку та аналіз даних, аналіз інцидентів безпеки. Розроблена архітектура дозволяє замінювати або розширювати елементи на кожному із виділених ресурсів без зміни загальної структури, тобто забезпечити масштабованість.

Кожен рівень може бути розглянутий окремо як комплекс задач. Кожному рівню відповідає свій набір технологій, компонентів, що може бути реалізовано окремими компонентами чи розробками окремих команд IT-фахівців та спеціалістів з обробки даних.

Кожному рівню архітектури відповідають етапи розробки системи КД:

1) визначення складу параметрів, які можуть бути отримані про діяї користувачів, способи їх збору та передачі;

2) формування віртуальної обчислювальної інфраструктури, необхідної на вирішення завдань обробки інформації КД;

3) оцінка параметрів обчислювальних ресурсів;

4) розробка компонент аналізу інформації.

Запропонована архітектура дозволяє замінювати або розширювати елементи на кожному із виділених ресурсів без зміни загальної структури і визначає етапи завдань з розробки та впровадження, тим самим забезпечуючи масштабованість та технологічний розвиток системи.

3.3 Розробка апаратного рівня архітектури системи контролю доступу

На рисунку 3.3 зображено архітектуру серверної системи обробки даних (1 рівень архітектури). Система надає доступ клієнтним пристроям до даних та послуг через веб-сервіси. Система обробки даних включає структуру

зв'язку, яка забезпечує зв'язок між процесорним блоком, пам'яттю, постійним сховищем, блоком комунікаційного обладнання.

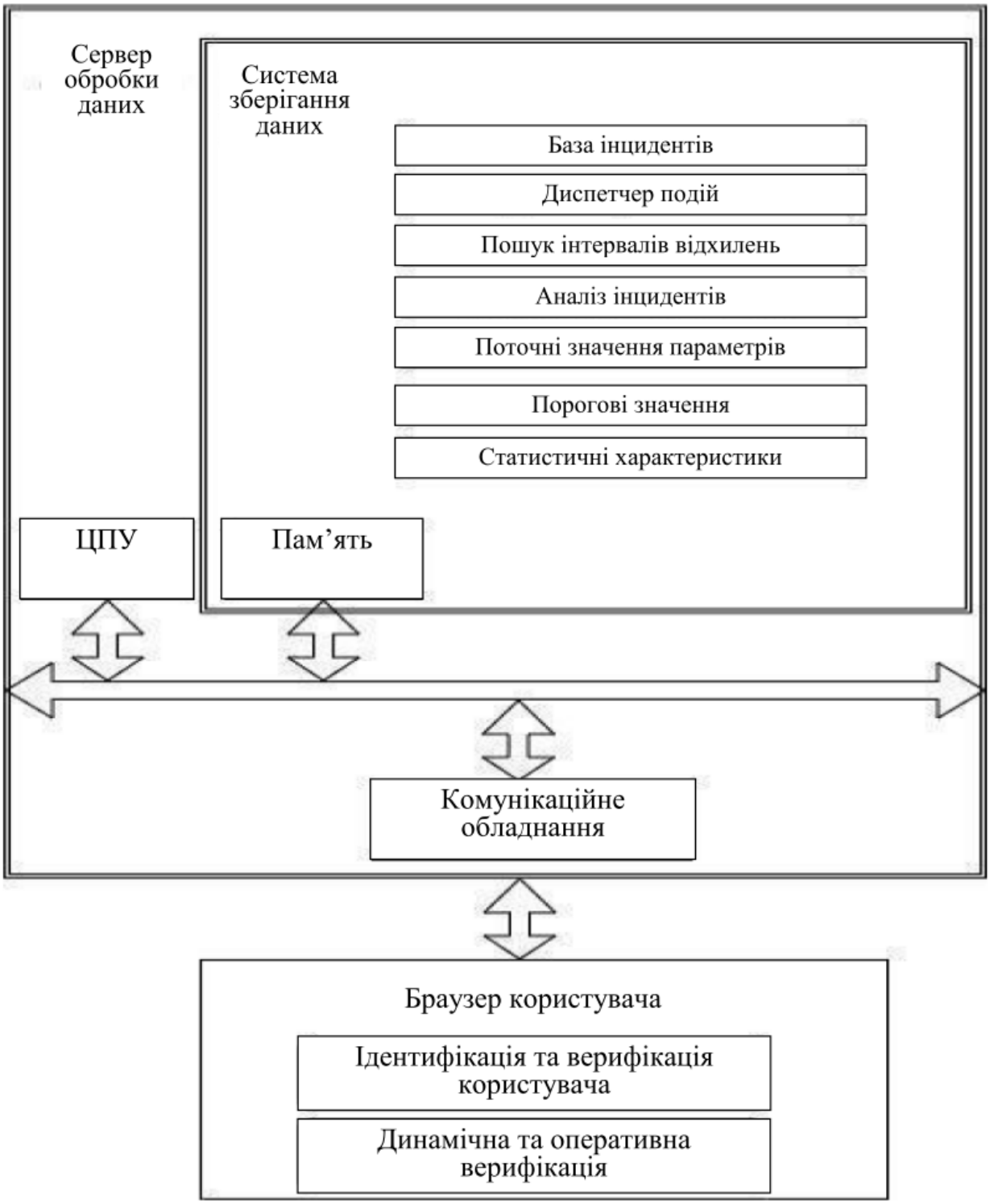

Рисунок 3.3 - Апаратний рівень КД

У системах зберігання даних, що являють собою сукупність серверного обладнання та СЗД, містяться компоненти, що реалізують КД до обчислювального комплексу. У систему КД включені такі компоненти:

- база інцидентів, що містить інформацію про можливі варіанти поведінки системи та/або користувача при несанкціонованому доступі, або загрозам цілісності даних, або компонентам обчислювального комплексу;

- диспетчер подій — може бути окремим апаратним або програмно-апаратним модулем, що відповідає за фіксування подій безпеки та КД через мережі;

- аналізатор інцидентів — програмний модуль, що забезпечує оперативний КД на основі аналізу подій;

- модуль порівняння отриманих значень параметрів доступу та характеристик подій із заданими моделями чи пороговими значеннями;

- поточні значення параметрів, що характеризують контроль доступу користувачів, збирання статистичних даних;

- порогові значення - база значень, що характеризують події, при яких слід забезпечувати програмні або апаратні сценарії захисту, блокування користувача, повторної верифікації тощо, а також можливі варіанти перерахунку порогових значень;

- статистичні характеристики — модуль, що зберігає та обчислює значення статистичних параметрів конкретних користувачів, груп користувачів та інших параметрів, які виконуються при аналізі інцидентів.

3.4 Опис тестового стенда з багаторівневим контролем доступу

На рисунку 3.4 проілюстрована можлива схема розгортання стенда з багаторівневим КД. Веб-сервер websrv розгорнутий як необхідний для роботи аналітичного кластера компонент, що захищається. Відмовостійкість компонента журналу пояснюється наявністю первинного і вторинного примірників rsyslog.

