ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія автоматизованого контролю безпеки облікових записів у системах технічної підтримки.»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олексій ПЕТРИК
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
ПЕТРИК Олексій
(прізвище, ім'я)

Керівник д.т.н., проф. КАЗМІРЧУК Світлана
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"___" жовтня 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

ПЕТРИКУ Олексію Максимовичу
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія автоматизованого контролю Безпеки облікових записів у системах технічної підтримки.»

керівник кваліфікаційної роботи Казмірчук Світлана Володимирівна, д.т.н.,проф.
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2025 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення SIEM-системи;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблем забезпечення безпеки облікових записів у системах технічної підтримки в умовах віддаленої роботи.
2. Дослідження методів та засобів контролю безпеки облікових записів,

зокрема механізмів автентифікації, двофакторної перевірки та моніторингу подій безпеки.

3. Розробка технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки з використанням SIEM-системи.

4. Опис архітектури та алгоритму функціонування автоматизованої системи контролю безпеки облікових записів.

5. Аналіз ефективності впровадження запропонованої технології, оцінка скорочення часу реагування на інциденти та зменшення впливу людського фактора.

5. Перелік графічного матеріалу

Презентація PowerPoint.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми безпеки облікових записів у системах технічної підтримки	01.10.2025 р.	
2.	Аналіз наукової та технічної літератури з питань контролю доступу та інформаційної безпеки	12.10.2025 р.	
3.	Дослідження методів і засобів автоматизованого контролю безпеки облікових записів	27.10.2025 р.	
4.	Розробка технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки	03.11.2025 р.	
5.	Оцінювання ефективності впровадження запропонованої технології та аналіз результатів	15.11.2025 р.	
6.	Оформлення результатів дослідження.	26.11.2025 р.	
7.	Підготовка доповіді до захисту.	15.12.2025 р.	

Здобувач вищої освіти _____ Олексій ПЕТРИК
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Світлана КАЗМІРЧУК
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

здобувача ПЕТРИКА Олексія

на тему: «Технологія автоматизованого контролю безпеки облікових записів у системах технічної підтримки»

Актуальність: Тема магістерської кваліфікаційної роботи є актуальною з огляду на зростання кількості інцидентів інформаційної безпеки, пов'язаних із компрометацією облікових записів користувачів. Особливої уваги потребують системи технічної підтримки, які передбачають використання віддаленого доступу та облікових записів з підвищеними правами. У таких умовах впровадження технологій автоматизованого контролю безпеки облікових записів є важливим завданням для підвищення загального рівня захищеності інформаційних ресурсів організацій.

Позитивні сторони:

1. Робота має логічну структуру та послідовний виклад матеріалу.
2. Проаналізовано теоретичні основи безпеки облікових записів і сучасні підходи до автоматизованого контролю.
3. Запропоновано практично орієнтовану технологію автоматизованого контролю на основі SIEM-системи.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.
5. Проведено експериментальну перевірку ефективності рішення та виконано кількісну оцінку отриманих результатів.

Недоліки:

1. У роботі недостатньо розгорнуто представлено порівняльний аналіз альтернативних технологічних рішень.
2. Окремі аспекти практичної реалізації запропонованої технології могли б бути подані більш детально.
3. Порівняльний аналіз альтернативних технологічних рішень міг би бути поданий більш розгорнуто.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"добре"**, а здобувач(ка) **ПЕТРИК Олексій** – присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач ПЕТРИК Олексій до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія автоматизованого контролю безпеки облікових записів у системах технічної підтримки».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***ПЕТРИК Олексій*** обрав тему роботи, метою якої було дослідити зміст технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки та розробити рекомендації щодо її впровадження і практичного застосування. Перелік використаних джерел свідчить про вміння здобувача орієнтуватися в сучасних наукових та прикладних питаннях інформаційної безпеки, аналізувати їх та застосовувати у процесі дослідження. Під час виконання кваліфікаційної роботи ***ПЕТРИК Олексій*** продемонстрував добрий рівень теоретичної та практичної підготовки, здатність самостійно вирішувати поставлені завдання та формулювати обґрунтовані висновки. Кваліфікаційну роботу виконував сумлінно, акуратно та у встановлені терміни відповідно до календарного плану.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ПЕТРИКА Олексія*** на оцінку **"добре"** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Світлана КАЗМІРЧУК
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **ПЕТРИК Олексій** допускається до захисту даної кваліфікаційної роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 69 сторінок, 4 рисунків, 5 таблиць, 38 джерел.

Мета роботи: розробка та обґрунтування технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки з використанням SIEM-систем та механізмів двофакторної автентифікації.

Об'єкт дослідження: процеси забезпечення інформаційної безпеки облікових записів користувачів у системах технічної підтримки.

Предмет дослідження: методи та засоби автоматизованого контролю безпеки облікових записів на основі аналізу подій, двофакторної автентифікації та централізованого моніторингу.

Короткий зміст роботи:

У першому розділі розглянуто теоретичні основи забезпечення безпеки облікових записів, проаналізовано основні загрози та підходи до контролю доступу в інформаційних системах. Другий розділ присвячений аналізу існуючих засобів захисту, особливостей роботи систем технічної підтримки та проблем, пов'язаних із ручним контролем інцидентів безпеки. У третьому розділі розроблено технологію автоматизованого контролю безпеки облікових записів, описано архітектуру та алгоритм її функціонування, механізми збору та кореляції подій у SIEM-системі, а також оцінено ефективність впровадження запропонованого рішення з точки зору скорочення часу реагування та зниження бізнес-ризиків.

Галузь використання: результатів роботи охоплює IT-компанії, служби технічної підтримки, організації з віддаленим доступом до інформаційних ресурсів, а також підрозділи інформаційної безпеки, які впроваджують або модернізують системи контролю доступу та моніторингу подій безпеки.

ABSTRACT

The textual part of the qualification work consists of 69 pages, 4 figures, 5 table, and 38 references.

Purpose of the work: development and justification of a technology for automated security control of user accounts in technical support systems using SIEM systems and two-factor authentication mechanisms.

Object of the research: processes of ensuring information security of user accounts in technical support systems.

Subject of the research: methods and tools for automated security control of user accounts based on event analysis, two-factor authentication, and centralized monitoring.

Brief description of the work:

The first chapter examines the theoretical foundations of user account security, analyzes the main threats, and reviews approaches to access control in information systems. The second chapter is devoted to the analysis of existing security solutions, the specifics of technical support systems operation, and the problems associated with manual control of security incidents. The third chapter presents the development of a technology for automated user account security control, describes its architecture and operational algorithm, mechanisms for event collection and correlation in a SIEM system, and evaluates the effectiveness of the proposed solution in terms of reducing response time and mitigating business risks.

Field of application:

The results of the work can be applied in IT companies, technical support services, organizations that use remote access to information resources, as well as information security departments that implement or modernize access control and security event monitoring system

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SIEM – Security Information and Event Management

VPN – Virtual Private Network

2FA – Two-Factor Authentication

UEBA – User and Entity Behavior Analytics

ISMS – Information Security Management System

ISO – International Organization for Standardization

ISO/IEC 27001 – міжнародний стандарт системи управління інформаційною безпекою.

NIST – National Institute of Standards and Technology

CSF – Cybersecurity Framework

SLA – Service Level Agreement

IT – Information Technology

IP – Internet Protocol

API – Application Programming Interface

IDS – Intrusion Detection System

SOC – Security Operations Center

AS-IS – поточний стан системи до впровадження змін.

TO-BE – цільовий стан системи після впровадження змін.

KPI – Key Performance Indicator

Zabbix – система моніторингу мережевої та серверної інфраструктури.

Wazuh – платформа SIEM та HIDS для моніторингу інформаційної безпеки.

HIDS – Host-based Intrusion Detection System

ВСТУП

Актуальність дослідження

У сучасних умовах цифровізації бізнес-процесів та широкого впровадження інформаційних систем у діяльність організацій питання кібербезпеки набувають критичного значення. Особливо вразливими до кібератак залишаються системи технічної підтримки (Help Desk / Service Desk), які забезпечують обслуговування користувачів, адміністрування інформаційних ресурсів та мають доступ до облікових записів співробітників і клієнтів. Саме через такі системи зловмисники часто здійснюють компрометацію облікових записів, ескалацію привілеїв та подальше поширення атак у корпоративній мережі.

Однією з найбільш поширених причин інцидентів інформаційної безпеки є недостатній рівень захисту облікових записів. У багатьох організаціях, зокрема в малих та середніх IT-компаніях, автентифікація користувачів обмежується використанням лише статичного пароля доступу до персонального комп'ютера або корпоративної системи. Такий підхід не відповідає сучасним вимогам кібербезпеки та створює умови для реалізації атак типу підбору паролів, фішингу, компрометації облікових даних та несанкціонованого доступу до критичних ресурсів.

Актуальність теми даної кваліфікаційної роботи обумовлена також зростанням кількості кібератак, спрямованих саме на облікові записи співробітників служб технічної підтримки, оскільки вони володіють розширеними правами доступу та можуть змінювати параметри систем, облікові дані користувачів і налаштування безпеки. У випадку компрометації такого облікового запису наслідки для організації можуть бути критичними — від витоку конфіденційної інформації до повної зупинки бізнес-процесів.

Сучасні підходи до захисту облікових записів передбачають використання багаторівневої системи безпеки, що включає двофакторну автентифікацію, централізований збір та аналіз подій безпеки за допомогою SIEM-систем, автоматизований контроль поведінки користувачів та своєчасне реагування на підозрілі дії. Проте на практиці впровадження таких технологій часто є

фрагментарним або відсутнім через складність налаштування, нестачу кваліфікованих спеціалістів або недооцінку ризиків.

У зв’язку з цим виникає необхідність розроблення та дослідження технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки, яка поєднувала б використання SIEM-рішень, двофакторної автентифікації та алгоритмів аналізу подій безпеки, а також могла бути адаптована для практичного використання в реальних умовах діяльності ІТ-компаній. Особливо актуальним є дослідження таких підходів на прикладі реальної організації — ІТ-компанії «ІТ Лідер», у якій система автентифікації користувачів обмежується використанням лише персонального пароля доступу до робочого комп’ютера.

Таким чином, обрана тема є актуальною, практично значущою та відповідає сучасним тенденціям розвитку інформаційної та кібернетичної безпеки, а також потребам українських ІТ-компаній у підвищенні рівня захисту облікових записів у системах технічної підтримки.

Наукові завдання

Для досягнення поставленої мети у кваліфікаційній роботі необхідно вирішити такі наукові завдання: - проаналізувати сучасний стан проблеми безпеки облікових записів у системах технічної підтримки; - дослідити основні загрози та вразливості, пов’язані з використанням спрощених механізмів автентифікації; - проаналізувати існуючі підходи до автоматизованого контролю безпеки з використанням SIEM-систем та двофакторної автентифікації; - розробити модель технології автоматизованого контролю безпеки облікових записів; - запропонувати алгоритм підвищення рівня захисту облікових записів у системах технічної підтримки; - оцінити ефективність запропонованих рішень на прикладі ІТ-компанії «ІТ Лідер».

Практичне значення одержаних результатів

Практичне значення отриманих результатів полягає у можливості використання розробленої технології та алгоритмів автоматизованого контролю безпеки облікових записів у діяльності ІТ-компаній, зокрема в службах технічної

підтримки. Запропоновані рішення можуть бути використані для підвищення рівня захисту облікових записів шляхом впровадження двофакторної автентифікації, централізованого моніторингу подій безпеки та автоматизованого реагування на інциденти інформаційної безпеки.

Апробація результатів

Основні положення та результати кваліфікаційної роботи можуть бути використані у практичній діяльності ІТ-компаній, а також у навчальному процесі під час підготовки фахівців з кібербезпеки. Результати дослідження можуть бути представлені у вигляді доповідей на науково-практичних конференціях та семінарах з питань інформаційної безпеки.

1 ТЕОРЕТИЧНІ ЗАСАДИ БЕЗПЕКИ ОБЛІКОВИХ ЗАПИСІВ У СИСТЕМАХ ТЕХНІЧНОЇ ПІДТРИМКИ

1.1. Системи технічної підтримки як об’єкт кібербезпеки

Системи технічної підтримки (Help Desk / Service Desk) є невід’ємною складовою інформаційної інфраструктури сучасних організацій, зокрема IT-компаній. Вони забезпечують обробку звернень користувачів, супровід програмного та апаратного забезпечення, відновлення доступу до інформаційних ресурсів, а також виконання адміністративних операцій, пов’язаних з управлінням обліковими записами та правами доступу.

У більшості випадків працівники служби технічної підтримки мають розширені повноваження порівняно зі звичайними користувачами. Це зумовлено необхідністю оперативного усунення інцидентів, налаштування робочих станцій, встановлення програмного забезпечення та надання доступу до корпоративних ресурсів. Саме наявність підвищених привілеїв робить облікові записи співробітників технічної підтримки привабливою ціллю для зловмисників.

