ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:
«Дослідження шляхів та розроблення рекомендацій щодо захисту від інсайдерських атак на основі Device LockDLP»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Поліщук А.С.
(прізвище та ініціали)
Керівник Марченко В.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Поліщуку Артему Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розроблення рекомендацій щодо захисту від інсайдерських атак на основі Device LockDLP»
керівник бакалаврської роботи Марченко Віталій Вікторович, ст. викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24» лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
корпоративна інформаційна система;
програмний комплекс DLP;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Вступ
2. Аналіз засобів та методів від інсайдерських атак
2.1 Поняття інсайдерської атаки та її видів:
2.2 Причини та наслідки інсайдерських атак:
2.3 Методи виявлення інсайдерських атак
2.4 Методи за засоби захисту від інсайдерських атак

2.5 Визначення потреби в додаткових заходах захисту

2.6 Аналіз вразливостей інформаційної системи

2.7 Основні потенційні вразливості інформаційних систем:

2.8 Аналіз можливих шляхів зламу системи внутрішніми користувачами

3. Дослідження методів за засобів захисту від інсайдерських атак

3.1 Device Lock DLP

3.2 Рекомендації

5. Перелік графічного матеріалу
(презентація)

6. Дата видачі завдання 24.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми інсайдерських атак.	24.02.2023 р.	
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	25.02.2023 р.	
3.	Аналіз методів та засобів захисту від інсайдерських атак.	4.03.2023 р.	
4.	Розроблення рекомендацій щодо застосування методів та засобів захисту від інсайдерських атак.	15.03.2023 р.	
5.	Оформлення результатів дослідження.	22.05.2023 р.	
6.	Підготовка доповіді до захисту.	29.05.2023 р.	

Студент _____ Поліщук А.С.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на бакалаврську роботу

студента Поліщука Артема Сергійовича
на тему: «Дослідження шляхів та розроблення
рекомендацій щодо захисту від інсайдерських атак на основі Device LockDLP»

Актуальність: Інсайдери можуть зловживати своїми повноваженнями та надавати несанкціонований доступ до конфіденційної інформації, що може призвести до серйозних наслідків, включаючи витоки даних, фінансові збитки, репутаційні втрати та інші проблеми.

Тому розробка ефективних методів та заходів захисту від інсайдерських атак є критично важливою задачею для бізнесу та урядових установ. Програма Acronis Device Lock DLP та інші заходи захисту від інсайдерських атак можуть допомогти зменшити ризики та запобігти несанкціонованому доступу до конфіденційної інформації.

Позитивні сторони:

1. У бакалаврській роботі було проведено дослідження та визначено потребу в захисті від інсайдерських атак, що є важливим для бізнесу в епоху цифрової трансформації.

2.Автор досліджував різні методи та засоби захисту від інсайдерських атак та проводив експерименти з використанням програми Acronis Device Lock DLP, що свідчить про практичну спрямованість роботи.

3. Робота містить чіткі та змістовні висновки, а також рекомендації щодо захисту від інсайдерських атак.

Недоліки:

1. Робота могла б містити більше порівняльного аналізу різних програм та технологій захисту від інсайдерських атак.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **відмінно**, а студент **Поліщук А.С.** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Поліщук А.С. до захисту бакалаврської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Дослідження шляхів та розроблення рекомендацій щодо застосування засобів багатовимірного візуального аналізу під час розслідування кіберінцидентів».
Бакалаврська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Поліщук А.С. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Берестяна Т.В

Секретар інституту, факультету (відділення) _____
(підпис)

Висновок керівника бакалаврської роботи

Студент ***Поліщук А.С.*** обрав тему роботи, метою якої було дослідження шляхів та розроблення рекомендацій щодо захисту від інсайдерських атак на основі Device LockDLP. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Поліщук А.С. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану бакалаврську роботу студента Поліщука Артема Сергійовича на оцінку **«відмінно»** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека .

Керівник бакалаврської роботи _____ Марченко В.В.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Поліщук А.С.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2023 року

РЕФЕРАТ

Текстова частина бакалаврської роботи: 54 сторінок, 19 рисунків, 1 таблиця, 29 джерел.

Об'єкт дослідження: захист інформації від інсайдерських атак.

Предмет дослідження: програма Acronis Device Lock DLP.

Мета роботи: дослідити шляхи та розробити рекомендації щодо захисту від інсайдерських атак на основі програми Acronis Device Lock DLP.