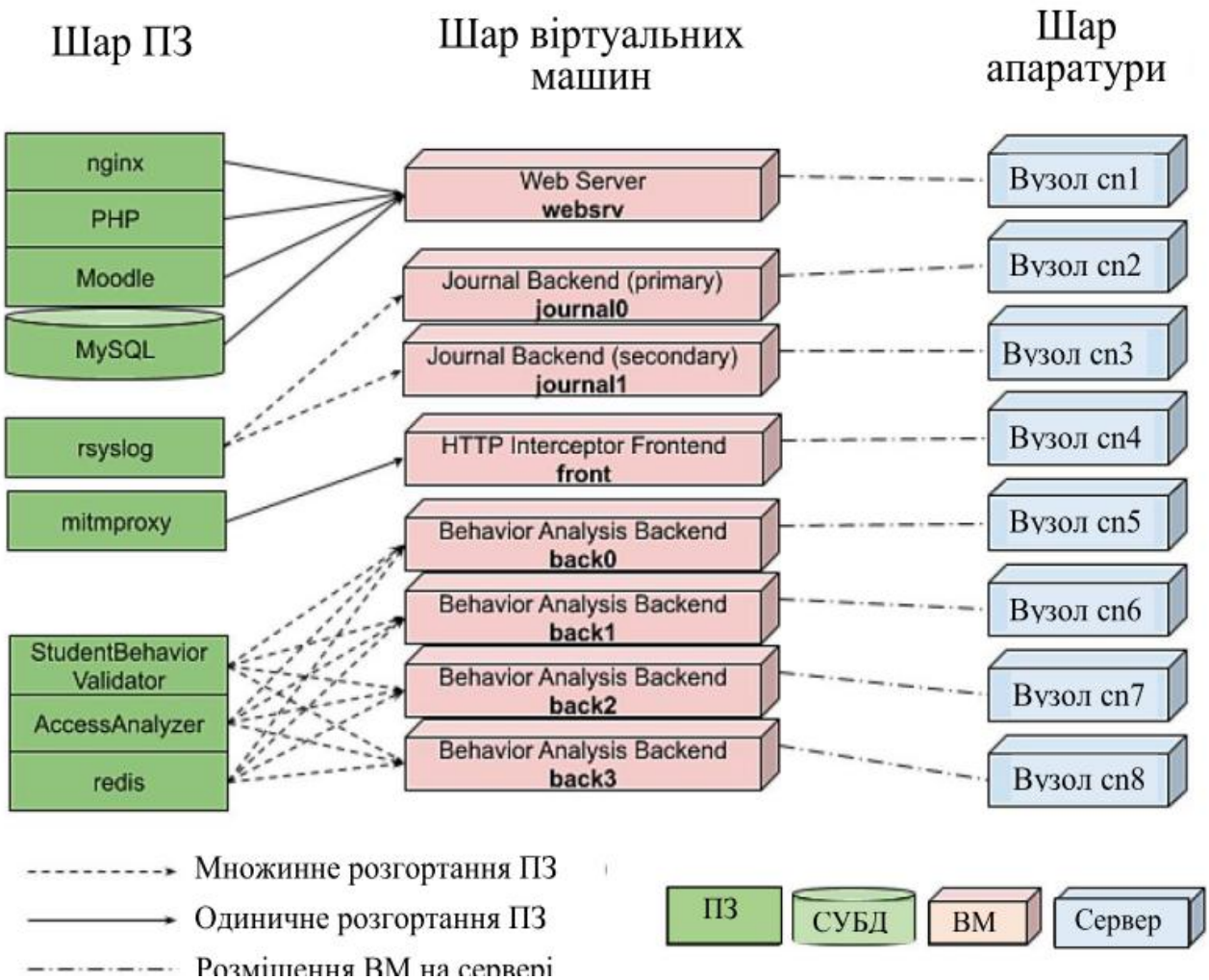

Рисунок 3.4 - Розміщення віртуальних машин та програмного забезпечення

Конфігурація така, що при пошкодженні первинного екземпляру дані прямують на вторинний. Після ремонту первинний екземпляр знову приймає дані. Відмовостійкість кластера Behavior Analysis Backend пояснюється множинністю екземплярів аналітичних компонентів AccessAnalyzer і StudentBehaviorValidator, а також розподіленого відмовостійкого сховища redis, що реалізує зберігання розподілених структур даних.

Експериментальні дослідження проводилося під таким навантаженням: на вхід елемента front подавалися HTTP-запити із випадковим інтервалом від 0 до 100 мс (ГПВЧ працює згідно з рівномірним розподілом). Повна кількість запитів - 1200. Використовуються два типи запитів:

1) «легковаговий», що вимагає меншої кількості обчислювальних ресурсів для обробки, і що індукує передачу даних по мережі в обох їх

напрямках до 1 Мбіт. Прикладом такого запиту є виставлення оцінки за студентську роботу;

2) «важковаговий», що вимагає більшої кількості обчислювальних ресурсів для обробки, що індукує передачу даних через мережу у вихідному напрямку до 15 Мбіт. Передача даних по мережі у вхідному напрямі потрібна тільки для передачі запиту і не перевищує 1 Мбіт. Прикладом такого запиту є відкриття журналу оцінок для потоків, що включають багато груп студентів.

На 9 «легковагових» запитів припадає 1 «важковаговитий». Повний час роботи для обслуговування усіх прийнятих запитів - 61 с.

На рисунку 3.5 наведено графіки для споживання ресурсів кожної віртуальної машини.

Есперимантальне тестування показало таке. Наявність асиметричного навантаження на мережевий інтерфейс машини websrv через наявність «важковагових» запитів, відповіді на які навантажують вихідний канал.

Машина front значно більш навантажена за процесором, ніж по інших ресурсах. Це пояснюється тим, що на проксування трафіку HTTP витрачається у помітному обсязі процесорний час сервісом mitmproxy, в той час, як HTTP-запити та відповіді на них не такі великі, щоб утилізувати мережевий канал навіть на 10%.

Зауважимо, що навантаження на її вхідний канал включає як запити, адресовані websrv, так і відповіді на них, що виходять від websrv, що обумовлено виконуваним на машині front проксіюванням HTTP-трафіку. Прийнятий HTTP-запит направляється також на аналітичні машини Behavior Analysis Backend. На них виробляються операції аналізу користувальницької поведінки, але не при надходженні кожного окремого запиту, а при накопиченні 50 непроаналізованих запитів, які формують статистику, доступну для аналізу. При цьому кожен поступаючий запит веде до запису активності користувача в журналі на машині journal0 (journal1 перебуває в резерві та не навантажений).