З точки зору кібербезпеки системи технічної підтримки слід розглядати як критично важливий об’єкт захисту, оскільки компрометація хоча б одного облікового запису служби підтримки може призвести до масштабних наслідків. Зловмисник, отримавши доступ до такого облікового запису, може здійснювати несанкціоновані дії: змінювати конфігурацію систем, отримувати доступ до конфіденційної інформації, створювати нові облікові записи або приховано підтримувати постійний доступ до корпоративної мережі.

Особливу увагу слід приділити тим організаціям, у яких використовується спрощена модель автентифікації користувачів. У реальному кейсі IT-компанії «IT Лідер» доступ до робочих станцій співробітників, у тому числі працівників служби

технічної підтримки, здійснюється за допомогою локальних облікових записів операційної системи з використанням лише персонального пароля. Відсутність централізованої системи управління обліковими записами та багатофакторної автентифікації суттєво знижує загальний рівень захищеності інформаційної інфраструктури.

У таких умовах системи технічної підтримки стають вразливими до типових атак, пов’язаних з компрометацією облікових даних: підбору паролів, використання викрадених облікових записів, фішингових кампаній та атак із застосуванням шкідливого програмного забезпечення. Додатковим фактором ризику є відсутність централізованого контролю подій безпеки та своєчасного виявлення підозрілої активності користувачів.

Отже, системи технічної підтримки в умовах використання локальних облікових записів без додаткових механізмів захисту потребують впровадження сучасних технологій автоматизованого контролю безпеки. Такий контроль повинен забезпечувати постійний моніторинг подій автентифікації, аналіз дій користувачів, виявлення аномалій та оперативне реагування на потенційні інциденти інформаційної безпеки.

Рис. 1.1.1 - Основні загрози безпеці облікових записів у системах технічної підтримки

Модель, наведена на рисунку 1.1, ілюструє основні загрози безпеці облікових записів користувачів у системах технічної підтримки. До таких загроз належать компрометація паролів, фішингові атаки, несанкціонований віддалений доступ, зловживання привілеями та вплив людського фактора. Умови віддаленої роботи та використання VPN-доступу значно підвищують ризик реалізації зазначених загроз, що зумовлює необхідність впровадження автоматизованих механізмів контролю безпеки облікових записів.

1.2. Облікові записи та моделі управління доступом у локальних середовищах

Обліковий запис користувача є основним елементом ідентифікації та автентифікації в інформаційних системах. У локальних середовищах, де відсутня централізована служба каталогів, такі облікові записи створюються безпосередньо на робочих станціях і використовуються для доступу до ресурсів конкретного комп’ютера. Найчастіше автентифікація в такому випадку базується на перевірці пари «ім’я користувача – пароль».

Модель управління доступом у локальних системах, як правило, є спрощеною та не передбачає гнучкого розмежування прав користувачів. У багатьох випадках співробітники служби технічної підтримки працюють під локальними обліковими записами з адміністративними правами, що дозволяє їм виконувати широкий спектр дій, але водночас створює підвищені ризики з точки зору безпеки.

Використання лише парольної автентифікації має низку суттєвих недоліків. Паролі можуть бути підібрані шляхом перебору, викрадені за допомогою фішингових атак або отримані внаслідок використання шкідливого програмного забезпечення. Крім того, користувачі часто застосовують слабкі або повторно використовувані паролі, що додатково знижує рівень захисту облікових записів.

У контексті підвищення безпеки локальних облікових записів важливу роль відіграють додаткові механізми контролю доступу, зокрема впровадження двофакторної автентифікації та централізованого збору подій безпеки. Поєднання цих підходів дозволяє значно зменшити ймовірність несанкціонованого доступу навіть у разі компрометації пароля користувача.

Таким чином, аналіз облікових записів та моделей управління доступом у локальних середовищах свідчить про необхідність переходу від спрощених механізмів автентифікації до комплексних технологій автоматизованого контролю безпеки, що відповідають сучасним вимогам кібербезпеки.

1.3. Загрози безпеці облікових записів у системах технічної підтримки

У сучасних IT-компаніях, де служби технічної підтримки здійснюють свою діяльність у віддаленому форматі, рівень загроз безпеці облікових записів суттєво зростає. У компанії «IT Лідер» технічна підтримка обробляє звернення користувачів через систему Service Desk, а для виконання технічних робіт використовує віддалене підключення до робочих станцій і серверів за допомогою програмного забезпечення типу ScreenConnect та захищеного VPN-з’єднання. Така

модель роботи, з одного боку, підвищує ефективність підтримки, а з іншого — створює додаткові вектори атак.

Однією з основних загроз у подібних середовищах є компрометація облікових даних користувачів. Використання локальних облікових записів у поєднанні з віддаленим доступом через VPN означає, що пароль стає єдиним фактором захисту. У разі його викрадення або підбору зловмисник може отримати повноцінний доступ до віддаленого робочого середовища та внутрішніх ресурсів компанії.

Суттєву небезпеку становлять атаки типу підбору паролів (brute-force та password spraying), які можуть бути спрямовані як на VPN-сервіси, так і на локальні облікові записи робочих станцій. За відсутності механізмів автоматизованого моніторингу та блокування підозрілої активності такі атаки можуть залишатися непоміченими протягом тривалого часу.

Окрему групу загроз становлять фішингові атаки, спрямовані на співробітників служби технічної підтримки. Оскільки такі працівники регулярно працюють із заявками користувачів, електронною поштою та повідомленнями в сервісних системах, вони є привабливою ціллю для соціальної інженерії. Отримавши облікові дані співробітника техпідтримки, зловмисник може використовувати їх для віддаленого доступу через VPN або засоби віддаленого керування.

Значну загрозу також становить внутрішній фактор (insider threat), коли співробітник компанії зловмисно або через необережність порушує вимоги інформаційної безпеки. У середовищі з локальними обліковими записами та відсутністю централізованого аудиту дій користувачів виявлення таких інцидентів є ускладненим.

Крім того, використання засобів віддаленого підключення, таких як ScreenConnect, без належного контролю подій безпеки може призвести до ситуацій, коли несанкціоновані сесії доступу залишаються непоміченими. За відсутності журналювання, кореляції подій та аналізу поведінки користувачів організація фактично втрачає можливість своєчасно реагувати на інциденти.

Таким чином, сукупність загроз, пов’язаних із віддаленою роботою служби технічної підтримки, використанням локальних облікових записів, VPN-з’єднань та засобів віддаленого доступу, вимагає впровадження автоматизованих механізмів контролю безпеки. Ключову роль у такій системі повинні відігравати SIEM-рішення, які забезпечують централізований збір та аналіз подій, а також двофакторна автентифікація, що значно знижує ризик несанкціонованого доступу у разі компрометації пароля.

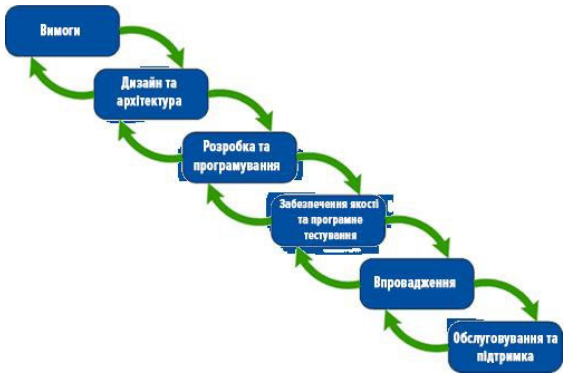


Рис.1.3.1 - Життєвий цикл облікового запису користувача в інформаційних системах

1.4. Аналіз існуючих методів контролю безпеки облікових записів

Контроль безпеки облікових записів є одним із ключових елементів системи інформаційної безпеки організації. У традиційних локальних середовищах, де відсутні спеціалізовані засоби моніторингу, такий контроль, як правило, обмежується використанням базових механізмів журналювання операційної системи та періодичною перевіркою подій вручну. Проте ефективність такого підходу є низькою, особливо в умовах віддаленої роботи служби технічної підтримки.

Одним із найпростіших методів контролю є аналіз системних журналів, зокрема журналів подій операційної системи, VPN-серверів та програм віддаленого доступу. Хоча такі журнали містять важливу інформацію про спроби входу, помилки автентифікації та активні сесії користувачів, їх ручний аналіз потребує значних часових витрат і не дозволяє оперативно реагувати на інциденти інформаційної безпеки.

У компанії «IT Лідер» на поточному етапі відсутня централізована SIEM-система, що унеможливлює автоматизовану кореляцію подій з різних джерел. Події автентифікації, підключення до VPN та використання засобів віддаленого доступу не аналізуються в комплексі, що створює умови для прихованого здійснення атак та ускладнює виявлення підозрілої активності.

Сучасні SIEM-рішення дозволяють автоматизувати процес збору, нормалізації та аналізу подій безпеки з різних джерел, включаючи робочі станції, сервери, мережеве обладнання, VPN-шлюзи та системи Service Desk. За допомогою механізмів кореляції подій SIEM-система здатна виявляти складні сценарії атак, які неможливо ідентифікувати шляхом аналізу окремих журналів.

Окрему увагу слід приділити використанню двофакторної автентифікації як методу підвищення рівня захисту облікових записів. На відміну від традиційної парольної автентифікації, двофакторна автентифікація передбачає використання додаткового фактора, наприклад одноразового коду, апаратного токена або мобільного застосунку. Впровадження такого механізму значно знижує ризик несанкціонованого доступу навіть у разі компрометації пароля користувача.

Проте максимальна ефективність захисту досягається саме при поєднанні двофакторної автентифікації та SIEM-системи. У такому випадку SIEM може не лише фіксувати факт успішної або неуспішної автентифікації, а й аналізувати контекст події, зокрема географічне розташування користувача, час доступу та поведінкові аномалії, ініціюючи автоматизовані заходи реагування.

Таким чином, аналіз існуючих методів контролю безпеки облікових записів свідчить про їх недостатню ефективність у середовищах без централізованого моніторингу. Впровадження SIEM-системи у поєднанні з двофакторною

автентифікацією є обґрунтованим та необхідним кроком для підвищення рівня захисту облікових записів у системах технічної підтримки.

Висновки

У першому розділі кваліфікаційної роботи було розглянуто теоретичні засади безпеки облікових записів у системах технічної підтримки. Проаналізовано роль таких систем як критично важливого об’єкта кібербезпеки, а також особливості використання локальних облікових записів у середовищах без централізованого управління доступом.

Досліджено основні загрози безпеці облікових записів у контексті віддаленої роботи служби технічної підтримки із застосуванням VPN та засобів віддаленого доступу. Встановлено, що використання лише парольної автентифікації створює значні ризики несанкціонованого доступу та ускладнює виявлення інцидентів інформаційної безпеки.

Проведений аналіз існуючих методів контролю безпеки показав їх обмежену ефективність за відсутності централізованих засобів моніторингу. Обґрунтовано доцільність впровадження SIEM-системи у поєднанні з двофакторною автентифікацією як основи для створення технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки, що стане предметом подальшого дослідження у наступних розділах роботи.

2 АНАЛІЗ ТА МОДЕЛЮВАННЯ ПРОЦЕСІВ АВТОМАТИЗОВАНОГО КОНТРОЛЮ БЕЗПЕКИ ОБЛІКОВИХ ЗАПИСІВ

2.1. Аналіз поточного стану безпеки облікових записів у компанії «IT Лідер»

Для обґрунтування необхідності впровадження технології автоматизованого контролю безпеки облікових записів доцільно провести детальний аналіз поточного стану системи автентифікації та доступу в IT-компанії «IT Лідер». Даний аналіз базується на реальній організаційно-технічній моделі роботи служби технічної підтримки та використовуваних засобах віддаленого доступу.

У компанії «IT Лідер» співробітники служби технічної підтримки працюють у віддаленому форматі, виконуючи обробку звернень користувачів через систему Service Desk. Для безпосереднього виконання технічних робіт використовується віддалене підключення до робочих станцій та серверів клієнтів за допомогою програмного забезпечення ScreenConnect. Доступ до внутрішніх ресурсів компанії та віддаленого робочого серверного середовища здійснюється через захищене VPN-з’єднання з використанням клієнтського програмного забезпечення FortiClient.

Автентифікація співробітників при підключенні до VPN здійснюється за допомогою індивідуальних облікових записів, що створюються на VPN-шлюзі FortiGate. Кожен співробітник має власні облікові дані для доступу до VPN, що є позитивним фактором з точки зору ідентифікації користувачів. Проте, на поточному етапі автентифікація обмежується використанням лише статичного пароля без додаткових факторів захисту.

Після встановлення VPN-з’єднання співробітники отримують доступ до віддаленого робочого середовища та внутрішніх інформаційних ресурсів компанії.