Методи дослідження: аналіз наукової літератури, аналіз результатів, порівняльний аналіз, опрацювання літератури за даною темою, аналіз експлуатаційної документації.

В бакалаврській роботі приведено основні відомості про інсайдерські атаки. Методи та засоби захисту від них.

Обґрунтовано важливість захисту від інсайдерських атак.

Проаналізовано різні види загроз та наведено їх класифікацію.

Досліджено методи та засоби захисту персональної та конфіденційної інформації від інсайдерських атак.

Розроблено рекомендації щодо щодо захисту від інсайдерських атак.

Галузь використання – інформаційна безпека.

ВРАЗЛИВОСТІ, ЗАХИСТ ДАНИХ, ВПЛИВ НА ІНФОРМАЦІЮ, ПЕРСОНАЛЬНА ТА КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ

ЗМІСТ

ВСТУП

Інформаційна безпека є найважливішою складовою функціонування будь-якої організації, що займається обробкою інформації. Однак, не тільки зовнішні загрози можуть погрожувати інформаційній безпеці, але й внутрішні – інсайдерські атаки. Інсайдерська атака – це злочинні дії особи, яка має легальний доступ до інформаційних ресурсів організації, з метою їх зловживання або використання в особистих цілях.

Предмет дослідження*:* програма Acronis Device Lock DLP.

Актуальність теми дослідження полягає в тому, що інсайдерські атаки можуть призвести до серйозних фінансових втрат, порушення бізнес-процесів та втрати довіри клієнтів. Тому дослідження шляхів та розробка рекомендацій щодо захисту від інсайдерських атак є важливою задачею для будь-якої організації.

Мета дослідження – дослідити шляхи захисту від інсайдерських атак та розробити рекомендації щодо їх застосування.

Завдання дослідження:

1. Вивчити теоретичні аспекти інсайдерських атак.
2. Проаналізувати вразливості інформаційної системи.
3. Розробити методи захисту від інсайдерських атак.
4. Розробити рекомендації щодо захисту від інсайдерських атак.

Методи дослідження*:* аналіз наукової літератури, аналіз результатів, порівняльний аналіз, опрацювання літератури за даною темою, аналіз експлуатаційної документації.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на конференції.

Науково-практична конференція «цифрова трансформація кібербезпеки», навчально-наукового інституту захисту інформації, 27 квітня 2023 р.

1 АНАЛІЗ ЗАСОБІВ ТА МЕТОДІВ ВІД ІНСАЙДЕРСЬКИХ АТАК

Інсайдерська атака є однією з найбільш складних викликів, з якими зіштовхуються організації у забезпеченні безпеки своєї інформації. Інсайдерська атака відбувається, коли працівник організації, який має легальний доступ до конфіденційної інформації, використовує цей доступ для зловживання чи збирання інформації зі своїх власних особистих мотивів. Інсайдерські атаки можуть призвести до втрати конфіденційної інформації, фінансових втрат, втрати довіри клієнтів та інших наслідків.

1.1 Поняття інсайдерської атаки та її видів:

Інсайдерська атака - це злочинні дії, що вчиняються особами з внутрішньою доступністю до інформаційної системи, з метою зловживання або використання конфіденційної інформації в особистих цілях. Існують два види інсайдерських атак: активна та пасивна [5].

Активна інсайдерська атака - це випадки, коли працівник організації зловживає своїми повноваженнями та вчиняє дії, які завдають шкоди інформаційній системі. Наприклад, працівник може зламати систему безпеки та отримати доступ до конфіденційної інформації або видалити важливі дані.

Пасивна інсайдерська атака - це випадки, коли працівник організації отримує конфіденційну інформацію, не вчиняючи активних дій, які можуть завдати шкоди організації. Наприклад, працівник може неправильно зберігати чутливу інформацію або не захистити свій пристрій з інформацією від несанкціонованого доступу.

1.2 Причини та наслідки інсайдерських атак:

Існує безліч факторів, які можуть призвести до виникнення інсайдерських атак. До основних причин можна віднести [5]:

- Недостатній рівень кваліфікації працівників у питаннях безпеки інформації;
- Недостатня увага до заходів забезпечення безпеки інформації в організації;
- Фінансові труднощі або недовіра до організації;
- Особисті мотиви, такі як ревнощі, бажання влади або бажання збагатитися.
- Втрати конфіденційної інформації;
- Порушення інтелектуальної власності;
- Зниження довіри клієнтів та партнерів;
- Фінансові втрати внаслідок зловживань та викрадень;
- Пошкодження репутації організації.