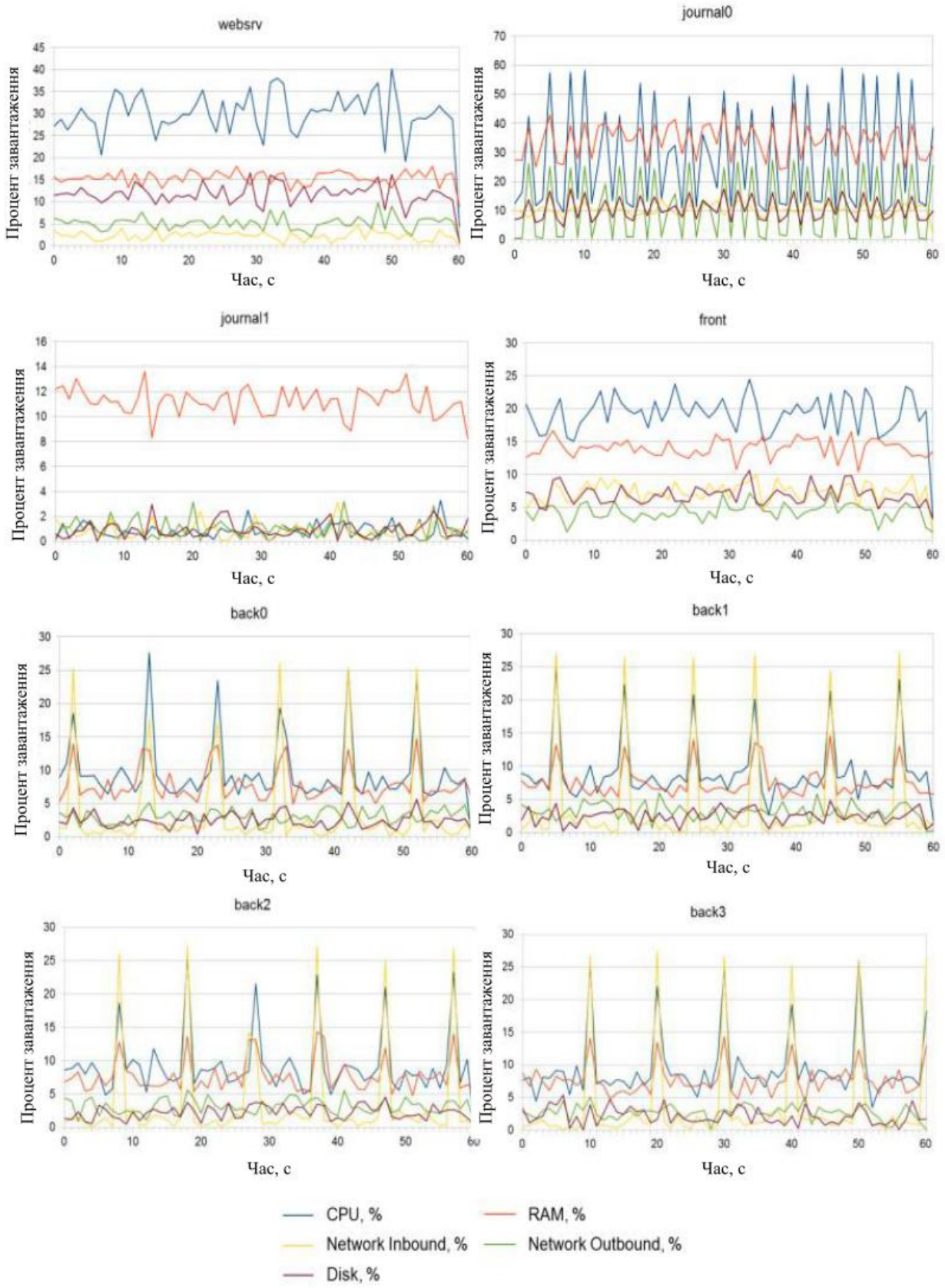

Рисунок 3.5 - Споживання ресурсів віртуальними машинами

Сплески активності на машині journal0 обумовлені запуском аналітичних процедур на машинах back0, …, back3, які роблять читання непроаналізованих подій активності користувача з журналу. Вхідний мережевий канал має більш рівномірне навантаження, ніж вихідний, оскільки обслуговує однорідні запити на запис подій, а не обслуговує масивні, але поодинокі запити читання. Робота аналітичних процедур на машинах back0, …, back3 помітна з піків навантаження на процесор, пам'ять та вхідний мережевий канал. Кількість піків активності журналу відповідає загальній кількості піків активності на аналітичних машинах, оскільки навантаження на них балансується за алгоритмом round-robin. Графік на рисунку 3.6 показує завантаження аналітичних процесорів машин.

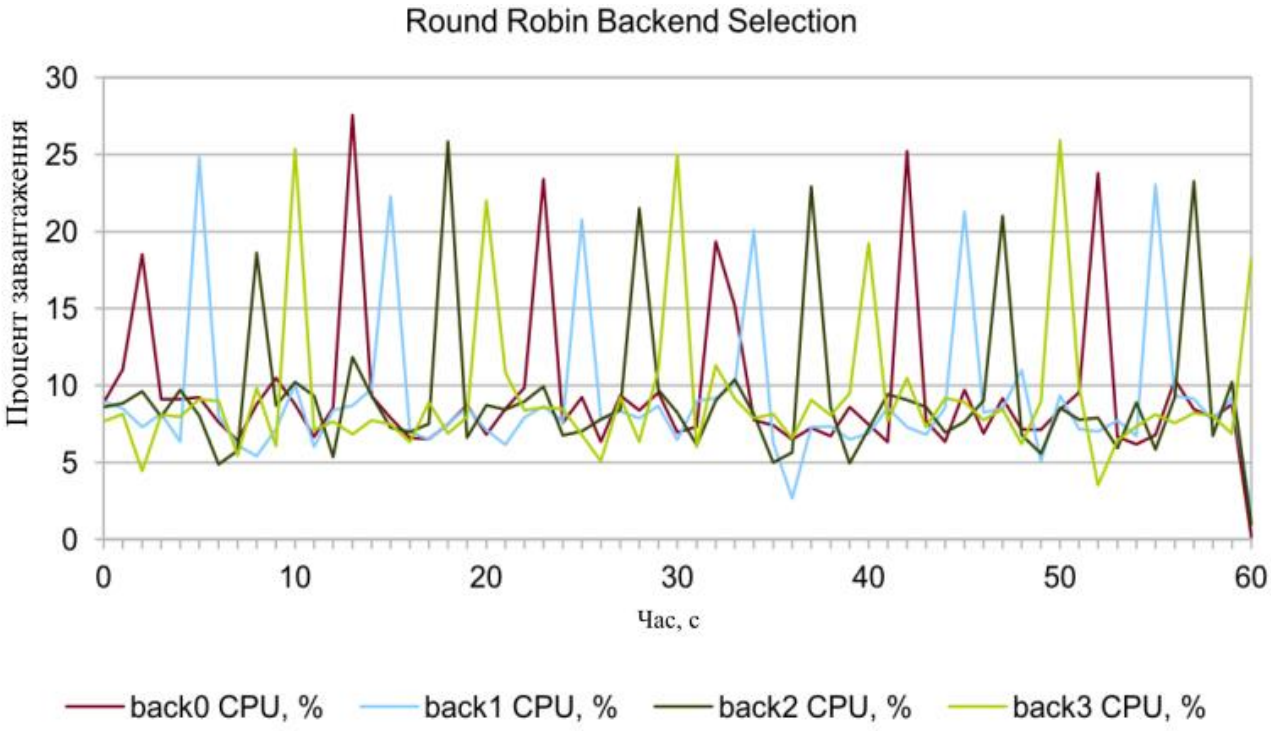

Рисунок 3.6 - Споживання ресурсів процесора аналітичними віртуальними машинами

В таблиці 3.1 наведено середнє завантаження ресурсів на вісьмох віртуальних машинах.