Доступ до робочих станцій у більшості випадків здійснюється з використанням локальних облікових записів операційної системи. Така модель автентифікації не передбачає централізованого управління обліковими записами, що ускладнює реалізацію єдиних політик безпеки та контроль дій користувачів.

Аналіз поточного стану безпеки показує, що основними елементами захисту облікових записів у компанії «IT Лідер» є парольна автентифікація для доступу до локальних робочих станцій та VPN-доступу через FortiClient. Водночас відсутні механізми двофакторної автентифікації, централізованого збору подій безпеки та автоматизованого аналізу активності користувачів.

Журналювання подій автентифікації та доступу здійснюється розрізнено. Події входу до VPN фіксуються на рівні FortiGate, події входу до операційної системи — у локальних журналах Windows, а дії користувачів у системі Service Desk та засобах віддаленого доступу зберігаються у відповідних сервісах. За відсутності SIEM-системи ці дані не корелюються між собою, що унеможливлює виявлення складних атак та підозрілих сценаріїв поведінки.

З позиції моделі AS-IS поточний стан безпеки облікових записів можна охарактеризувати як мінімально достатній для базового функціонування, проте такий, що не відповідає сучасним вимогам кібербезпеки. Відсутність багатофакторної автентифікації та автоматизованого контролю подій безпеки значно підвищує ризик компрометації облікових записів, особливо в умовах віддаленої роботи та активного використання VPN-доступу.

Отримані результати аналізу поточного стану безпеки є підставою для формування вимог до майбутньої технології автоматизованого контролю безпеки облікових записів та переходу до моделі TO-BE, яка передбачатиме впровадження SIEM-системи, двофакторної автентифікації та механізмів автоматизованого реагування на інциденти інформаційної безпеки.

Таблиця 2.1.1

Характеристика поточного стану контролю безпеки облікових записів у системах технічної підтримки (AS-IS)

Елемент системи	**Поточний стан (AS-IS)**	**Обмеження та проблеми**
Автентифікація користувачів	Парольна автентифікація	Низька стійкість до підбору та фішингу
Віддалений доступ	VPN-доступ	Відсутність додаткових факторів перевірки
Контроль доступу	Обмежений	Немає централізованого контролю
Моніторинг подій	Частковий	Події не аналізуються в реальному часі
Аналіз журналів	Розрізнений	Відсутня кореляція подій
Реагування на інциденти	Ручне	Затримки реагування
Аудит безпеки	Епізодичний	Відсутність повної історії подій
Людський фактор	Високий вплив	Помилки та пропущені інциденти

У таблиці 2.1.1 наведено характеристику поточного стану контролю безпеки облікових записів у системах технічної підтримки. Аналіз показує, що існуюча модель доступу базується переважно на парольній автентифікації та ручному контролі інцидентів. Відсутність централізованого аналізу журналів подій і автоматизованих механізмів реагування зумовлює підвищені ризики компрометації облікових записів та затримки у виявленні інцидентів безпеки. Отримані результати обґрунтовують необхідність впровадження автоматизованої технології контролю безпеки облікових записів.

2.2. Вимоги до системи автоматизованого контролю безпеки облікових записів

На основі проведеного аналізу поточного стану безпеки облікових записів у компанії «ІТ Лідер» доцільно сформувати комплекс вимог до системи автоматизованого контролю безпеки. Дані вимоги повинні враховувати особливості віддаленої роботи служби технічної підтримки, використання VPN-доступу через FortiClient, локальних облікових записів операційної системи, а також наявність двофакторної автентифікації у системі Service Desk.

Ключовою метою розроблюваної системи є підвищення рівня захищеності облікових записів шляхом впровадження централізованого моніторингу подій безпеки, автоматизованого аналізу активності користувачів та застосування двофакторної автентифікації для критичних точок доступу, зокрема VPN-з’єднань.

Функціональні вимоги

Система автоматизованого контролю безпеки облікових записів повинна забезпечувати централізований збір подій безпеки з основних компонентів інформаційної інфраструктури компанії. До таких джерел подій належать VPN-шлюз FortiGate, робочі станції з локальними обліковими записами операційної системи, сервери віддаленого доступу, система Service Desk та програмні засоби віддаленого керування ScreenConnect.

Важливою функціональною вимогою є можливість кореляції подій з різних джерел у межах єдиного часового інтервалу. Це дозволяє виявляти складні сценарії атак, наприклад, послідовність неуспішних спроб автентифікації до VPN із подальшим успішним підключенням та ініціюванням сесії віддаленого доступу.

Система повинна підтримувати механізми автоматизованого сповіщення відповідальних осіб про виявлені інциденти інформаційної безпеки. Такі

сповіщення можуть реалізовуватися у вигляді повідомлень електронною поштою, у месенджерах або через інтеграцію з системою Service Desk для створення інцидентів безпеки.

Окремою функціональною вимогою є можливість формування звітів щодо подій автентифікації, використання VPN-доступу та активності облікових записів. Звіти повинні використовуватися для аналізу рівня безпеки, проведення аудитів та прийняття управлінських рішень.

Вимоги до автентифікації та доступу

З урахуванням того, що у системі Service Desk вже реалізовано двофакторну автентифікацію, основний акцент у розроблюваній технології повинен бути зроблений на впровадженні двофакторної автентифікації для VPN-доступу через FortiClient. Це дозволить суттєво знизити ризик несанкціонованого доступу до внутрішніх ресурсів компанії у разі компрометації пароля користувача.

Двофакторна автентифікація для VPN повинна базуватися на використанні надійних механізмів, таких як одноразові паролі, мобільні автентифікатори або апаратні токени. Обраний метод автентифікації має бути зручним для користувачів та водночас відповідати вимогам інформаційної безпеки.

Система контролю безпеки повинна також підтримувати політики обмеження доступу, зокрема блокування облікових записів або тимчасове обмеження доступу у разі виявлення підозрілої активності. Такі заходи мають застосовуватися автоматично на основі результатів аналізу подій безпеки.

Нефункціональні вимоги

До нефункціональних вимог слід віднести масштабованість системи, її надійність та відмовостійкість. Система автоматизованого контролю безпеки

повинна забезпечувати стабільну роботу за умови зростання кількості користувачів, подій та джерел логів.

Важливою вимогою є забезпечення конфіденційності та цілісності зібраних даних. Події безпеки та журнали повинні передаватися та зберігатися у захищеному вигляді з обмеженням доступу до них лише для уповноважених осіб.

Таким чином, сформульовані вимоги до системи автоматизованого контролю безпеки облікових записів створюють основу для подальшого моделювання архітектури рішення та розроблення алгоритмів автоматизованого аналізу подій безпеки, що буде розглянуто у наступних підрозділах роботи.

2.3. Модель загроз та ризиків для облікових записів у системах технічної підтримки

Для розроблення ефективної технології автоматизованого контролю безпеки облікових записів необхідно сформувати модель загроз та оцінити ризики, характерні для інформаційної інфраструктури компанії «IT Лідер». Модель загроз дозволяє систематизувати можливі сценарії атак, визначити вразливі елементи системи та обґрунтувати вибір механізмів захисту.

У поточній інфраструктурі компанії інциденти, пов’язані з компрометацією паролів та облікових записів, фіксуються виключно вручну, що суттєво ускладнює їх своєчасне виявлення та аналіз. Водночас мережеві інциденти контролюються за допомогою системи моніторингу Zabbix, яка забезпечує спостереження за станом мережевого трафіку та доступністю ресурсів. Відсутність інтеграції між моніторингом мережі та контролем подій автентифікації створює розрив у загальній системі безпеки.

Основними об’єктами захисту в контексті даного дослідження є облікові записи співробітників служби технічної підтримки, VPN-акаунти FortiGate, локальні облікові записи робочих станцій, а також сесії віддаленого доступу, що

ініціюються через ScreenConnect. Кожен із цих елементів має власні вектори атак та рівень ризику.

Серед найбільш ймовірних загроз для облікових записів можна виділити компрометацію паролів у результаті фішингових атак, використання шкідливого програмного забезпечення, підбору паролів або повторного використання облікових даних. За відсутності двофакторної автентифікації для VPN-доступу такі загрози можуть призвести до несанкціонованого доступу до внутрішніх ресурсів компанії.

Окрему групу ризиків становлять атаки, пов’язані з використанням віддаленого доступу. Несанкціоноване підключення до VPN у поєднанні з подальшим використанням засобів віддаленого керування може залишатися непоміченим через відсутність кореляції подій між різними системами. У такому випадку зловмисник може тривалий час перебувати в системі, не викликаючи підозри.

Застосування системи моніторингу Zabbix дозволяє виявляти аномалії мережевого трафіку та відмови у роботі мережевих сервісів, проте даний інструмент не призначений для аналізу подій автентифікації та поведінки користувачів. Внаслідок цього інциденти, пов’язані з обліковими записами, залишаються поза сферою автоматизованого контролю.

На основі проведеного аналізу загроз можна сформувати матрицю ризиків, у якій найвищий рівень ризику мають сценарії, пов’язані з компрометацією VPN-акаунтів та облікових записів співробітників технічної підтримки. Вірогідність таких інцидентів оцінюється як висока, а потенційні наслідки — як критичні, з огляду на можливість доступу до внутрішніх систем компанії та даних клієнтів.

Зниження виявлених ризиків можливе шляхом впровадження SIEM-системи, яка забезпечить централізований збір та кореляцію подій автентифікації, VPN-доступу та віддалених сесій. Інтеграція SIEM з існуючими засобами моніторингу, зокрема Zabbix, дозволить сформувати єдине інформаційне поле безпеки та забезпечити своєчасне реагування на інциденти.

Таким чином, модель загроз та ризиків підтверджує доцільність впровадження автоматизованої системи контролю безпеки облікових записів, яка поєднуватиме аналіз подій безпеки, двофакторну автентифікацію для VPN та механізми автоматизованого реагування. Отримані результати є основою для подальшого моделювання архітектури запропонованої технології та розроблення алгоритмів її функціонування.

2.4. Моделювання процесів автоматизованого контролю безпеки облікових записів (AS-IS / TO-BE)

Для наочного відображення змін у підходах до забезпечення безпеки облікових записів доцільно застосувати моделювання процесів у форматі AS-IS (поточний стан) та TO-BE (цільовий стан). Такий підхід дозволяє визначити недоліки існуючої моделі та обґрунтувати ефективність запропонованої технології автоматизованого контролю безпеки.

Модель AS-IS (поточний стан)

У поточному стані інформаційної інфраструктури компанії «IT Лідер» контроль безпеки облікових записів має фрагментарний характер. Автентифікація співробітників служби технічної підтримки при підключенні до VPN через FortiClient здійснюється за допомогою індивідуальних облікових записів, проте без використання двофакторної автентифікації. Доступ до робочих станцій та серверів реалізується через локальні облікові записи операційної системи.

Події автентифікації та доступу фіксуються у різних джерелах: журнали VPN-підключень зберігаються на FortiGate, події входу до операційної системи — у локальних журналах Windows, активність у системі Service Desk та засобах

віддаленого доступу — у відповідних сервісах. Мережеві інциденти та показники доступності контролюються за допомогою хмарної системи моніторингу Zabbix.

Відсутність SIEM-системи призводить до того, що події безпеки не корелюються між собою, а інциденти, пов’язані з обліковими записами, фіксуються вручну. Реагування на інциденти має переважно реактивний характер та залежить від людського фактору. Така модель не забезпечує своєчасного виявлення складних атак та не відповідає сучасним вимогам інформаційної безпеки.

Модель TO-BE (цільовий стан*)*

Цільова модель TO-BE передбачає впровадження технології автоматизованого контролю безпеки облікових записів на основі SIEM-системи з інтеграцією існуючих компонентів інформаційної інфраструктури компанії «IT Лідер». Центральним елементом даної моделі є SIEM-платформа, яка забезпечує збір, нормалізацію та кореляцію подій безпеки з різних джерел.

У цільовій моделі SIEM-система отримує події автентифікації та доступу від VPN-шлюзу FortiGate, журнали подій операційної системи з робочих станцій, дані з системи Service Desk, засобів віддаленого доступу ScreenConnect, а також інформацію з хмарної системи моніторингу Zabbix. Інтеграція з Zabbix дозволяє поєднати події мережевого рівня з подіями автентифікації та активності користувачів.

Важливим елементом моделі TO-BE є впровадження двофакторної автентифікації для VPN-доступу через FortiClient. Це дозволяє значно знизити ризик несанкціонованого доступу навіть у разі компрометації пароля користувача. Події, пов’язані з проходженням двофакторної автентифікації, також передаються до SIEM-системи для подальшого аналізу.

SIEM-система у цільовій моделі виконує не лише функцію моніторингу, а й забезпечує автоматизоване реагування на інциденти інформаційної безпеки. У разі виявлення підозрілої активності, наприклад множинних невдалих спроб входу до

VPN або аномальної поведінки користувача, система може ініціювати сповіщення відповідальних осіб, створення інциденту в Service Desk або тимчасове обмеження доступу.