Інсайдерські атаки можуть мати різні форми прояву, включаючи крадіжку даних, втручання у роботу системи, неправомірну розкриття інформації та інші. Відновлення даних та систем, а також відновлення довіри партнерів та клієнтів можуть зайняти значний час та кошти. Тому захист від інсайдерських атак є дуже важливим завданням для будь-якої організації.

1.3 Визначення потреби в додаткових заходах захисту

Для визначення потреби в додаткових заходах захисту від інсайдерських атак необхідно провести оцінку загроз та ризиків. Для цього можна використовувати методологію оцінки загроз та ризиків, таку як методологію ISO 27005 або методологію NIST SP 800-30 [5].

У процесі оцінки загроз та ризиків, можна виявити потенційні

вразливості в системі та ідентифікувати можливі наслідки інсайдерських атак. Наприклад, можуть бути виявлені ризики несанкціонованого доступу до конфіденційної інформації, втрати даних або порушення робочих процесів.

Після оцінки загроз та ризиків, можна визначити необхідність додаткових заходів захисту, таких як [5]:

Встановлення більш жорстких політик паролів, які вимагатимуть від користувачів використання складних паролів та їх регулярну зміну.

Використання системи моніторингу активності користувачів з можливістю виявлення підозрілих дій або несподіваної активності.

Впровадження двофакторної автентифікації для підвищення рівня захисту від несанкціонованого доступу до системи.

Застосування криптографічних методів захисту даних для забезпечення їх конфіденційності та цілісності.

Встановлення системи контролю доступу до ресурсів системи та моніторингу прав доступу користувачів.

Регулярне проведення тренінгів та навчання користувачів щодо безпеки інформації та захисту від інсайдерських атак.

Впровадження процедур перевірки та аудиту системи для виявлення можливих вразливостей.

1.4 Аналіз вразливостей інформаційної системи

У цьому розділі дослідження буде проведено аналіз вразливостей інформаційної системи, що можуть бути використані для проведення інсайдерських атак. Для цього будуть визначені потенційні вразливості системи та проведений аналіз можливих шляхів зламу системи внутрішніми користувачами.

Опис інформаційної системи та її функцій [5]

Перед проведенням аналізу вразливостей системи, необхідно детально описати інформаційну систему та її функції. У даному дослідженні буде розглянута інформаційна система компанії, що містить конфіденційну інформацію про клієнтів та фінансові операції. Система забезпечує доступ до цієї інформації внутрішнім користувачам компанії, таким як фінансові аналітики, адміністратори баз даних, менеджери та інші.

Система має декілька модулів, включаючи модуль бази даних, модуль зберігання файлів та модуль управління доступом. База даних містить інформацію про клієнтів, їхні фінансові операції та інші конфіденційні дані. Модуль зберігання файлів дозволяє зберігати та обмінюватися файлами між внутрішніми користувачами компанії. Модуль управління доступом забезпечує контроль доступу до системи та її модулів.

1.5 Основні потенційні вразливості інформаційних систем:

Вразливості в програмному забезпеченні. Це можуть бути недоліки в коді програм або програмні баги, які можуть бути використані для злому системи. Такі вразливості можуть бути виявлені інсайдерами або зловмисниками, які використовують вразливі місця програм для незаконного доступу до системи.

Вразливості в мережевому забезпеченні. Це можуть бути проблеми з безпекою мережі, які можуть дозволити зловмисникам отримати доступ до системи. Такі вразливості можуть бути використані для перехоплення даних або для введення зловмисного коду.

Вразливості в людському факторі. Це можуть бути недоліки в системах управління доступом, які дозволяють зловмисникам отримати доступ до системи з допомогою соціальної інженерії або зловживанням довіри співробітників.

Вразливості в апаратному забезпеченні. Це можуть бути проблеми з безпекою комп'ютерів або інших пристроїв, які можуть бути використані для злому системи. Наприклад, зловмисники можуть використовувати фізичний доступ до комп'ютера для виконання зловмисних дій.