Таблиця 3.1 - Середнє завантаження ресурсів на віртуальних машинах

ВМ	Середнє навантаження CPU, %	Середнє навантаження RAM, %	Середнє навантаження мережі, вхідний канал, %	Середнє навантаження мережі, вихідний канал, %	Середнє навантаження диску, %
websrv	29,83	15,43	2,25	5,18	11,62
journal0	28,03	33,95	10,22	10,56	10,53
journal1	0,86	11,19	0,85	1,00	0,94
front	19,15	14,03	7,30	4,34	6,86
back0	9,50	7,80	3,59	3,03	2,41
back1	9,04	7,58	3,66	3,16	2,46
back2	9,24	7,71	3,50	3,16	2,23
back3	9,34	7,68	3,63	2,69	2,14

З даних, наведених у таблиці 3.1, можна констатувати, що тестовий аналітичний кластер має значний потенціал для оптимізації через скорочення обсягу оперативної пам'яті, яка виділяється віртуальним машинам. Завантаженість процесорів знаходиться на помірному рівні, при цьому зберігається достатній резерв обчислювальної потужності для опрацювання раптових збільшень кількості вхідних запитів. Якщо ж додавати нові аналітичні плагіни у майбутньому, потребу в ресурсах віртуальних машин потрібно заново оцінити з використанням експериментальних імітаційних стендів.

Практичний ефект розробки та впровадження подібного програмного забезпечення полягає в забезпеченні справжності користувачів, об'єктивності оцінювання, а також захищеності професійної репутації фахівців зокрема та установи загалом.

Оскільки на даний час немає жодних конкретних вимог до плагінів, за винятком реалізації одного загального інтерфейсу, який повинен забезпечувати управління моделлю коректності, тому і відсутні певні технічні складності під час реалізації модельно-орієнтованих підходів для перевірки

даних, що дозволяє програмістам розширювати запропоновану систему за допомогою нових сучасних аналізаторів, коли з'являються нові ефективні методи.

Програмна реалізація описаних архітектур може бути основою фреймворку, який призначений для збору і аналізу даних користувацької поведінки щодо їх справжності. Наявність подібного інструментарію допоможе дослідникам, що працюють у вказаному напрямі, спростити збір даних і експериментальні дослідження для моделей машинного навчання.

Запропонована архітектура системи контролю доступу готова до обробки достатньо великих даних при перевірці коректності поведінки користувача. Умова відмовостійкості - це наявність кластеризованих екземплярів компонентів, які будуть розгорнуті на різних машинах з наявністю чи відсутністю рівня контейнеризації чи віртуалізації. Перспективним напрямком розвитку для аналітичних компонентів є використання сучасних підходів щодо розпаралелювання програм та інструментів для обробки великих даних, а також методів штучного інтелекту.

ВИСНОВКИ

1. Здійснено аналіз системних факторів впливу на процес контролю доступу, що дозволило визначити сучасні тенденції та перспективи розвитку технологій контролю доступу.

2. На основі формування політик захищеності доступу до обчислювальних комплексів розроблено концепцію побудови моделі системи контролю доступу до інформаційних ресурсів.

3. На основі формування вимог та умов для проектування архітектури контролю доступу розроблено чотирирівневу архітектуру для моделі системи контролю доступу.

4. Розроблено модель багаторівневої системи контролю доступу, наведено опис тестового стенда з багаторівневим контролем доступу, що дозволило верифікувати отримані теоретичні результати.

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. К.: ДУТ, 2015. 288 с.
2. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці. К. : НІСД, 2016. 528 с.
3. Волокітін А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. Інформаційна безпека державних організацій і комерційних фірм. К.: Юніор, 2012. 303 с.
4. Максимчук М.А. Модуль аналітичної обробки даних програмних засобів підтримки процесу оптимізації покриття оператора мобільного зв’язку. Інженерія програмного забезпечення. 2011. №2(6). С.106-110.
5. Дузь-Крятченко О. П., Грицай П. М., Грищенко В. П., Клименко В. С. та ін. Основи стратегії національної безпеки та оборони держави: підруч. К. : НУОУ ім. Івана Черняховського, 2015. – 620 с.
6. Козловський А.В., Паночишин Ю.М., Погрішук Б.В. Комп'ютерна техніка та інформаційні технології: навч. посіб. К.: Знання, 2014. 463с.
7. Антонюк А.О., Жора В.В. Теоретичні основи моделювання та аналізу систем захисту інформації: [монографія] / Ірпінь Національний університет ДПС України, 2010. 310 с.
8. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.
9. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. К.: ДУТ, 2015. 449 с.
10. Пількевич І.А., Лобанчикова Н.М.,. Молодецька К.В. Захист інформації в автоматизованих системах управління: посібник. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

11. Cai F., He J., Ali Zardari Z., Han S. Distributed management of permission for access control model // Journal of Intelligent & Fuzzy Systems. 2020. Vol. 38. No. 2. P. 1539–1548.

12. Yarmand M. H., Sartipi K., Down D. G. Behavior-based access control for distributed healthcare systems // Journal of Computer Security. 2013. Vol. 21. No. 1. P. 1–39. 280

13. Walker A., Svacina J., Simmons J., Cerny T. On automated role-based access control assessment in enterprise systems. In Information Science and Applications. — Springer, Singapore, 2020, pp. 375–385.

14. Nyame G., Qin Z. Precursors of role-based access control design in KMS: A conceptual framework // Information. 2020. Vol. 11. No. 6. P. 334.

15. Trnka M., Cerný T. On security level usage in context-aware role-based access control. In Proceedings of the SAC, Symposium on Applied Computing. Pisa, Italy, 4–8 April 2016, pp. 1192–1195.

16. Степанюк О.В., Залізняк В.В., Касянчук М.М. Архітектура обчислювального комплексу з багаторівневим контролем доступу. Збірник матеріалів науково-практичного симпозіуму «Захист інформації’2025». Тернопіль, 2025. С.99-101.

17. Степанюк О.В., Прончук Д.С. Сучасні перспективи автоматизованих систем контролю доступу. Збірник матеріалів науково-практичного симпозіуму «Технології Інтернету речей: системи та рішення» (TIP:CT-2025). Тернопіль, 2022. С.31-33.

18. Elshoush H. T., Osman I. M. Alert correlation in collaborative intelligent intrusion detection systems — a survey // Applied Soft Computing. 2011. P. 4349–4365.

19. Xi X., Zhang T., Ye W., Wen Z., Zhang S., Du D., Gao Q. An ensemble approach for detecting anomalous user behaviors // International Journal of Software Engineering and Knowledge Engineering. 2018. Vol. 28. P. 1637–1656.

20. Lee J., Kim J., Kim I., Han K. Cyber threat detection based on artificial neural networks using event profiles // IEEE Access. 2019. Vol. 7. P. 165607–165626.

21. Csaba K., Péter H. B. Analysis of cyberattack patterns by user behavior analytics // AARMS – Academic and Applied Research in Military Science. 2018. Vol. 17. No. 3. P. 101–114.