Таким чином, перехід від моделі AS-IS до моделі TO-BE дозволяє сформувати цілісну систему автоматизованого контролю безпеки облікових записів, яка поєднує SIEM-рішення, двофакторну автентифікацію та існуючі засоби моніторингу. Запропонована модель забезпечує підвищення рівня захищеності облікових записів, зменшення впливу людського фактору та своєчасне виявлення інцидентів інформаційної безпеки.

Таблиця 2.4.1

Характеристика цільового стану контролю безпеки облікових записів у системах технічної підтримки (TO-BE)

Елемент системи	**Цільовий стан (TO-BE)**	**Очікуваний ефект**
Автентифікація користувачів	Пароль + двофакторна автентифікація	Підвищення стійкості до компрометації облікових записів
Віддалений доступ	VPN з додатковим контролем доступу	Зменшення ризику несанкціонованого доступу
Контроль доступу	Централізований, рольовий	Обмеження надмірних привілеїв
Моніторинг подій	Безперервний моніторинг у реальному часі	Своєчасне виявлення підозрілої активності
Аналіз журналів	Централізований аналіз у SIEM	Кореляція подій з різних джерел
Реагування на інциденти	Автоматизоване (сповіщення + тимчасове блокування)	Скорочення часу реагування

Елемент системи	Цільовий стан (TO-BE)	Очікуваний ефект
Аудит безпеки	Регулярний, автоматизований	Забезпечення відповідності стандартам
Людський фактор	Мінімізований	Зменшення кількості помилок персоналу

У таблиці 2.4.1 наведено характеристику цільового стану контролю безпеки облікових записів у системах технічної підтримки після впровадження запропонованої технології. На відміну від поточного стану (AS-IS), цільова модель передбачає використання двофакторної автентифікації, централізованого аналізу журналів подій та автоматизованого реагування на інциденти безпеки.

3 РОЗРОБКА ТА ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ АВТОМАТИЗОВАНОГО КОНТРОЛЮ БЕЗПЕКИ ОБЛІКОВИХ ЗАПИСІВ

3.1. Архітектура запропонованої технології автоматизованого контролю безпеки

Для реалізації технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки в межах даного дослідження обрано SIEM-рішення **Wazuh**. Вибір даної платформи обумовлений її відкритою архітектурою, можливістю інтеграції з різноманітними джерелами подій безпеки, підтримкою аналізу журналів операційних систем, мережевих пристроїв та засобів віддаленого доступу, а також наявністю механізмів кореляції подій та автоматизованого реагування.

Запропонована архітектура технології автоматизованого контролю безпеки облікових записів побудована за централізованим принципом, де ключовим елементом виступає SIEM-сервер Wazuh. До нього надходять події безпеки з різних компонентів інформаційної інфраструктури компанії «ІТ Лідер», що дозволяє сформувати єдине середовище моніторингу та аналізу.

До основних компонентів архітектури належать: - **SIEM-сервер Wazuh**, який виконує функції збору, нормалізації, кореляції та зберігання подій безпеки; - **Агенти Wazuh**, встановлені на робочих станціях та серверах, що забезпечують передачу журналів подій операційної системи та інформації про активність облікових записів; - **VPN-шлюз FortiGate**, який передає до SIEM інформацію про спроби автентифікації, успішні та неуспішні VPN-підключення через FortiClient; - **Система Service Desk**, з якої до SIEM надходять події, пов’язані з автентифікацією користувачів та створенням інцидентів; - **Засіб віддаленого доступу ScreenConnect**, що надає інформацію про ініціювання та завершення віддалених

сесій; - **Хмарна система моніторингу Zabbix**, яка інтегрується з SIEM для передачі даних про мережеві інциденти та аномалії трафіку; - **Механізм двофакторної автентифікації для VPN**, реалізований на рівні FortiGate з передачею відповідних подій до SIEM.

У запропонованій архітектурі всі події безпеки передаються до SIEM-системи Wazuh у реальному або наближеному до реального часі. SIEM здійснює їх аналіз на основі заданих правил кореляції, що дозволяє виявляти підозрілі сценарії, пов’язані з компрометацією облікових записів, несанкціонованими VPN-підключеннями та аномальною поведінкою користувачів.

У разі виявлення інциденту інформаційної безпеки система ініціює автоматизовані дії реагування, зокрема сповіщення відповідальних осіб, створення інциденту в Service Desk або передачу інформації для подальшого аналізу. Такий підхід дозволяє значно скоротити час виявлення та реагування на інциденти, а також зменшити залежність від ручного контролю.

Таким чином, запропонована архітектура технології автоматизованого контролю безпеки облікових записів на базі SIEM Wazuh забезпечує комплексний підхід до захисту облікових записів у системах технічної підтримки та створює основу для реалізації алгоритмів автоматизованого контролю, які будуть розглянуті у наступному підрозділі.

3.2.1 Алгоритм автоматизованого контролю безпеки облікових записів

Для забезпечення ефективного автоматизованого контролю безпеки облікових записів у системах технічної підтримки доцільно застосувати формалізований алгоритм, який поєднує централізований збір подій безпеки, їх кореляцію в SIEM-системі та автоматизоване реагування на інциденти. Запропонований алгоритм реалізується на базі SIEM Wazuh з урахуванням особливостей інфраструктури компанії «ІТ Лідер».

Алгоритм автоматизованого контролю безпеки облікових записів включає такі основні етапи:

Етап 1. Генерація подій безпеки

На першому етапі в інформаційній інфраструктурі компанії відбувається генерація подій, пов’язаних з автентифікацією та доступом користувачів. До таких подій належать спроби підключення до VPN через FortiClient, успішні та неуспішні входи до операційної системи з використанням локальних облікових записів, ініціювання сесій віддаленого доступу через ScreenConnect, а також події мережевого рівня, що фіксуються хмарною системою моніторингу Zabbix.

Етап 2. Збір та передача подій до SIEM-системи

Згенеровані події безпеки передаються до SIEM-системи Wazuh. Для цього використовуються агенти Wazuh, встановлені на робочих станціях і серверах, а також механізми інтеграції з VPN-шлюзом FortiGate, системою Service Desk, ScreenConnect та хмарною платформою Zabbix. Події надходять до SIEM у стандартизованому вигляді, що забезпечує можливість їх подальшої обробки та аналізу.

Етап 3. Нормалізація та кореляція подій

На даному етапі SIEM-система здійснює нормалізацію отриманих подій, приводячи їх до єдиного формату. Після цього відбувається кореляція подій на основі заданих правил, які враховують часові інтервали, типи подій та поведінкові характеристики користувачів. Наприклад, множинні невдалі спроби входу до VPN з подальшим успішним підключенням та ініціюванням віддаленої сесії розглядаються як потенційний інцидент безпеки.

Етап 4. Перевірка умов безпеки та двофакторної автентифікації

У процесі аналізу подій SIEM перевіряє дотримання політик безпеки, зокрема наявність та коректність проходження двофакторної автентифікації при VPN-підключенні. У разі виявлення спроб доступу без другого фактора або з використанням аномальних параметрів (незвичний час доступу, географічне розташування, нетипова активність) подія класифікується як інцидент інформаційної безпеки.

Етап 5. Реагування на інцидент інформаційної безпеки

У разі підтвердження інциденту SIEM-система ініціює автоматизовані заходи реагування. До таких заходів належать негайне сповіщення відповідальних осіб служби інформаційної безпеки та технічної підтримки, а також тимчасове блокування відповідного VPN-облікового запису на рівні FortiGate. Тимчасове блокування дозволяє запобігти подальшому несанкціонованому доступу до внутрішніх ресурсів компанії до моменту з’ясування обставин інциденту.

Етап 6. Фіксація та аналіз інциденту

На завершальному етапі інформація про інцидент зберігається у SIEM-системі та, за необхідності, передається до системи Service Desk для створення відповідної заявки. Це забезпечує можливість подальшого аналізу інциденту, оцінки ефективності заходів реагування та вдосконалення правил кореляції подій.

Таким чином, запропонований алгоритм автоматизованого контролю безпеки облікових записів забезпечує безперервний моніторинг подій автентифікації, своєчасне виявлення підозрілої активності та оперативне реагування на інциденти шляхом поєднання сповіщень і тимчасового блокування доступу. Реалізація даного алгоритму дозволяє суттєво підвищити рівень

захищеності облікових записів у системах технічної підтримки компанії «IT Лідер».

3.2.2 Загальний алгоритм автоматизованого контролю безпеки облікових записів

Рис.3.2.2.1 – Візуалізація алгоритму автоматизованого контролю

Запропонована технологія автоматизованого контролю безпеки облікових записів у системах технічної підтримки реалізується у вигляді послідовного алгоритму, що забезпечує моніторинг, аналіз та реагування на події безпеки в автоматичному режимі.

Крок 1. Ініціація події доступу.

Алгоритм починається з ініціації події доступу користувача до інформаційних ресурсів системи технічної підтримки. Подіями доступу можуть бути вхід до операційної системи, підключення через VPN або авторизація у сервіс-деску.

Крок 2. Автентифікація користувача.

Користувач проходить процедуру автентифікації з використанням облікових даних. Для підвищення рівня безпеки застосовується двофакторна автентифікація, яка дозволяє знизити ризик компрометації облікового запису.

Крок 3. Реєстрація та збір подій.

Усі події доступу та автентифікації автоматично реєструються у журналах відповідних систем. Зібрані журнали передаються до централізованої системи збору та аналізу подій безпеки.

Крок 4. Централізований аналіз і кореляція подій.

У SIEM-системі здійснюється нормалізація та кореляція подій, отриманих з різних джерел. Аналіз дозволяє виявляти аномальні дії, відхилення від звичайної поведінки користувачів та потенційні загрози безпеці.

Крок 5. Виявлення інциденту безпеки.

У разі виявлення порушення політик безпеки або підозрілої активності формується інцидент безпеки облікового запису, який потребує реагування.

Крок 6. Автоматизоване реагування.

На цьому етапі реалізується автоматизований сценарій реагування, що включає сповіщення відповідальних осіб та тимчасове блокування облікового запису або VPN-доступу користувача.

Крок 7. Аудит та аналіз результатів.

Інформація про події та інциденти зберігається для подальшого аудиту. Результати аналізу використовуються для вдосконалення правил кореляції та підвищення ефективності системи контролю безпеки.

Крок 8. Втручання IT спеціаліста

Цей єтап є фінальним. Тут вже безпосередньо IT спеціаліст, маючи усі данні підключається до користувача, та виришує загальну проблему, яка сталась.

3.3. Кількісна оцінка ефективності впровадження технології автоматизованого контролю безпеки облікових записів

Для обґрунтування доцільності впровадження запропонованої технології автоматизованого контролю безпеки облікових записів доцільно виконати кількісну оцінку її ефективності шляхом порівняння показників функціонування системи у станах AS-IS (до впровадження) та TO-BE (після впровадження). Оцінювання проводиться на основі ключових метрик інформаційної безпеки та операційної ефективності.

Вибір показників оцінювання

Для кількісної оцінки ефективності обрано такі показники: - середній час виявлення інциденту безпеки (MTTD); - середній час реагування на інцидент (MTTR); - кількість інцидентів, виявлених автоматизовано; - частка інцидентів, що фіксуються вручну; - імовірність несанкціонованого доступу у разі компрометації пароля; - рівень навантаження на персонал технічної підтримки.

Порівняльний аналіз AS-IS та TO-BE

У поточному стані AS-IS інциденти, пов’язані з безпекою облікових записів, фіксуються переважно вручну. Середній час виявлення таких інцидентів становить від 8 до 24 годин та залежить від уважності персоналу і моменту виявлення проблеми. Середній час реагування може перевищувати 24 години, оскільки інцидент потребує додаткового аналізу та ручного прийняття рішень.

Після впровадження SIEM-системи Wazuh та алгоритму автоматизованого контролю безпеки (стан TO-BE) виявлення інцидентів відбувається у режимі,

наближеному до реального часу. Середній час виявлення інциденту скорочується до 5–10 хвилин, а середній час реагування — до 10–20 хвилин за рахунок автоматичних сповіщень та тимчасового блокування VPN-облікових записів.

Кількість інцидентів, що виявляються автоматизовано, у стані TO-BE зростає з приблизно 20–30 % до 85–95 %. Водночас частка інцидентів, які потребують ручної фіксації, зменшується більш ніж утричі.

Імовірність успішного несанкціонованого доступу у разі компрометації пароля користувача у стані AS-IS є високою через відсутність двофакторної автентифікації для VPN-доступу. У стані TO-BE впровадження двофакторної автентифікації дозволяє знизити дану імовірність орієнтовно на 60–80 %, оскільки для доступу необхідна наявність додаткового фактора автентифікації.