Аналіз потенційних вразливостей системи та визначення можливих шляхів зламу є важливою частиною дослідження, оскільки це дозволяє виявити недоліки у захисті системи та розробити стратегії їх усунення. [7]

1.6 Аналіз можливих шляхів зламу системи внутрішніми користувачами

Інсайдерські атаки можуть бути здійснені через різні шляхи, тому важливо проаналізувати можливі шляхи злому інформаційної системи внутрішніми користувачами. Деякі з таких шляхів можуть включати [8]:

Використання власних облікових записів: Зловмисники можуть використовувати власні облікові записи з правами доступу до конфіденційної інформації.

Використання скомпрометованих облікових записів: Зловмисники можуть використовувати облікові записи, які були скомпрометовані під час попередніх атак або завдяки необережному поводженню користувачів.

Використання слабких паролів: Зловмисники можуть складати переліки можливих паролів або використовувати програмні засоби для перебору паролів.

Використання шпигунського програмного забезпечення: Зловмисники можуть встановлювати шпигунське програмне забезпечення на комп'ютери в організації для збору конфіденційної інформації.

Фішинг: Зловмисники можуть використовувати фішингові атаки для отримання доступу до облікових записів користувачів.

Соціальна інженерія: Зловмисники можуть використовувати соціальну інженерію для переконання користувачів у наданні доступу до конфіденційної інформації.

Використання USB-носіїв: Зловмисники можуть використовувати USB-носії для крадіжки конфіденційної інформації або введення шкідливого програмного забезпечення.

Висновок до розділу 1:

В даній частині дипломної роботи було проведено дослідження засобів та методів захисту від інсайдерських атак. Було розглянуто поняття інсайдерської атаки, її види, причини та наслідки. Досліджено методи виявлення інсайдерських атак, методи захисту від них та визначено потребу в додаткових заходах захисту. Також було проведено аналіз вразливостей інформаційної системи та основні потенційні вразливості, а також аналіз можливих шляхів зламу системи внутрішніми користувачам

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗА ЗАСОБІВ ЗАХИСТУ ВІД ІНСАЙДЕРСЬКИХ АТАК

Продукти на основі UEBA

Exabeam - це платформа, яка використовує машинне навчання та аналітику для виявлення незвичайної поведінки користувачів та сутностей в комп'ютерних системах.

Splunk - Splunk використовує UEBA для аналізу поведінки користувачів та виявлення загроз безпеці в реальному часі.

Rapid7 - це рішення, яке використовує UEBA для виявлення аномальної поведінки, що може вказувати на компрометацію системи або крадіжку даних.

Securonix - це платформа, яка використовує UEBA для аналізу даних в режимі реального часу та виявлення незвичайної поведінки, яка може вказувати на загрози безпеці.

IBM QRadar - це продукт, який використовує UEBA для аналізу великих обсягів даних та виявлення аномальної поведінки, яка може вказувати на компрометацію системи або крадіжку даних.

Продукти на основі DLP

Symantec Data Loss Prevention - це рішення для захисту даних, яке надає комплексний підхід до контролю за даними, включаючи контроль за мережевим трафіком, файлами та електронною поштою.

McAfee Data Loss Prevention - це інша популярна система захисту даних, яка надає засоби для моніторингу вихідного трафіку, контролю за веб-додатками, файлами та друкуванням.

Forcepoint DLP - це рішення для захисту даних, яке надає засоби для

виявлення та захисту конфіденційної інформації, зокрема, контролю за вихідним трафіком, файлами, електронною поштою та іншими каналами.

Digital Guardian - це інша система захисту даних, яка надає засоби для моніторингу вихідного трафіку, захисту файлів та даних на кінцевих пристроях, контролю доступу та аудиту.

Ці продукти на основі DLP дозволяють організаціям захистити свою конфіденційну інформацію від витоків даних та неправомірного використання. Вони надають різноманітні інструменти для моніторингу та контролю за даними, що дозволяє організаціям забезпечити безпеку своєї інформації та відповідати вимогам законодавства.

2.1 Методи виявлення інсайдерських атак:

Існує декілька методів виявлення інсайдерських атак, серед них [2]:

Моніторинг діяльності користувачів - цей метод полягає у відстеженні активності користувачів та аналізі їх поведінки на системі. Можна використовувати спеціальні інструменти, що дозволяють виявляти аномальні дії користувачів.

Аналіз журналів - збір журналів системи та їх аналіз можуть допомогти виявити неправомірні дії користувачів, такі як намагання отримати доступ до конфіденційної інформації або змінити налаштування системи.