22. Kufel L. Security event monitoring in a distributed systems environment // IEEE Secur. Priv. 2013. Vol. 11. Iss. 1. P. 36–43. 281

23. Sancho J. C., Caro A., Ávila M., Bravo A. New approach for threat classification and security risk estimations based on security event management // Future Generation Computer Systems. 2020. Vol. 113. P. 488–505.

24. Schefer-Wenzl S., Strembeck M. Modelling context-aware RBAC models for mobile business processes // International Journal of Wireless and Mobile Computing. 2013. Vol. 6. No. 5. P. 448–462.

25. Security QRadar SIEM. [Электронный ресурс]. URL: http://www.siem.su/docs/ibm/IBM_Security_QRadar.pdf

26. Sekharan S. S., Kandasamy K. Profiling SIEM tools and correlation engines for security analytics. In Proceedings of 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). IEEE, 2017, pp. 717–721.

27. Symantec Security Information Manager (SSIM). [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Symantec_Security_Information_Manager

28. El Arass M., Souissi N. Smart SIEM: From big data logs and events to smart data alerts // Int. J. Innov. Technol. Explor. Eng. 2019. Vol. 8. Iss. 8. P. 3186–3191.

29. Coppolino L. et al. Enhancing SIEM technology to protect critical infrastructures. In Proceedings of the International Workshop on Critical Information Infrastructures Security, 2013, pp. 10–21.

30. Hasan M., Sugla B., Viswanathan R. A conceptual framework for network management event correlation and filtering systems. In Proceedings of the Sixth IFIP/IEEE International Symposium on Integrated Network Management. 1999, pp. 233–246.

31. Moukafih N., Orhanou G., El Hajji S. Neural network-based voting system with high capacity and low computation for intrusion detection in SIEM/IDS systems // Security and Communication Networks. 2020. P. 3512737.

32. Kayes A. S. M., Kalaria R., Sarker I. H., Islam M., et al. A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues // Sensors. 2020. Vol. 20. No. 9. P. 2464.




ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ
ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
"ЗАХИСТ'ІНФОРМАЦІЇ'2025"

28 листопада 2025
Тернопіль

ПЕРЕРВА Дмитро…… **62**
УДОСКОНАЛЕНІ ПІДХОДИ ДО ЗМЕНШЕННЯ ВИТОКУ МЕТАДАНИХ У СИСТЕМАХ БЕЗПЕЧНОГО ОБМІНУ ПОВІДОМЛЕННЯМИ

ПЕЧЕНЮК Максим, ЦАВОЛИК Тарас…… **65**
БАГАТОРІВНЕВІ АРХІТЕКТУРИ БЕЗПЕКИ IOT: ПОРІВНЯЛЬНИЙ АНАЛІЗ ФРЕЙМВОРКІВ NIST, ISO/IEC 27400 ТА OWASP

ПИТЕЛЬ Роман, СЕГЕДА Євген…… **71**
АЛГОРИТМ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА КІНЦЕВИХ ВУЗЛАХ МЕРЕЖІ

ПІДГУРСЬКИЙ Д.В…… **75**
ІНТЕЛЕКТУАЛЬНІ МЕТОДИ КЛАСИФІКАЦІЇ ДЕФЕКТІВ ВІТРОВИХ ТУРБІН ТА ЗАХИСТУ КАНАЛІВ ПЕРЕДАЧІ ДІАГНОСТИЧНИХ ДАНИХ

ПІДЛИСЬКИЙ Дмитро, ДАВЛЕТОВА Аліна…… **79**
ПЛАТФОРМА МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА БАЗІ KIBANA

ПОМАЗИБІДА Василь, НЕТРЕБЯК Микола…… **83**
АНАЛІЗ РОЗВИТКУ ХМАРНИХ ОБЧИСЛЕНЬ ТА ПРОБЛЕМИ ЇХ БЕЗПЕКИ

РУЩАК Владислав…… **86**
ПОРІВНЯННЯ FLOW ТА TYPESCRIPT В JAVASCRIPT

САРАПУК О.І., ЧЕРНЯК В.А.…… **91**
СТРУКТУРА МЕРЕЖІ КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ ЗА ВЕРСІЄЮ ETSI

СОКОЛІК Максим, КУЛИНА Сергій…… **94**
АНАЛІЗ СУЧАСНИХ АЛГОРИТМІВ ВИДІЛЕННЯ ОЗНАК В БІОМЕТРІЇ

ЛУКАШ Остап…… **97**
ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ ДЛЯ АУДИТУ БЕЗПЕКИ БЛОКЧЕЙН-СИСТЕМ

СТЕПАНЮК О.В., ЗАЛІЗНЯК В.В., КАСЯНЧУК М.М…… **99**
АРХІТЕКТУРА ОБЧИСЛЮВАЛЬНОГО КОМПЛЕКСУ З БАГАТОРІВНЕВИМ КОНТРОЛЕМ ДОСТУПУ

ХМЕЛИК Вадим…… **102**
ДОСЛІДЖЕННЯ АРХІТЕКТУРИ ОПЕРАЦІЙНОГО ЦЕНТРУ БЕЗПЕКИ

ЧУХНІЙ Максим, ВЕЛЕЩУК Андрій…… **106**
СУЧАСНІ ЗАГРОЗИ БЕЗПЕКИ ВЕБ–ДОДАТКІВ

УДК 004.056

Степанюк О.В., Залізняк В.В., Касянчук М.М.

Західноукраїнський національний університет

АРХІТЕКТУРА ОБЧИСЛЮВАЛЬНОГО КОМПЛЕКСУ З БАГАТОРІВНЕВИМ КОНТРОЛЕМ ДОСТУПУ

Вступ. Актуальність розробки архітектури обчислювального комплексу з багаторівневим контролем доступу (КД) зумовлена зростаючими вимогами до захисту інформації в умовах інтенсивної цифровізації та переходу до розподілених обчислювальних середовищ [1]. Поява нових кіберзагроз вимагає впровадження гнучких та стійких архітектур, здатних запобігати несанкціонованому доступу навіть у разі часткового порушення безпеки. Багаторівневий КД дозволяє розмежовувати права на різних рівнях, що суттєво зменшує ризики внутрішніх і зовнішніх порушень [2]. Таким чином, дослідження та розробка архітектури обчислювального комплексу з багаторівневим КД є актуальною науковою та практичною задачею.

Мета. Метою даної роботи є розробка архітектури обчислювального комплексу з багаторівневим КД, що спрямована на підвищення стійкості інформаційних систем, мінімізацію ризиків порушення безпеки та забезпечення надійного функціонування критичних цифрових інфраструктур.

1. Архітектура обчислювального комплексу з багаторівневим контролем доступу

Стосовно систем обробки даних проблема КД зводиться, перш за все, до КД до різних інформаційних систем: операційної системи, баз даних, системи електронного документообігу тощо, до технічних засобів обробки даних та інших об'єктів. В останні десятиліття ця проблема ще більше загострилася в зв'язку з інтенсивним розвитком інтернету, що призвело до появи великої кількості нових видів загроз – мережевих. Ці види загроз виявилися істотно більш небезпечними, що породило великий сплеск у розвитку різних засобів і механізмів мережевого захисту комп'ютерних систем. Політична громадськість багатьох країн гостро ставить питання про забезпечення повного державного контролю над мережевими трафіками національного рівня, розроблення своїх програмно–апаратних засобів обробки даних.