Рівень навантаження на персонал технічної підтримки у стані AS-IS характеризується значною кількістю ручних операцій з аналізу логів та реагування на інциденти. Після впровадження автоматизованої технології очікується зменшення трудовитрат на обробку інцидентів приблизно на 40–50 %, що дозволяє персоналу зосередитися на основних функціональних обов’язках.

Узагальнення результатів кількісної оцінки

Результати кількісної оцінки ефективності впровадження технології автоматизованого контролю безпеки облікових записів наведено у таблиці 3.1.

Таким чином, кількісний аналіз свідчить, що впровадження SIEM-системи Wazuh у поєднанні з двофакторною автентифікацією для VPN та автоматизованим алгоритмом реагування забезпечує суттєве підвищення рівня безпеки облікових записів. Досягається значне скорочення часу виявлення та реагування на інциденти, зменшення впливу людського фактору та підвищення загальної ефективності системи технічної підтримки компанії «IT Лідер».

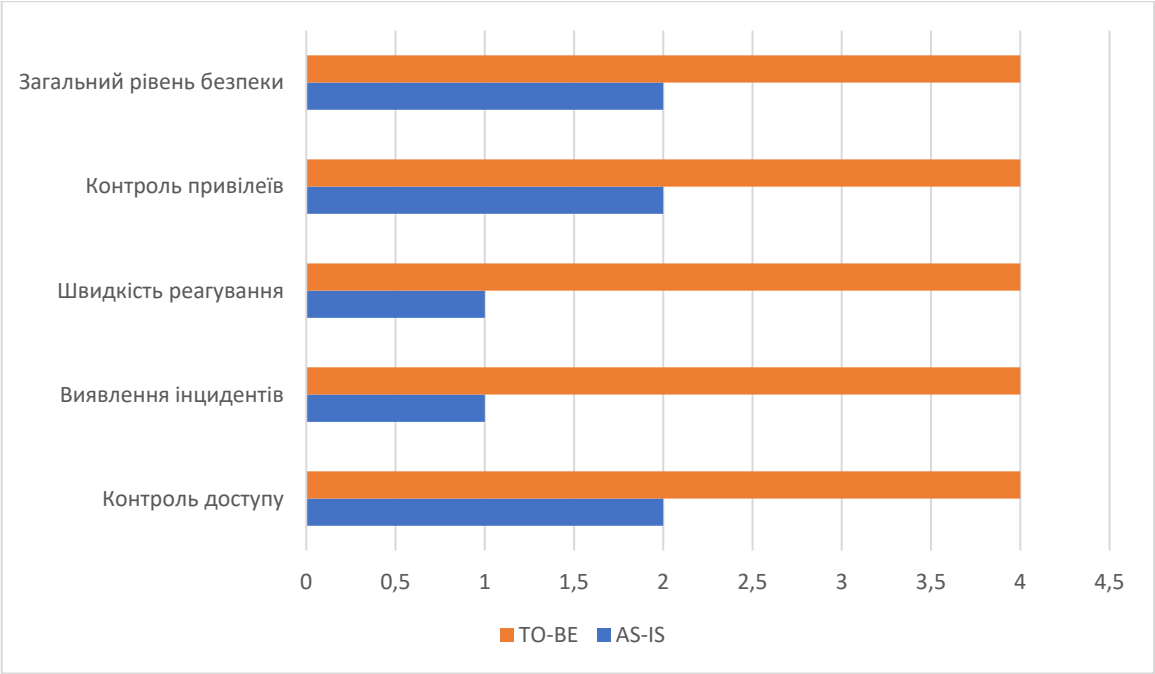


Рис.3.1. - Порівняння рівня безпеки AS-IS та TO-BE

3.4 Архітектура системи автоматизованого контролю безпеки облікових записів

Архітектура системи автоматизованого контролю безпеки облікових записів у системах технічної підтримки визначає взаємодію між компонентами, що забезпечують збір, аналіз та реагування на події інформаційної безпеки. У запропонованій технології архітектура будується за принципом централізованого управління з використанням SIEM-системи як ядра контролю.

Основними компонентами архітектури є джерела подій, система збору та обробки журналів, аналітичний модуль та механізми реагування. До джерел подій належать VPN-шлюзи, сервери операційних систем, системи Service Desk, а також засоби моніторингу мережі. Кожен з цих компонентів генерує журнали подій, які містять інформацію про автентифікацію користувачів, доступ до ресурсів та виконання дій у межах системи.

Центральним елементом архітектури є SIEM-система, яка забезпечує приймання, нормалізацію та зберігання журналів подій. Нормалізація дозволяє привести події з різних джерел до єдиного формату, що є необхідною умовою для

подальшого аналізу та кореляції. Завдяки цьому система може працювати з гетерогенними джерелами даних без втрати контексту подій.

Аналітичний модуль SIEM-системи відповідає за виявлення аномалій та підозрілої активності облікових записів. У межах даного модуля використовуються правила кореляції, порогові значення та елементи поведінкового аналізу. Наприклад, поєднання подій невдалої автентифікації, успішного VPN-підключення та доступу до нетипових ресурсів може бути інтерпретовано як потенційна компрометація облікового запису.

Механізми реагування є завершальним компонентом архітектури системи автоматизованого контролю. Вони реалізують сценарії реагування на інциденти безпеки, які можуть включати сповіщення відповідальних осіб, тимчасове блокування доступу або створення інциденту у системі Service Desk. Такий підхід дозволяє забезпечити швидку реакцію на загрози без необхідності постійного ручного втручання.

Таким чином, запропонована архітектура системи автоматизованого контролю безпеки облікових записів забезпечує комплексний підхід до захисту, що поєднує технічні та організаційні механізми, а також відповідає специфіці роботи систем технічної підтримки.

3.5 Алгоритм функціонування автоматизованого контролю облікових записів

Алгоритм функціонування автоматизованого контролю безпеки облікових записів визначає послідовність дій, що виконуються системою з моменту виникнення події до завершення реагування на інцидент. Формалізація алгоритму дозволяє забезпечити повторюваність процесів та зменшити залежність від людського фактора.

Першим етапом алгоритму є фіксація події безпеки. Подія може бути ініційована спробою автентифікації користувача, встановленням VPN-з’єднання, доступом до сервісів технічної підтримки або мережевою аномалією. Усі події

реєструються відповідними системами та передаються до SIEM-системи для подальшої обробки.

На другому етапі здійснюється аналіз та нормалізація отриманих подій. SIEM-система приводить дані до уніфікованого формату, що дозволяє застосовувати єдині правила аналізу незалежно від джерела події. Паралельно відбувається первинна фільтрація подій з метою відокремлення незначущих записів від потенційно небезпечних.

Третій етап алгоритму передбачає кореляцію подій та виявлення інцидентів безпеки. Окремі події аналізуються у взаємозв'язку між собою з урахуванням часових інтервалів, типу активності та контексту використання облікового запису. У разі виявлення відхилень від нормальної поведінки система формує інцидент безпеки.

Четвертий етап полягає у виборі та виконанні сценарію реагування. Залежно від рівня ризику інциденту можуть застосовуватися різні заходи реагування, зокрема сповіщення адміністратора, тимчасове блокування VPN-доступу або створення заявки в системі Service Desk. Важливою особливістю алгоритму є використання тимчасових обмежень доступу, що дозволяє знизити ризики безпеки без повної зупинки роботи користувача.

Завершальним етапом алгоритму є фіксація результатів реагування та збереження інформації для подальшого аналізу. Дані про інциденти використовуються для аудиту, формування звітів та вдосконалення правил кореляції. Це забезпечує безперервний цикл покращення системи автоматизованого контролю безпеки облікових записів.

Таким чином, запропонований алгоритм функціонування забезпечує чітку та формалізовану модель автоматизованого контролю, яка може бути реалізована на практиці у системах технічної підтримки з використанням сучасних SIEM-рішень.

3.6 Аналіз журналів подій та кореляція в SIEM

Журнали подій є базовим джерелом інформації для систем автоматизованого контролю безпеки. У контексті систем технічної підтримки ключове значення мають журнали VPN-доступу, події автентифікації операційних систем та журнали прикладних сервісів. VPN-журнали містять інформацію про час підключення, IP-адреси, результати автентифікації та використані методи доступу. Аналіз таких даних дозволяє виявляти аномальні спроби входу. SIEM-система Wazuh забезпечує кореляцію подій з різних джерел шляхом нормалізації логів та застосування правил кореляції, що значно підвищує ефективність виявлення інцидентів. Кореляція подій дозволяє об’єднати окремі низькорівневі події у цілісні інциденти безпеки, що зменшує навантаження на персонал та прискорює реагування.

Окрім журналів VPN-доступу, важливим джерелом інформації для аналізу безпеки облікових записів є журнали подій операційних систем. Події автентифікації, зміни прав доступу, запуск привілейованих процесів та спроби доступу до захищених ресурсів дозволяють отримати детальне уявлення про дії користувачів у межах робочих станцій та серверів. У системах технічної підтримки такі журнали є особливо цінними, оскільки співробітники часто працюють з підвищеними привілеями.

Журнали прикладних сервісів, зокрема систем Service Desk та засобів віддаленого доступу, доповнюють загальну картину подій безпеки. Вони містять інформацію про створення та обробку заявок, підключення до клієнтських систем, а також виконання адміністративних дій. Аналіз цих журналів дозволяє співвіднести технічні дії користувача з його посадовими обов’язками та виявити потенційні порушення політик безпеки.

Централізований збір журналів подій у SIEM-системі забезпечує їх уніфікацію та нормалізацію. У процесі нормалізації події з різних джерел приводяться до єдиного формату, що дозволяє застосовувати універсальні правила аналізу та кореляції. Це особливо важливо в гетерогенних середовищах, де

використовуються різні операційні системи, мережеві пристрої та прикладні сервіси.

Кореляція подій у SIEM-системі полягає у виявленні взаємозв'язків між окремими подіями, які на перший погляд можуть не виглядати небезпечними. Наприклад, поєднання кількох невдалих спроб автентифікації, подальшого успішного входу та нетипового VPN-підключення може свідчити про компрометацію облікового запису. Об'єднання таких подій у єдиний інцидент дозволяє значно підвищити точність виявлення загроз.

У SIEM-системі Wazuh кореляція подій реалізується за допомогою набору правил, які враховують тип події, її джерело, часові характеристики та контекст. Гнучкість налаштування правил дозволяє адаптувати систему до специфіки роботи служби технічної підтримки та зменшити кількість хибнопозитивних спрацювань. Це особливо важливо в умовах обмежених ресурсів, коли надмірна кількість сповіщень може перевантажити персонал.

Автоматизований аналіз журналів подій та кореляція в SIEM-системі створюють основу для подальшого впровадження сценаріїв реагування на інциденти. На основі виявлених кореляцій система може ініціювати автоматичні дії, такі як сповіщення відповідальних осіб або тимчасове блокування доступу. Таким чином, аналіз журналів подій є не лише інструментом виявлення загроз, але й ключовим елементом побудови проактивної системи захисту облікових записів.

3.7 Інтеграція SIEM з VPN та хмарним моніторингом

Інтеграція SIEM-системи з VPN-інфраструктурою та засобами хмарного моніторингу є важливим етапом побудови комплексної системи автоматизованого контролю безпеки облікових записів. У системах технічної підтримки VPN використовується як основний механізм віддаленого доступу співробітників до внутрішніх ресурсів організації, що робить його критично важливим елементом з точки зору інформаційної безпеки.

VPN-шлюзи забезпечують реєстрацію великої кількості подій, пов’язаних з автентифікацією користувачів, встановленням та завершенням сесій, використаними криптографічними алгоритмами та параметрами з’єднання. Передача цих подій до SIEM-системи дозволяє здійснювати централізований аналіз доступу до корпоративної мережі та виявляти підозрілі шаблони поведінки. Зокрема, аналіз VPN-логів дає змогу фіксувати спроби підключення з нетипових IP-адрес, багаторазові невдалі спроби автентифікації та аномальну тривалість сесій.

У запропонованій технології SIEM-система використовується як центральний вузол збору та аналізу подій безпеки. Дані з VPN-шлюзу надходять до SIEM у режимі, наближеному до реального часу, що дозволяє оперативно реагувати на потенційні загрози. Кореляція VPN-подій з журналами операційних систем та систем Service Desk створює цілісне уявлення про активність користувачів у межах усієї інфраструктури.

Важливим доповненням до інтеграції з VPN є використання хмарного моніторингу, зокрема системи Zabbix, для збору інформації про стан мережевих сервісів і серверної інфраструктури. Дані хмарного моніторингу дозволяють виявляти мережеві аномалії, перевантаження каналів зв’язку та збої у роботі сервісів, які можуть бути наслідком або супутнім фактором інцидентів інформаційної безпеки.