Використання технологій машинного навчання - цей метод полягає в розробці моделей машинного навчання, що дозволяють виявляти аномальні дії користувачів. Наприклад, можна навчити модель розпізнавати типові дії користувачів та виявляти аномалії, які можуть бути пов'язані з інсайдерською атакою.

Використання систем детекції вторгнень - такі системи дозволяють виявляти незвичну активність користувачів та інші ознаки можливої

інсайдерської атаки.

Використання експертів - експерти з кібербезпеки можуть проводити аудит системи та досліджувати підозрілі активності користувачів. Їх досвід та знання можуть допомогти виявити інсайдерську атаку.

Кожен з цих методів має свої переваги та недоліки, тому оптимальний варіант виявлення інсайдерської атаки зазвичай полягає в комплексному підході, використовуючи декілька методів одночасно.

Огляд існуючих заходів захисту від інсайдерських атак:

Існує безліч заходів захисту від інсайдерських атак, які можуть бути реалізовані на різних рівнях, від технічних до організаційних. Деякі з них включають:

Організаційні заходи - це може включати створення правил та процедур для користувачів, навчання користувачів про те, як діяти у випадку виявлення підозрілої активності та зміцнення контролю над користувачами, які мають доступ до конфіденційної інформації.

Встановлення систем контролю доступу - це може включати використання механізмів автентифікації та авторизації, що дозволяють контролювати доступ користувачів до різних ресурсів та обмежувати їх можливості.

Захист мережі - це може включати використання мережевих механізмів захисту, таких як файрволи, інтрусіонні системи детекції та запобігання вторгненням, віртуальні приватні мережі (VPN) та ін.

Захист даних - це може включати використання шифрування даних, управління ключами, контролю доступу до файлів та мережевих ресурсів, збереження резервних копій даних та ін.

Моніторинг та виявлення - це може включати використання систем моніторингу, які виявляють підозрілу активність користувачів, аналізують

журнали та інші дані, щоб виявляти ознаки інсайдерської атаки.

DLP система (англ. Data Loss Prevention system) - це комплекс технологій та інструментів, що призначений для запобігання втрати конфіденційної інформації організації або її неправомірному використанню.

Такі системи мають різноманітні можливості, серед яких можна виділити:

Моніторинг вихідного трафіку: система аналізує мережевий трафік, що виходить з комп'ютера чи мережі, та перевіряє його на наявність конфіденційної інформації, наприклад, кредитних карток, персональних даних, важливих документів тощо. Якщо система виявляє таку інформацію, вона може зупинити передачу даних та повідомити про це адміністратора;

Аналіз файлів: система може аналізувати файли на наявність конфіденційної інформації та управляти правами доступу до цих файлів;

Контроль доступу: система може встановлювати правила доступу до інформації на основі ролей користувачів, часу, місця тощо;

Аудит: система може збирати та зберігати журнали дій користувачів з конфіденційною інформацією для подальшого аналізу.

DLP системи є важливим інструментом для захисту конфіденційної інформації, що допомагає організаціям запобігати витокам даних та неправомірному використанню конфіденційної інформації.

UEBA означає "User and Entity Behavior Analytics". UEBA заснована на машинному навчанні та аналізі даних з метою ідентифікації аномальних моделей поведінки, які можуть бути пов'язані з кібератаками, витоками даних або іншими загрозами безпеці.

UEBA аналізує не тільки дії користувачів, але й поведінку різних сутностей в комп'ютерних системах, таких як програми, пристрої та сервіси. Вона забезпечує пошук аномалій у поведінці, які можуть вказувати на загрози

безпеці, такі як несподівана активність на рівні мережі, вивантаження даних на зовнішніх серверах або використання даних у незвичайний спосіб.

UEBA може використовуватися як додатковий інструмент в системах безпеки, що доповнює традиційні методи захисту, такі як вогнепровіди, антивірусні програми.

2.2 Методи за засоби захисту від інсайдерських атак

Для захисту від інсайдерських атак можна використовувати наступні методи [4]:

1. Розробка системи контролю доступу до інформації та ресурсів системи: необхідно розробити політику контролю доступу, яка визначає права доступу користувачів до різних ресурсів системи. Також можна використовувати принцип найменших привілеїв, який обмежує доступ користувачів до функцій та ресурсів, які не є необхідними для їх роботи.