Таким чином, об'єктами доступу, що становлять інтерес для зловмисних дій, є інформаційні системи об'єкта захисту, технічні засоби обробки даних, а також безпосередньо процеси обробки даних. Сучасна система доступу до обчислювальних систем включає велику кількість засобів контролю, ідентифікації та верифікації користувачів (рисунок 1).

Вимоги до забезпечення КД та умови функціонування можуть бути сформульовані наступним чином. Обчислювальний комплекс із системою захищеного КД по комп'ютерних мережах забезпечує можливість доступу з будь–якого пристрою, який використовує користувач.

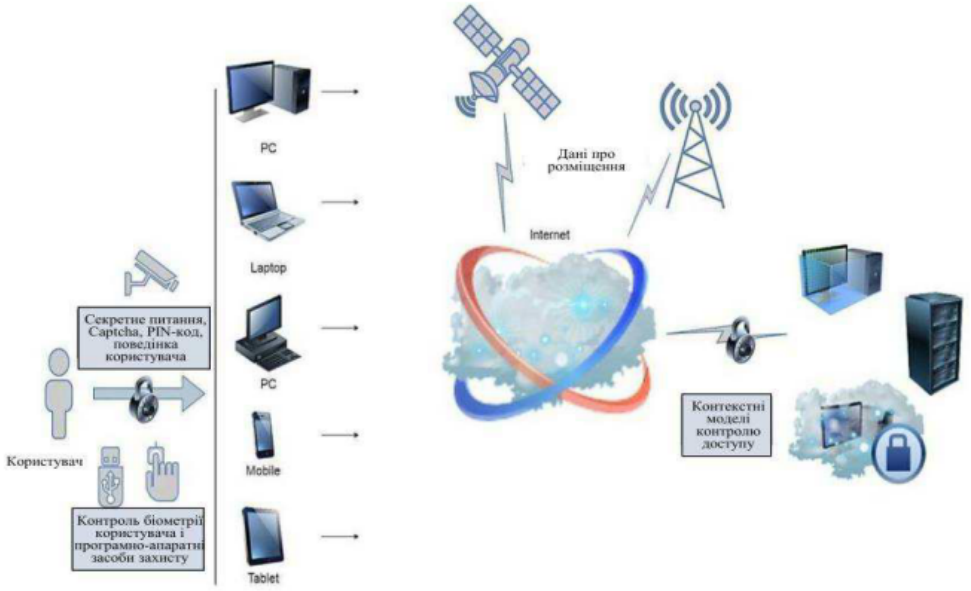

Рисунок 1 – Архітектура обчислювального комплексу з багаторівневим КД

При цьому відбувається ідентифікація користувача з використанням різних засобів біометрії (наприклад, відбиток пальця, вбудовані або зовнішні камери), в процесі доступу використовуються програмні засоби верифікації (секретне питання, PIN–коди, Captcha). В даний час розвиваються системи, пов'язані з аналізом поведінки користувачів (наприклад, реакції користувачів на запитання доступу чи поведінкові моделі). Елементом КД є облік локації користувача, ці дані можуть бути порівняні з даними у профілі користувача. Для доступу до сервісів існує рівень КД, що забезпечується контекстними моделями. Такими моделями можуть бути політики, побудова моделей за журналами подій, відповідним групам користувачів, а також спеціалізовані методики, що належать до предметної області сервісу – медичні, банківські, освітні, які мають свої спеціалізовані протоколи та особливості доступу На рівні обчислювальних ресурсів – серверів, віртуальних машин, баз даних, здійснюється апаратний КД.

Таким чином, змістовно процес доступу до обчислювальної системи описується відношенням певної групи суб'єктів до заданої сукупності ресурсів, до яких ці суб'єкти хочуть мати доступ. Для опису, формалізації, аналізу або синтезу системи КД необхідно, перш за все, описати три основні його компоненти: суб'єктів, що беруть участь у системі КД; ресурси; об'єкти, які є предметом інтересів суб'єктів.

Зазначимо, що у процесі КД ставиться завдання забезпечення безпеки всіх необхідних властивостей (або, узагальнено усієї обчислювальної системи) даних обмеженого доступу.

Під суб'єктом розуміється не лише фізична чи юридична особа, яка бажає скористатися певним програмно–апаратним чи інформаційним ресурсом в інформаційній системі, а також інформаційні процеси, програмно–апаратні засоби, які можуть отримати доступ до обчислювальної системи. Таким чином, під суб'єктом розуміється будь–який об'єкт або процес, який може здійснити певну дію в інформаційній системі з використанням процесорних пристроїв

системи. Приклади суб'єктів програмно–апаратного типу: операційна система; антивірусні та мережеві засоби; інформаційні системи конкретного призначення (редактори, СУБД, системи електронного документообігу, системи для обслуговування бізнес–процесів, зокрема, 1С тощо).

Під об'єктом, що здійснює доступ, розуміються будь–які поіменовані елементи інформаційної системи, до яких може отримати доступ хоча б один з процесорних пристроїв: периферійне та мережеве обладнання; файли; носії інформації; зовнішні пристрої різного призначення. Більше того, одні об'єкти доступу можуть бути частиною інших об'єктів (якщо вони поіменовані та доступні для процесорів); наприклад, флешка та файли, записані на ній є об'єктами доступу, такими ж є база даних і окремі записи, що містяться в ній, міжмережевий екран та окремі його параметри, доступні для процесорів.

Доступ описує безпосередньо набір тих дій, які може здійснювати даний суб'єкт над цим об'єктом. Таким чином, доступ прив'язаний до пари «суб'єкт–об'єкт» і являє собою набір дозволених (санкціонованих) дій, які може вчиняти суб'єкт над об'єктом. Основними видами доступів є читання та запис даних. Багато інших видів дій з даними можуть з деяким ступенем умовності зведені до цих видів доступу. Наприклад, видалення файлу може розглядатися як запис порожніх даних у файл – у цьому випадку порожній файл ототожнюється з віддаленим файлом, що в цілому не завжди коректно. Далі, додавання даних у файл ототожнено із записом даних. Однак, якщо дані структуровані (наприклад, у базах даних), то подібне додавання вимагає попереднього формування структурного скелета нового запису, що вже не вкладається у схему просто запису даних у файл. Тому до перерахованих видів дій, які можуть входити в доступ, додаються також видалення об'єкта (файлу, пристрою з переліку тощо), додавання об'єкта (записи, пристрої), активації об'єкта (запуску програми, включення технічного пристрою), модифікація (заміна), блокування, контроль права власності (включаючи авторизацію, підтвердження авторства чи авторських прав). До складу можливих видів доступу можуть бути включені інші більш специфічні дії.

Процес формування та реалізації доступів для кожної пари «суб'єкт–об'єкт» із заданих переліків суб'єктів та об'єктів, а також порядок зміни цих доступів у процесі функціонування інформаційної системи становить основний зміст політики управління доступом.