Інтеграція SIEM з системою хмарного моніторингу дозволяє корелювати події безпеки з технічним станом інфраструктури. Наприклад, різке зростання мережевого трафіку після встановлення VPN-з’єднання може свідчити про несанкціоновану активність або спробу витоку даних. Поєднання таких подій у межах одного інциденту значно підвищує точність аналізу та зменшує кількість хибнопозитивних спрацювань.

Таким чином, інтеграція SIEM-системи з VPN та хмарним моніторингом забезпечує комплексний підхід до контролю безпеки облікових записів, що є особливо важливим для систем технічної підтримки з віддаленим режимом роботи.

Таблиця 3.7.1

Основні джерела журналів подій у SIEM-системі

Джерело подій	**Тип журналів**	**Основні параметри**	**Потенційні загрози**
VPN-шлюз	Журнали підключень	IP-адреса, час сесії, метод автентифікації	Підбір паролів, несанкціонований доступ
Операційні системи	Події автентифікації	Логіни, помилки входу, зміна прав	Компрометація облікового запису
Service Desk	Журнали дій користувачів	Створення заявок, підключення	Зловживання повноваженнями
Хмарний моніторинг	Мережеві події	Навантаження, трафік, збої	Атаки, витік даних

Таблиця 3.7.2

Приклади кореляції подій у SIEM

Подія 1	**Подія 2**	**Подія 3**	**Результат кореляції**
Невдала автентифікація VPN	Успішний вхід	Підключення з іншої IP	Підозра компрометації
VPN-підключення	Різке зростання трафіку	Аномалія в Zabbix	Можливий витік даних
Вхід поза графіком	Доступ до критичних ресурсів	–	Порушення політик

3.8 Забезпечення відповідності вимогам стандартів інформаційної безпеки та аудит

Забезпечення відповідності вимогам міжнародних стандартів інформаційної безпеки є важливою складовою впровадження технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки. У сучасних умовах інформаційна безпека розглядається не лише як сукупність технічних засобів захисту, а як комплексна система управління, що охоплює організаційні, технічні та процедурні заходи.

Одним із ключових міжнародних стандартів у сфері інформаційної безпеки є стандарт ISO/IEC 27001, який визначає вимоги до системи управління інформаційною безпекою організації. Згідно з цим стандартом, особлива увага приділяється управлінню доступом, контролю облікових записів, реєстрації подій безпеки та реагуванню на інциденти. Для систем технічної підтримки, де співробітники працюють з віддаленим доступом та використовують облікові записи з підвищеними привілеями, дотримання цих вимог є критично важливим.

Запропонована у роботі технологія автоматизованого контролю безпеки облікових записів забезпечує виконання основних вимог стандарту ISO/IEC 27001 шляхом впровадження централізованого збору та аналізу журналів подій, використання двофакторної автентифікації та автоматизованого реагування на інциденти. Застосування SIEM-системи дозволяє здійснювати безперервний моніторинг подій автентифікації, VPN-доступу та дій користувачів у системах технічної підтримки.

Окрім стандарту ISO/IEC 27001, у роботі враховано рекомендації NIST Cybersecurity Framework, який визначає п’ять основних функцій кібербезпеки: ідентифікація, захист, виявлення, реагування та відновлення. Запропонована технологія охоплює всі зазначені функції, оскільки передбачає ідентифікацію ризиків, впровадження захисних механізмів доступу, автоматизоване виявлення інцидентів безпеки, оперативне реагування на них та підтримку процесів аналізу і відновлення.

Важливим елементом забезпечення відповідності стандартам інформаційної безпеки є організація процесів аудиту. Аудит дозволяє оцінити ефективність впроваджених заходів захисту, виявити потенційні вразливості та визначити напрями подальшого вдосконалення системи безпеки. У межах запропонованої технології аудит реалізується шляхом централізованого зберігання журналів подій та формування звітів на основі даних SIEM-системи.

Централізований аудит подій безпеки забезпечує прозорість процесів доступу до інформаційних ресурсів та дозволяє відслідковувати дії користувачів у разі виникнення інцидентів. Автоматизоване формування звітів значно спрощує проведення внутрішніх перевірок та підготовку до зовнішніх аудитів відповідності вимогам міжнародних стандартів інформаційної безпеки.

Регулярний аналіз результатів аудиту дає змогу коригувати політики управління обліковими записами, удосконалювати правила кореляції подій та оптимізувати сценарії реагування на інциденти. Таким чином забезпечується безперервний процес підвищення рівня інформаційної безпеки у системах технічної підтримки.

Отже, впровадження технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки забезпечує відповідність вимогам міжнародних стандартів інформаційної безпеки, зокрема ISO/IEC 27001 та рекомендаціям NIST, а також створює ефективну основу для проведення аудиту та подальшого вдосконалення системи захисту.

Таблиця 3.8.1

Відповідність вимог стандарту ISO/IEC 27001 реалізованим заходам безпеки

Розділ ISO/IEC 27001	**Вимоги стандарту**	**Реалізовані заходи у дипломній роботі**	**Засоби та інструменти**
A.5 Політики інформаційної безпеки	Наявність та підтримка політик ІБ	Розробка та документування політик управління обліковими записами	Внутрішні регламенти
A.6 Організація інформаційної безпеки	Розмежування відповідальності	Визначення ролей та прав доступу користувачів	Рольова модель доступу
A.7 Безпека персоналу	Контроль доступу співробітників	Ідентифікація та автентифікація користувачів	Облікові записи, 2FA
A.8 Управління активами	Захист інформаційних ресурсів	Моніторинг доступу до систем технічної підтримки	SIEM, журнали подій
A.9 Контроль доступу	Обмеження та контроль доступу	Використання двофакторної автентифікації	VPN + 2FA
A.10 Криптографія	Захист даних під час передавання	Захищені VPN-з’єднання	Криптографічні протоколи
A.12 Операційна безпека	Реєстрація та аналіз подій	Централізований збір і кореляція журналів	SIEM (Wazuh)
A.13 Безпека мереж	Контроль мережевого доступу	Моніторинг VPN-трафіку та мережевих з’єднань	VPN, Zabbix

Розділ ISO/IEC 27001	Вимоги стандарту	Реалізовані заходи у дипломній роботі	Засоби та інструменти
A.16 Управління інцидентами	Реагування на інциденти безпеки	Сповіщення та тимчасове блокування доступу	SIEM, Service Desk
A.18 Відповідність	Проведення аудиту та контролю	Внутрішній аудит подій безпеки	Звіти SIEM

3.9 Поведінковий аналіз користувачів у SIEM-системах

Поведінковий аналіз користувачів (User and Entity Behavior Analytics, UEBA) є одним із ключових сучасних підходів до виявлення інцидентів інформаційної безпеки, які не можуть бути ідентифіковані традиційними методами контролю доступу. На відміну від класичних механізмів, що базуються на фіксованих правилах і сигнатурах, поведінковий аналіз зосереджується на вивченні динаміки дій користувачів та виявленні відхилень від їхньої типової активності. У системах технічної підтримки, де персонал працює віддалено, використовує VPN-доступ і засоби віддаленого керування, такий підхід є особливо актуальним.

Основною ідеєю поведінкового аналізу є формування базового профілю нормальної поведінки користувача. Цей профіль створюється на основі історичних даних, що накопичуються у журналах подій операційних систем, VPN-шлюзів, сервісів Service Desk та інших інформаційних систем. До ключових параметрів профілю належать час входу в систему, тривалість сесій, географічне розташування, використовувані пристрої, типи ресурсів, до яких здійснюється доступ, а також характер виконуваних дій. З часом система накопичує достатній обсяг даних для визначення того, що є типовою поведінкою конкретного користувача.

У контексті діяльності служби технічної підтримки поведінковий аналіз дозволяє виявляти широкий спектр потенційних загроз. Наприклад, якщо

співробітник, який зазвичай працює у визначені робочі години, раптово починає здійснювати підключення до корпоративної мережі вночі або у вихідні дні, це може свідчити як про зміну робочого графіка, так і про можливу компрометацію облікового запису. Аналогічно, різка зміна географічного розташування під час VPN-підключення або одночасна активність з різних регіонів є типовими ознаками зловмисної діяльності.

SIEM-системи відіграють ключову роль у реалізації поведінкового аналізу, оскільки вони забезпечують централізований збір, нормалізацію та кореляцію подій з різних джерел. У випадку систем технічної підтримки такими джерелами є журнали автентифікації операційних систем, логи VPN-доступу, події систем віддаленого доступу, а також записи про дії користувачів у системі Service Desk. Об’єднання цих даних у єдиному інформаційному просторі дозволяє отримати цілісне уявлення про активність кожного облікового запису.

Однією з важливих переваг поведінкового аналізу є можливість виявлення внутрішніх загроз та зловживань повноваженнями. У системах технічної підтримки співробітники часто мають розширені права доступу до інфраструктури клієнтів або внутрішніх ресурсів компанії. Навіть у випадку, коли доступ здійснюється з легітимного облікового запису, нетипова послідовність дій, надмірна кількість підключень або доступ до ресурсів, що не відповідають посадовим обов’язкам, можуть свідчити про порушення політик безпеки.

Поведінковий аналіз також ефективний для виявлення атак, пов’язаних із компрометацією облікових даних. У багатьох випадках зловмисники використовують дійсні логіни та паролі, отримані шляхом фішингу або витоку даних, що ускладнює їхнє виявлення традиційними засобами захисту. Однак навіть у таких ситуаціях поведінка зловмисника, як правило, відрізняється від звичної поведінки легітимного користувача. Це може проявлятися у зміні часу активності, спробах швидкого доступу до великої кількості ресурсів або нетипових діях у системах керування.

У рамках запропонованої технології автоматизованого контролю безпеки облікових записів поведінковий аналіз використовується як додатковий рівень захисту, що доповнює традиційні механізми автентифікації та авторизації. Результати аналізу можуть використовуватися для ініціювання автоматизованих дій реагування, таких як підвищення рівня автентифікації, тимчасове блокування доступу або сповіщення відповідальних осіб. Це дозволяє оперативно реагувати на потенційні загрози без необхідності постійного ручного моніторингу.

Важливим аспектом впровадження поведінкового аналізу є зменшення кількості хибнопозитивних спрацювань. Для цього необхідно враховувати контекст діяльності користувачів, зокрема специфіку роботи служби технічної підтримки, можливі зміни робочих графіків та характер виконуваних завдань. Налаштування правил і порогових значень повинно здійснюватися з урахуванням реальних бізнес-процесів, що дозволяє підвищити точність виявлення інцидентів.

Таким чином, поведінковий аналіз користувачів у SIEM-системах є ефективним інструментом підвищення рівня безпеки облікових записів у системах технічної підтримки. Його застосування дозволяє виявляти складні та нетипові загрози, зменшувати вплив людського фактора та забезпечувати проактивний підхід до захисту інформаційних ресурсів організації.

3.10 Оцінювання ризиків компрометації облікових записів

Оцінювання ризиків компрометації облікових записів є фундаментальним етапом побудови ефективної системи інформаційної безпеки в організаціях, що використовують віддалені моделі роботи та системи технічної підтримки. У таких умовах обліковий запис співробітника стає ключовою точкою доступу до інформаційних ресурсів, а його компрометація може призвести до значних фінансових, репутаційних та операційних втрат. Саме тому систематичний аналіз ризиків є необхідною передумовою для впровадження автоматизованих механізмів контролю та реагування.

Ризик компрометації облікового запису визначається як поєднання ймовірності реалізації загрози та величини потенційних наслідків. Ймовірність характеризує те, наскільки часто може виникнути певна загроза, тоді як наслідки відображають масштаб шкоди, яку може зазнати організація у разі успішної атаки. У системах технічної підтримки обидва ці параметри, як правило, мають підвищені значення через розширені права доступу співробітників та постійне використання віддалених каналів зв'язку.

Основними загрозами для облікових записів у системах технічної підтримки є фішингові атаки, атаки методом підбору паролів, використання скомпрометованих облікових даних, а також зловживання внутрішніми повноваженнями. Фішинг залишається одним із найпоширеніших векторів атак, оскільки дозволяє зловмисникам отримати легітимні облікові дані без необхідності технічного злому систем. Атаки підбору паролів, у свою чергу, особливо ефективні у випадках використання слабких або повторно застосованих паролів.

Окрему категорію ризиків становлять внутрішні загрози, пов'язані з навмисними або ненавмисними діями співробітників. У службах технічної підтримки персонал часто має доступ до критично важливих систем клієнтів або внутрішньої інфраструктури компанії. Помилки конфігурації, порушення політик безпеки або навмисне зловживання правами доступу можуть призвести до інцидентів, наслідки яких за масштабом не поступаються зовнішнім атакам.

Для систематичного оцінювання ризиків доцільно використовувати матриці ризиків, які дозволяють класифікувати загрози за рівнем критичності. У такій матриці кожна загроза оцінюється за двома осями: ймовірність реалізації та рівень впливу. Наприклад, компрометація VPN-облікового запису співробітника технічної підтримки може мати середню або високу ймовірність реалізації, але водночас характеризуватися високим рівнем впливу, оскільки надає зловмиснику доступ до внутрішньої мережі організації.