Висновок. Розроблено архітектуру обчислювального комплексу з багаторівневим контролем доступу.

Перелік використаних джерел.

1. Gil–Garcia J.R., Flores–Zúñiga M.Á. Towards a comprehensive understanding of digital government success: Integrating implementation and adoption factors. Government Information Quarterly. 2020. Vol.37. No. 4. P. 101518.

2. Cai F., He J., Ali Zardari Z., Han S. Distributed management of permission for access control model. Journal of Intelligent & Fuzzy Systems. 2020. Vol. 38. No. 2. P. 1539–1548.

науково-практичний симпозіум

ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ:
СИСТЕМИ ТА РІШЕННЯ

2025

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
КАФЕДРА СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ
ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

науково-практичний симпозіум

ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ: СИСТЕМИ ТА РІШЕННЯ (ТІР:СТ – 2025)

24 жовтня 2025 року
м. Тернопіль

Збірник матеріалів науково-практичного симпозіуму «Технології Інтернету речей: системи та рішення» (TIP:CT - 2025), Тернопіль, 2025. -116 с.

До збірника увійшли тези доповідей, подані учасниками науково-практичного симпозіуму «Технології Інтернету речей: системи та рішення», який проводився 24 жовтня 2025 р. у ЗУНУ кафедрою спеціалізованих комп'ютерних систем спільно з ГО «Кібербезпека і автоматизація».

Адреса організаторів:
вул. Олени Теліги 8, м. Тернопіль 46003,
кафедра спеціалізованих комп'ютерних систем,
Західноукраїнський національний університет.
Контакти: conferenceakit@gmail.com.

ЗМІСТ

Максим ПЕЧЕНЮК, Тарас ЦАВОЛИК
ЕВОЛЮЦІЯ КРИПТОГРАФІЧНИХ МЕТОДІВ ТА СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ IoT 5

Аліна ДАВЛЕТОВА
ПРОЕКТУВАННЯ ЗАХИЩЕНИХ БАЗ ДАНИХ У РОЗПОДІЛЕНИХ IoT-СИСТЕМАХ 10

Сергій СОРОКА, Микола БЕРНАДСЬКИЙ, Оксана БУРЛАК
МОДЕЛЬНО-ОРІЄНТОВАНЕ КЕРУВАННЯ ТИПУ INTERNAL MODEL CONTROL В СИСТЕМАХ РЕГУЛЮВАННЯ ТЕМПЕРАТУРИ 14

Михайло КОБЕЛЯ
ДОСЛІДЖЕННЯ ТА ОПТИМІЗАЦІЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ВИСОКОТЕМПЕРАТУРНОЮ ТЕХНОЛОГІЧНОЮ УСТАНОВКОЮ 18

Віталій КЛІМ, Тарас ЦАВОЛИК
АРХІТЕКТУРА СИСТЕМИ БЕЗПЕКИ KUBERNETES 22

Світозар ВАСЕНКО, Степан ІВАСЬЄВ
ВІДСТЕЖЕННЯ ДІЙ КОРИСТУВАЧА НА ОСНОВІ РЕЄСТРУ WINDOWS 24

Володимир ДМИТРУСЬ, Ренат ДАВЛЕТОВ
АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ АВТОНОМНОЮ ЕНЕРГЕТИЧНОЮ УСТАНОВКОЮ 27

СТЕПАНЮК О.В., ПРОНЧУК Д.С.
СУЧАСНІ ПЕРСПЕКТИВИ АВТОМАТИЗОВАНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ 31

Олександр КУХАРУК
АВТОМАТИЗАЦІЯ ПРОЦЕСІВ АНАЛІЗУ ТА МОНІТОРИНГУ БЕЗПЕКИ СМАРТ-КОНТРАКТІВ 34

Наталія ЯЦКІВ, Аліна МИКОЛАЙСЬКА
КЛАСИФІКАЦІЯ КІБЕРРИЗИКІВ У ХМАРНИХ СЕРВІСАХ 37

Володимир ПРАЦІНЬ, Ігор ПІТУХ
АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ КОМПЛЕКСОМ ЗБЕРІГАННЯ НАФТОПРОДУКТІВ 41

Якименко Н., Слободян В., Якименко Ю., Хомяк Р.
МЕТОД КІЛЬКІСНОЇ ОЦІНКИ КІБЕРРИЗИКІВ НА ОСНОВІ ДОСТОВІРНИХ СТАТИСТИЧНИХ ІМОВІРНІСНИХ МОДЕЛЕЙ 46

Підгурський Д.В.
АНАЛІЗ КОНСТРУКЦІЇ ТА ТИПОВИХ ДЕФЕКТІВ ВІТРОВИХ ТУРБІН 51

УДК 004.056

Степанюк О.В., Прончук Д.С.

Західноукраїнський національний університет

СУЧАСНІ ПЕРСПЕКТИВИ АВТОМАТИЗОВАНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Вступ. У сучасних умовах стрімкого розвитку цифрових технологій та зростання обсягів інформації [1] особливої важливості набуває забезпечення комплексної безпеки об'єктів, інформаційних ресурсів і критично важливої інфраструктури [2].

Автоматизовані системи контролю доступу (АСКД) є ключовим елементом систем фізичного та інформаційного захисту, оскільки вони забезпечують керування доступом до приміщень, ресурсів та інформаційних систем на основі чітко визначених правил і прав користувачів [3].

Актуальність дослідження АСКД зумовлена кількома факторами. По-перше, зростає кількість загроз, пов'язаних із несанкціонованим доступом. По-друге, сучасні організації переходять до інтегрованих систем безпеки, де АСКД взаємодіють з відеоспостереженням, охоронною сигналізацією, біометричними датчиками та інформаційними платформами. По-третє, розвиток хмарних технологій, Інтернету речей та мобільних застосунків стимулює появу нових архітектур АСКД, що вимагають відповідності сучасним стандартам безпеки.

Таким чином, дослідження АСКД є вкрай актуальним, оскільки дозволяє підвищити ефективність захисту об'єктів, забезпечити надійність управління доступом, адаптувати системи до сучасних викликів кібербезпеки.

Мета: дослідити сучасні перспективи розвитку автоматизованих систем контролю доступу.

1. Перспективи автоматизованих систем контролю доступу

Програмні засоби Security information and event management (SIEM) - управління подіями інформаційної безпеки – стали доступними для придбання приблизно 1997 р. Їх функціонал дозволяв зменшити кількість «хибних спрацьовувань» систем виявлення мережевих вторгнень (IDS - intrusion detection system), які загрожували системам IDS. Аналіз експертних думок виявив напрямки з найбільшим потенціалом зростання, які сприятимуть технологічним рішенням АСКД, зокрема концепції SIEM, яка швидко розвивається:

- автоматизація відповіді на кіберінциденти;
- розвиток експертизи у сфері управління системою;
- одавання нового функціоналу SIEM за рахунок методів моніторингу поведінки об'єктів UBA;
- застосування хмарних обчислень як джерела інформації та надання інформації в рамках моделі «as a service»;
- аналіз ситуації на кінцевих вузлах та аналізу трафіку.

Протягом останніх 15 років під SIEM розуміють інструмент для збору

інформації з різних систем і засобів кореляції, при цьому дослідження отриманих масивів даних має на увазі тільки кореляційний аналіз.

Для того, щоб підвищити рівень моніторингу подій безпеки необхідно визначити такі параметри:

- правила, за якими відбуватиметься нормалізація;
- пакети із правилами виявлення загроз;
- методи налаштування джерел даних;
- методику активації джерел;
- зміст правил детектування;
- рекомендації для ситуацій спрацьовування правил.

На даний момент частка покриття SIEM-технології дорівнює 50-60%. Іншим трендом потенційного розвитку SIEM-рішень є автоматизація відповіді на інциденти. Виходячи з результатів опитування, проведеного Positive Technologies, одна четверта частина всіх опитаних спеціалістів у сфері ІБ працює в SIEM-системі щодня 2–4 години. Самими трудомісткими завданнями були названі: аналіз інцидентів (назвали 52% учасників опитування) та обробка хибних спрацьовувань - внесення змін до правил кореляції (58%). Налаштування джерел даних, а також моніторинг їх працездатності займають значну кількість часу на думку 30% фахівців. Така ситуація сприяє еволюції SIEM-рішень у бік програмних рішень Security orchestration and automated response (SOAR), які вирішують питання автоматичного реагування та оркестрації систем безпеки. Для цієї технології покриття приблизно дорівнює 60-70%.

Як третій напрямок для розвитку SIEM слід вказати взаємопроникнення технологій аналізу логів (SIEM-рішення), аналіз мережевого трафіку (Network Traffic Analysis, NTA-рішення), а також аналіз ситуації на кінцевих вузлах (Endpoint Detection & Response, EDR-рішення). За відсутності можливостей, що надаються EDR-системами та детального аналізу трафіку, моніторинг не можна вважати повним. Аналіз мережевого трафіку в найближчі роки буде обов'язковою процедурою при проведенні SIEM, аналіз ситуації на кінцевих вузлах стане опціональною можливістю функціоналу. Для цієї технології частка покриття дорівнює 60-70%.

Четвертою тенденцією можна назвати додавання можливостей UEBA-рішень (механізмів аналізу поведінки об'єктів) до інструментів SIEM, що дасть можливість отримання повної картини ситуації в інфраструктурі на єдиному екрані. Принципова різниця між UEBA та SIEM полягає в тому, що кошти UEBA розробляють моделі поведінки, а SIEM-рішення є деяким конструктором, що збирає логи. В алгоритмах пошуку та вивчення інцидентів можуть використовуватись різні підходи: машинне навчання, глибоке навчання, статистичний аналіз тощо. Ці підходи дають оператору інформацію про те, які об'єкти ведуть себе нетиповим для них чином і чому така поведінка нехарактерна для них. Частка покриття цієї технології складає 70-80%.

Наступний тренд у розвитку SIEM пов'язаний з використанням хмарних технологій. Дослідження, яке провела компанія Enterprise Strategy Group у 2019 р. на замовлення Intel Corp. і Dell Technologies, показало, що 64% організацій планували збільшення витрат на публічні хмарні платформи порівняно з попереднім роком. Ця тенденція стимулює вендорів до додавання найбільш широко використовуваних платформ (Google Cloud Platform, Microsoft Azure, Amazon Web Services) у перелік

підтримуваних джерел SIEM. Крім того, пропонуються системи SIEM за допомогою підходу «as a service», доповнюючи способи розгортання, налаштування та управління системою SIEM (хмарних, віртуальних пристроїв - virtual appliance). На думку експертів, покриття технології дорівнює 60-70%.

Деякі з цих тенденцій вже зараз виявляються певною мірою (рисунок 1), інші з них стануть актуальними протягом 1-3 років. Ці технології покращують рівень якості роботи з системами SIEM і дають можливість знизити навантаження на операторів, які здійснюють моніторинг і реагують на інциденти.

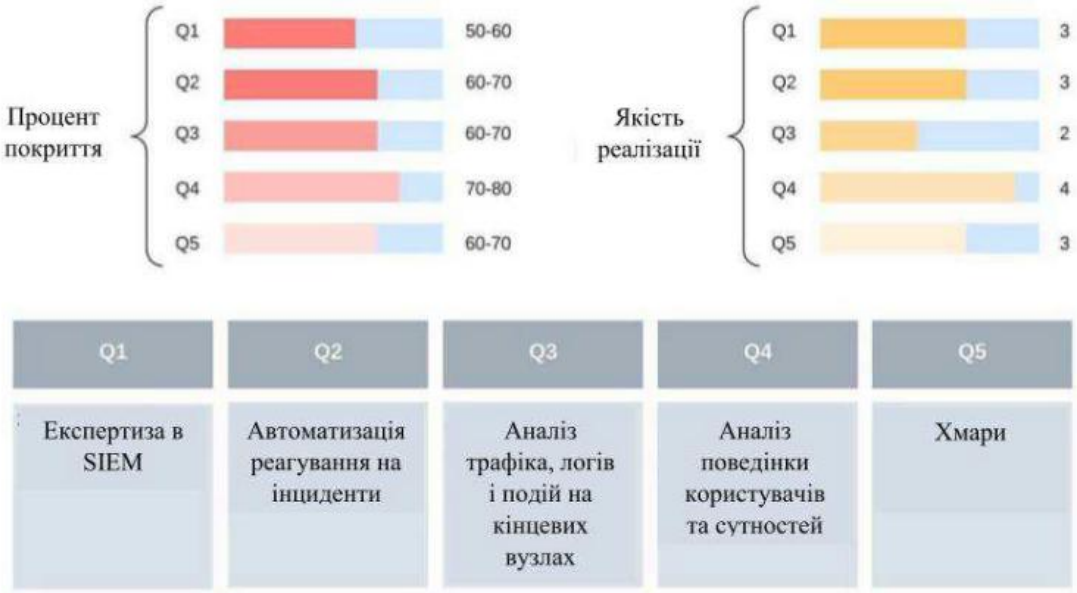

Рисунок 1 - Тренди розвитку SIEM-систем (оцінки якості реалізації: 1 - реалізовано погано; 2 - якість реалізації нижче середнього; 3 - якість реалізації середня; 4 - якість реалізації вище середнього; 5 - реалізовано добре

Подана інформація є експертною оцінкою компанії Positive Technologies. Тенденції є актуальними для компаній-лідерів на ринку SIEM (кількість компаній-лідерів було визначено з допомогою інформації, наданої IDC).

Висновок. Досліджено перспективи розвитку автоматизованих систем контролю доступу, визначено сучасні тенденції та продемонстровано експертні оцінки компанії Positive Technologies.

Перелік використаних джерел.

1. Gil-Garcia J.R., Flores-Zúñiga M.Á. Towards a comprehensive understanding of digital government success: Integrating implementation and adoption factors. Government Information Quarterly. 2020. Vol.37. No. 4. P. 101518..

2. Li F., Lu H., Hou M., Cui K., Darbandi M. Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. Technology in Society. 2021. Vol.64. No.5. P.101487.

3. Elia G., Margherita A., Passiante G. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. Technological Forecasting and Social Change. 2020. Vol.150. P.119791.