Результати оцінювання ризиків дозволяють визначити пріоритети впровадження заходів захисту. Загрози з високим рівнем ризику повинні бути оброблені в першу чергу шляхом застосування технічних та організаційних засобів

безпеки. До таких заходів належать використання двофакторної автентифікації, впровадження автоматизованого моніторингу подій безпеки, обмеження прав доступу відповідно до принципу найменших привілеїв та регулярний перегляд облікових записів.

SIEM-система відіграє важливу роль у процесі оцінювання ризиків, оскільки забезпечує збір та аналіз інформації про реальні події безпеки. На основі статистики інцидентів, зафіксованих у SIEM, можна коригувати початкові оцінки ризиків, враховуючи фактичну частоту реалізації загроз. Наприклад, якщо система фіксує значну кількість невдалих спроб автентифікації для певної групи користувачів, це може свідчити про підвищений ризик атак підбору паролів.

У рамках запропонованої технології автоматизованого контролю безпеки облікових записів результати оцінювання ризиків використовуються для налаштування правил кореляції та сценаріїв реагування. Для облікових записів із високим рівнем ризику можуть застосовуватися жорсткіші політики контролю, зокрема обов’язкове використання двофакторної автентифікації, зниження порогів спрацювання системи та автоматичне блокування доступу у разі виявлення аномальної активності.

Важливою особливістю процесу оцінювання ризиків є його динамічний характер. Рівень ризику не є статичним і може змінюватися залежно від зовнішніх факторів, таких як поява нових загроз, зміни в архітектурі інформаційних систем або трансформація бізнес-процесів. Тому оцінювання ризиків повинно здійснюватися на регулярній основі з урахуванням актуальної інформації про загрози та вразливості.

Таким чином, оцінювання ризиків компрометації облікових записів є необхідним елементом побудови комплексної системи захисту в службах технічної підтримки. Поєднання формалізованих методів аналізу ризиків із можливостями SIEM-систем дозволяє забезпечити обґрунтоване прийняття рішень щодо впровадження заходів безпеки та підвищити загальний рівень захищеності інформаційних ресурсів організації.

3.11 Організація процесу реагування на інциденти безпеки облікових записів

Організація процесу реагування на інциденти інформаційної безпеки є критично важливим елементом системи автоматизованого контролю облікових записів у службах технічної підтримки. Навіть найефективніші механізми виявлення загроз не забезпечують належного рівня захисту без чітко визначеного та оперативного процесу реагування. Умови віддаленої роботи, використання VPN-доступу та наявність облікових записів з розширеними привілеями зумовлюють необхідність мінімізації часу між моментом виявлення інциденту та вжиттям коригувальних заходів.

Інцидент безпеки облікового запису можна визначити як будь-яку подію або сукупність подій, що свідчать про можливе порушення конфіденційності, цілісності або доступності облікових даних користувача. До таких інцидентів належать багаторазові невдалі спроби автентифікації, підозрілі VPN-підключення, використання облікового запису з нетипових географічних регіонів, а також аномальна активність під час роботи з системами віддаленого доступу. Своєчасне реагування на подібні події дозволяє значно знизити потенційні збитки для організації.

Процес реагування на інциденти повинен бути формалізований у вигляді чітко визначених процедур і сценаріїв дій. Такий підхід забезпечує однаковість реакції на подібні інциденти та зменшує залежність від суб’єктивних рішень окремих фахівців. У сучасних системах управління інформаційною безпекою ці сценарії реалізуються у вигляді playbook-ів, які описують послідовність автоматизованих та ручних дій у відповідь на виявлену загрозу.

У контексті систем технічної підтримки playbook реагування на інциденти безпеки облікових записів може включати кілька основних етапів. Першим етапом є ідентифікація інциденту на основі даних, отриманих із SIEM-системи. Це може бути спрацювання правила кореляції, яке виявляє підозрілу комбінацію подій, наприклад, поєднання невдалих спроб автентифікації з подальшим успішним VPN-підключенням.

Другим етапом є початкове стримування інциденту, метою якого є запобігання подальшому розвитку загрози. На цьому етапі доцільно застосовувати автоматизовані дії реагування, такі як тимчасове блокування облікового запису, примусове завершення активних сесій або обмеження доступу до критичних ресурсів. Автоматизація цих дій дозволяє скоротити час реагування до мінімуму та зменшити вплив людського фактора.

Третій етап передбачає сповіщення відповідальних осіб про виявлений інцидент. Сповіщення можуть надсилатися фахівцям з інформаційної безпеки, адміністраторам систем або керівникам відповідних підрозділів. У системах технічної підтримки доцільно інтегрувати процес реагування з системою Service Desk, що дозволяє автоматично створювати заявку на інцидент та фіксувати всі дії, виконані у межах реагування.

Четвертий етап процесу реагування полягає у детальному аналізі інциденту та усуненні його причин. На цьому етапі фахівці аналізують журнали подій, визначають джерело загрози та оцінюють масштаб можливих наслідків. Залежно від результатів аналізу можуть бути вжиті додаткові заходи, такі як зміна облікових даних, посилення політик автентифікації або коригування правил кореляції у SIEM-системі.

Важливою особливістю ефективного процесу реагування є поєднання автоматизованих і ручних механізмів. Автоматизація дозволяє швидко реагувати на типові інциденти, однак складні або нестандартні ситуації потребують участі фахівців з інформаційної безпеки. Такий підхід забезпечує баланс між швидкістю реагування та якістю прийнятих рішень.

У рамках запропонованої технології автоматизованого контролю безпеки облікових записів особлива увага приділяється налаштуванню порогових значень і умов спрацювання автоматизованих дій. Надто агресивні налаштування можуть призвести до хибнопозитивних блокувань та зниження продуктивності роботи служби технічної підтримки. Тому параметри реагування повинні коригуватися з урахуванням специфіки бізнес-процесів та результатів попередніх інцидентів.

Завершальним етапом процесу реагування є документування інциденту та аналіз отриманого досвіду. Фіксація інформації про інциденти дозволяє формувати базу знань, яка може бути використана для підвищення ефективності системи безпеки в майбутньому. Аналіз тенденцій і повторюваних інцидентів дає змогу виявляти слабкі місця у системі захисту та вживати превентивних заходів.

Таким чином, організація процесу реагування на інциденти безпеки облікових записів є невід'ємною складовою технології автоматизованого контролю у системах технічної підтримки. Поєднання можливостей SIEM-систем, автоматизованих сценаріїв реагування та участі кваліфікованих фахівців дозволяє забезпечити своєчасне виявлення та ефективну нейтралізацію загроз, знижуючи ризики для інформаційних ресурсів організації.

3.12 Масштабування та розвиток системи автоматизованого контролю безпеки облікових записів

Масштабування та подальший розвиток системи автоматизованого контролю безпеки облікових записів є важливими чинниками забезпечення її довгострокової ефективності та відповідності зростаючим потребам організації. У сучасних умовах динамічного розвитку інформаційних технологій служби технічної підтримки постійно стикаються зі збільшенням кількості користувачів, розширенням функціоналу сервісів та ускладненням архітектури інформаційних систем. Це, у свою чергу, призводить до зростання обсягів подій безпеки та підвищення вимог до продуктивності й надійності систем контролю.

Одним із ключових аспектів масштабування є здатність системи ефективно обробляти зростаючі обсяги журналів подій. У службах технічної підтримки джерелами таких подій є VPN-шлюзи, операційні системи робочих станцій і серверів, системи Service Desk, а також засоби віддаленого доступу. Зі збільшенням кількості підключень і сесій віддаленої роботи обсяг логів може зростати

експоненційно, що потребує оптимізації процесів збору, зберігання та аналізу даних.

SIEM-система відіграє центральну роль у забезпеченні масштабованості автоматизованого контролю безпеки. Зокрема, використання розподіленої архітектури дозволяє розділяти навантаження між кількома компонентами системи, такими як агенти збору даних, сервери кореляції та сховища журналів. Такий підхід забезпечує можливість горизонтального масштабування, коли продуктивність системи підвищується шляхом додавання нових вузлів без необхідності кардинальних змін у її архітектурі.

Важливим завданням у процесі масштабування є оптимізація правил кореляції та сценаріїв реагування. Надмірна кількість правил або їх недостатня точність можуть призвести до перевантаження системи та збільшення кількості хибнопозитивних спрацювань. Тому розвиток системи автоматизованого контролю повинен супроводжуватися регулярним аналізом ефективності наявних правил і їх коригуванням відповідно до змін у загрозовому середовищі та бізнес-процесах організації.

Окрему увагу слід приділяти масштабуванню процесів реагування на інциденти. Зі зростанням кількості користувачів і подій безпеки збільшується навантаження на персонал служби інформаційної безпеки. У таких умовах автоматизація реагування стає не просто перевагою, а необхідністю. Розширення набору автоматизованих сценаріїв реагування дозволяє обробляти типові інциденти без залучення фахівців, зосереджуючи їхні зусилля на складніших випадках.

Розвиток системи автоматизованого контролю безпеки також передбачає інтеграцію з новими джерелами даних і сервісами. У міру впровадження нових інформаційних систем або змін у технологічному стеку служби технічної підтримки виникає потреба у включенні додаткових джерел журналів подій до SIEM-системи. Це можуть бути нові платформи віддаленого доступу, хмарні сервіси або системи управління ідентифікацією та доступом. Така інтеграція

дозволяє зберігати цілісність контролю безпеки та уникати появи «сліпих зон» у моніторингу.

Перспективним напрямом розвитку систем автоматизованого контролю є використання методів машинного навчання та штучного інтелекту. Застосування таких методів дозволяє підвищити точність виявлення аномалій та зменшити кількість хибнопозитивних спрацювань. У контексті контролю облікових записів це може включати більш глибокий аналіз поведінкових патернів користувачів, автоматичну адаптацію порогових значень та прогнозування потенційних інцидентів на основі історичних даних.

Разом із технічними аспектами масштабування важливу роль відіграють організаційні чинники. Розвиток системи автоматизованого контролю повинен супроводжуватися оновленням політик інформаційної безпеки, регламентів реагування на інциденти та процедур управління обліковими записами. Навчання персоналу та підвищення рівня обізнаності співробітників щодо питань безпеки є необхідною умовою ефективного використання впроваджених технологій.

У рамках запропонованої технології автоматизованого контролю безпеки облікових записів масштабування розглядається як безперервний процес, що враховує як поточні потреби організації, так і перспективи її розвитку. Такий підхід дозволяє забезпечити гнучкість системи та її здатність адаптуватися до нових викликів у сфері інформаційної безпеки без суттєвих витрат ресурсів.

Таким чином, масштабування та розвиток системи автоматизованого контролю безпеки облікових записів є необхідною умовою її ефективного функціонування в умовах зростання обсягів даних і ускладнення інформаційної інфраструктури. Поєднання масштабованої архітектури SIEM-системи, автоматизації процесів реагування та постійного вдосконалення правил контролю дозволяє забезпечити стійкий рівень безпеки та підтримувати надійний захист облікових записів у системах технічної підтримки.

ВИСНОВКИ

У даній магістерській роботі було розглянуто актуальну науково-практичну задачу підвищення рівня безпеки облікових записів у системах технічної підтримки шляхом впровадження технології автоматизованого контролю. Актуальність теми обумовлена зростанням кількості інцидентів інформаційної безпеки, пов’язаних із компрометацією облікових даних, а також широким використанням віддаленого доступу та VPN-технологій у діяльності сучасних IT-компаній.

У процесі виконання роботи було проаналізовано існуючі підходи до захисту облікових записів, зокрема механізми автентифікації, двофакторної автентифікації та централізованого моніторингу подій безпеки. Проведений аналіз поточного стану інформаційної інфраструктури компанії «IT Лідер» показав наявність низки вразливостей, зумовлених використанням лише парольної автентифікації для VPN-доступу, фрагментарним збором подій безпеки та ручною фіксацією інцидентів, пов’язаних з обліковими записами.

У роботі було сформовано вимоги до системи автоматизованого контролю безпеки облікових записів та побудовано модель загроз і ризиків, що дозволило обґрунтувати доцільність впровадження SIEM-системи та двофакторної автентифікації. На основі аналізу моделей AS-IS та TO-BE запропоновано цільову модель захисту облікових записів, яка забезпечує централізований збір, кореляцію та аналіз подій безпеки з різних джерел інформаційної інфраструктури.

У рамках дослідження розроблено архітектуру технології автоматизованого контролю безпеки облікових записів на базі SIEM-системи Wazuh з інтеграцією VPN-шлюзу FortiGate, системи Service Desk, засобу віддаленого доступу ScreenConnect, хмарної системи моніторингу Zabbix та механізмів двофакторної автентифікації. Запропонована архітектура забезпечує цілісний підхід до моніторингу та реагування на інциденти інформаційної безпеки.

Також було розроблено алгоритм автоматизованого контролю безпеки облікових записів, який охоплює всі основні етапи — від генерації та збору подій

безпеки до їх кореляції, перевірки дотримання політик автентифікації та автоматизованого реагування у вигляді сповіщення відповідальних осіб і тимчасового блокування VPN-облікових записів. Реалізація даного алгоритму дозволяє мінімізувати вплив людського фактору та забезпечити оперативне реагування на інциденти.

Кількісна оцінка ефективності впровадження запропонованої технології підтвердила її практичну доцільність. Зокрема, встановлено суттєве скорочення середнього часу виявлення та реагування на інциденти, зростання частки автоматично виявлених інцидентів до 85–95 %, зниження імовірності несанкціонованого доступу у разі компрометації пароля на 60–80 %, а також зменшення навантаження на персонал технічної підтримки на 40–50 %.

Отримані результати свідчать про те, що впровадження технології автоматизованого контролю безпеки облікових записів є ефективним інструментом підвищення рівня інформаційної безпеки в системах технічної підтримки. Запропоновані рішення можуть бути використані у практичній діяльності IT-компаній, а також можуть слугувати основою для подальших наукових досліджень у сфері автоматизації управління інцидентами інформаційної безпеки.

ДОДАТКИ

Додаток А. Структурна схема архітектури технології автоматизованого контролю безпеки облікових записів

У даному додатку наведено опис структурної схеми архітектури запропонованої технології автоматизованого контролю безпеки облікових записів у системах технічної підтримки. Центральним елементом архітектури є SIEM-система Wazuh, яка забезпечує збір, обробку та кореляцію подій інформаційної безпеки.

До SIEM-системи надходять події від таких компонентів: - VPN-шлюз FortiGate (події автентифікації, успішні та неуспішні VPN-підключення, результати двофакторної автентифікації); - робочі станції та сервери (журнали подій операційної системи Windows, активність локальних облікових записів); - система Service Desk (події автентифікації користувачів, створення та обробка інцидентів); - засіб віддаленого доступу ScreenConnect (події ініціювання та завершення віддалених сесій); - хмарна система моніторингу Zabbix (події мережевих інцидентів та аномалій трафіку).

SIEM-система Wazuh здійснює кореляцію подій та формує інциденти інформаційної безпеки, після чого ініціює автоматизоване реагування у вигляді сповіщення відповідальних осіб та тимчасового блокування VPN-облікових записів. Запропонована архітектура забезпечує централізований та масштабований підхід до контролю безпеки облікових записів.

Додаток Б. Алгоритм автоматизованого контролю безпеки облікових записів (текстова блок-схема)

Алгоритм автоматизованого контролю безпеки облікових записів у системах технічної підтримки може бути поданий у вигляді такої послідовності дій:

1. Початок процесу контролю безпеки.

2. Реєстрація події автентифікації або доступу (VPN, локальний вхід, віддалена сесія).
3. Передача події до SIEM-системи Wazuh.
4. Нормалізація події та перевірка її відповідності правилам кореляції.
5. Аналіз події на наявність ознак інциденту інформаційної безпеки.
6. Перевірка дотримання політик безпеки та проходження двофакторної автентифікації.
7. У разі відсутності порушень — завершення обробки події.
8. У разі виявлення інциденту — формування сповіщення відповідальних осіб.
9. Тимчасове блокування відповідного VPN-облікового запису.
10. Фіксація інциденту в SIEM та створення заявки в Service Desk.
11. Завершення процесу контролю безпеки.
12.

Додаток В. Порівняльна таблиця показників ефективності (AS-IS / TO-BE)

У таблиці наведено основні показники ефективності системи контролю безпеки облікових записів до та після впровадження запропонованої технології.

- Середній час виявлення інциденту (MTTD): AS-IS — 8–24 год, TO-BE — 5–10 хв.
- Середній час реагування на інцидент (MTTR): AS-IS — понад 24 год, TO-BE — 10–20 хв.
- Частка автоматично виявлених інцидентів: AS-IS — 20–30 %, TO-BE — 85–95 %.
- Імовірність несанкціонованого доступу при компрометації пароля: AS-IS — висока, TO-BE — знижена на 60–80 %.
- Рівень ручного навантаження на персонал: AS-IS — високий, TO-BE — знижений на 40–50 %

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. — Київ : ДП «УкрНДНЦ», 2016.
2. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Кодекс практики для засобів контролю інформаційної безпеки. — Київ : ДП «УкрНДНЦ», 2016.
3. ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management.
4. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. — NIST, 2020.
5. NIST Special Publication 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. — NIST, 2022.
6. Stallings W. Network Security Essentials: Applications and Standards. — 6th ed. — Pearson, 2017.
7. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. — 3rd ed. — Wiley, 2020.
8. Behl A., Behl K. Cyberwar: The Next Threat to National Security and What to Do About It. — Oxford University Press, 2017.
9. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). — NIST SP 800-94.
10. Kent K., Souppaya M. Guide to Computer Security Log Management. — NIST SP 800-92.
11. Wazuh Documentation. SIEM and XDR Platform Overview. — Wazuh Inc., 2024.
12. Wazuh Documentation. Log Data Analysis and Correlation Rules. — Wazuh Inc., 2024.

13. Fortinet Documentation. FortiGate VPN Security Guide. — Fortinet, 2024.

14. Fortinet Documentation. FortiClient Administration Guide. — Fortinet, 2024.

15. Fortinet Documentation. Two-Factor Authentication Configuration. — Fortinet, 2024.

16. Elastic. SIEM Architecture and Event Correlation Concepts. — Elastic Documentation.

17. Splunk Inc. Security Information and Event Management Fundamentals. — Splunk Whitepaper.

18. Chuvakin A., Schmidt K., Phillips C. Logging and Log Management. — Syngress, 2013.

19. Peltier T. Information Security Policies, Procedures, and Standards. — Auerbach, 2016.

20. Zabbix Documentation. Monitoring Network Traffic and Security Events. — Zabbix LLC, 2024.

21. Zabbix Documentation. Cloud-Based Monitoring Architecture. — Zabbix LLC, 2024.

22. OWASP Foundation. Authentication Cheat Sheet. — OWASP, 2023.

23. OWASP Foundation. Credential Stuffing Prevention. — OWASP, 2023.

24. OWASP Foundation. Security Logging and Monitoring Failures. — OWASP Top 10, 2021.

25. Sommerville I. Software Engineering. — 10th ed. — Pearson, 2016.

26. Pressman R. Software Engineering: A Practitioner’s Approach. — 8th ed. — McGraw-Hill, 2015.

27. Bishop M. Computer Security: Art and Science. — Addison-Wesley, 2019.

28. Pfleeger C., Pfleeger S., Margulies J. Security in Computing. — 5th ed. — Pearson, 2015.

29. RFC 4301. Security Architecture for the Internet Protocol.

30. RFC 5246. The Transport Layer Security (TLS) Protocol.

31. **ISO/IEC 27001 Information Security Management** https://www.iso.org/isoiec-27001-information-security.html (дата звернення: 25.12.2025)

32. **NIST Cybersecurity Framework** https://www.nist.gov/cyberframework (дата звернення: 25.12.2025)

33. **Wazuh – Open Source Security Platform** https://wazuh.com (дата звернення: 25.12.2025).

34. **Fortinet VPN Solutions** https://www.fortinet.com/products/vpn (дата звернення: 25.12.2025).

35. **OWASP Top 10 Security Risks** https://owasp.org/www-project-top-ten/ (дата звернення: 25.12.2025).

36. **Zabbix Documentation** https://www.zabbix.com/documentation (дата звернення: 25.12.2025).

37. **IBM Security – SIEM Solutions** https://www.ibm.com/security/siem (дата звернення: 25.12.2025).

38. **Google Cloud – Identity and Access Management** https://cloud.google.com/iam/docs/overview (дата звернення: 25.12.2025).

Демонстраційні матеріали(Презентація)

Об'єкт дослідження – процеси забезпечення інформаційної безпеки облікових записів

Предмет дослідження – методи та засоби автоматизованого контролю

2

Мета роботи розробка технології автоматизованого контролю безпеки облікових записів

Наукові завдання:

- Аналіз загроз безпеці облікових записів
- Дослідження систем технічної підтримки-
- Розробка алгоритму автоматизованого контролю
- Розробка алгоритму автоматизованого контролю
- Експериментальна перевірка ефективності

Апробація результатів Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

Розділ 1. Теоретичні засади безпеки облікових записів

3

1. Облікові записи є ключовим елементом контролю доступу в інформаційних системах

2. Системи технічної підтримки використовують облікові записи з підвищеними правами

3. Основні загрози: компрометація паролів, несанкціонований віддалений доступ, людський фактор

4. Використання лише парольної автентифікації є недостатнім для сучасних умов

4. Підвищення рівня безпеки потребує автоматизованого контролю, моніторингу подій та застосування двофакторної автентифікації

У першому розділі обґрунтовано актуальність проблеми безпеки облікових записів у системах технічної підтримки та необхідність автоматизації контролю доступу

Розділ 2. Аналіз поточного стану (ASIS)

4

1. Доступ до систем технічної підтримки здійснюється через VPN

2. Використовується переважно парольна автентифікація

3. Інциденти безпеки облікових записів фіксуються вручну

4. Відсутній централізований аналіз та кореляція подій

5. Час реагування залежить від людського фактора та є надмірним

Другий розділ показує, що поточна модель контролю доступу є недостатньо ефективною та потребує автоматизації

Розділ 3. Розробка технології та результати (TCBE)

5

Запропоновано технологію автоматизованого контролю безпеки облікових записів

Реалізовано загальний алгоритм контролю доступу та реагування на інциденти

Використано SIEM-систему та двофакторну автентифікацію

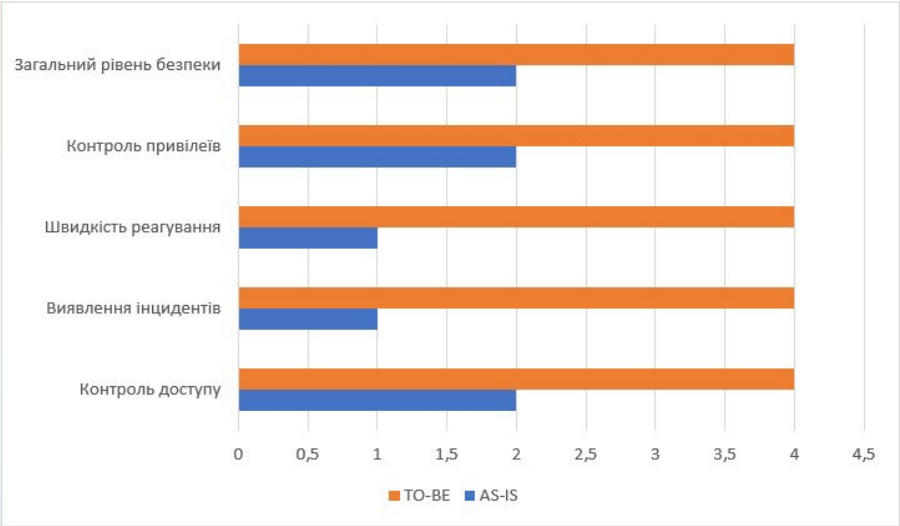
Проведено експериментальну перевірку ефективності рішення

Отримано скорочення часу реагування та зниження ризиків безпеки

У третьому розділі розроблено та експериментально підтверджено ефективність запропонованої технології

Порівняння рівня безпеки AS-IS та TO-BE

6



Розроблення рекомендацій щодо застосуваннятехнології автоматизованого контролю безпеки облікових записіву системах технічної підтримки

7

Використовувати централізований збір та аналіз подій безпеки

Застосовувати двофакторну автентифікацію для критичних облікових записів

Застосовувати двофакторну автентифікацію для критичних облікових записів

Обмежувати привілеї доступу відповідно до ролей користувачів

Регулярно проводити аудит та оновлення політик безпеки

Запропоновані рекомендації забезпечують підвищення рівня безпеки облікових записів за рахунок автоматизованого контролю та реагування

ВИСНОВКИ

1. Запропонована технологія забезпечує комплексний контроль безпеки облікових записів
2. Інтеграція SIEM дозволяє централізовано виявляти та аналізувати інциденти безпеки
3. Застосування UAM Syteca підвищує рівень внутрішньої безпеки та контроль дій користувачів
4. Автоматизоване реагування зменшує час реагування та вплив людського фактора
5. Рішення є практично доцільним та готовим до впровадження

Запропонована технологія дозволяє підвищити рівень безпеки облікових записів за рахунок автоматизації контролю та реагування на інциденти

Дякую за увагу!
Доповідь закінчено