Система контролю доступу має включати такі компоненти, як:

Автентифікація користувачів. Цей процес включає перевірку ідентифікаційної інформації користувача, такої як логін та пароль, та забезпечує доступ до системи тільки користувачам з вірними автентифікаційними даними.

Авторизація користувачів. Після того, як користувач пройшов процес автентифікації, система повинна перевірити, які ресурси та функції він може використовувати в системі. Це забезпечується за допомогою ролей користувачів та налаштування прав доступу.

Моніторинг доступу до ресурсів. Система моніторингу повинна реєструвати кожен доступ користувачів до ресурсів системи. Це дозволяє виявляти недопустимі дії користувачів та вчасно реагувати на них.

Аудит системи. Система повинна збирати та аналізувати дані про всі події, пов’язані з доступом користувачів до ресурсів системи. Це дозволяє виявляти та реагувати на порушення безпеки.

Розробка системи контролю доступу повинна бути індивідуальною для кожної інформаційної системи та враховувати її конкретні особливості та вимоги до безпеки.

2. Використання системи моніторингу активності користувачів: система моніторингу дозволяє виявляти незвичні активності користувачів, які можуть свідчити про можливі інсайдерські атаки. Наприклад, система може сповістити про зміну частоти та обсягу даних, які надсилає користувач.

Використання системи моніторингу активності користувачів є ефективним методом виявлення незвичних або підозрілих дій в системі, що можуть свідчити про інсайдерську атаку. Це дозволяє оперативно втручатися в події та зупиняти несанкціоновану діяльність. Система моніторингу може фіксувати дії користувачів, такі як спроби невдалого входу в систему, використання незвичних команд, зміну прав доступу до файлів та інші підозрілі дії.

Окрім того, використання системи моніторингу може бути корисним при розслідуванні інцидентів, які сталися в минулому. Зберігання лог-файлів дозволяє провести аналіз та встановити, як саме сталася інсайдерська атака та хто є винуватцем.

Проте, варто враховувати, що використання системи моніторингу може стати проблемою з точки зору конфіденційності та приватності користувачів. Отже, перед використанням системи необхідно розробити політику використання, яка забезпечить відповідність правилам захисту даних та захистить приватні дані користувачів від неправомірного використання.

3. Впровадження процедур автентифікації та авторизації користувачів: це дозволяє перевірити, що користувач, який намагається отримати доступ до системи, є легітимним користувачем та має відповідні права доступу до необхідних ресурсів системи.

Для забезпечення безпеки системи, користувачі повинні бути перевірені на наявність прав доступу до системи та на конкретні ресурси в системі. Для цього можна використовувати різні методи автентифікації та авторизації, такі як:

Логін та пароль: це найпоширеніший метод автентифікації, коли користувач вводить логін та пароль, щоб отримати доступ до системи. Паролі повинні бути достатньо складними та міцними, щоб запобігти можливості вгадування або перехоплення пароля.

Біометрична автентифікація: цей метод використовує фізіологічні чи поведінкові характеристики користувачів, такі як відбитки пальців, розпізнавання голосу або обличчя, які можна використовувати для автентифікації.

Ключові карти або токени: цей метод використовує карти або токени, що містять криптографічні ключі, для автентифікації користувачів.

Двофакторна автентифікація: цей метод використовує комбінацію двох з перерахованих методів для автентифікації користувача, зазвичай логін з паролем і кодом, який надсилається на мобільний телефон або на пошту.

4. Використання криптографічних методів захисту даних: за допомогою криптографічних методів можна захистити дані від незаконного доступу користувачів. Наприклад, можна використовувати шифрування даних, щоб захистити їх під час транспортування та зберігання. Також можна використовувати цифрові підписи для підтвердження автентичності даних та

осіб, які їх надсилають.

Для захисту даних використовують різні криптографічні методи, такі як:

Симетричне шифрування. Цей метод використовує один ключ для шифрування та розшифрування даних. Ключ може бути переданий між відправником та отримувачем, або ж може бути встановлений перед початком комунікації.

Асиметричне шифрування. Цей метод використовує два ключі - публічний та приватний. Публічний ключ використовується для шифрування даних, а приватний - для їх розшифрування. Цей метод більш безпечний, оскільки приватний ключ не повинен передаватись по мережі.

Хешування даних. Цей метод дозволяє отримати фіксований довжини "відбиток" даних, який неможливо перетворити на початкові дані. Це дозволяє використовувати хеш-функції для захисту паролів та інших конфіденційних даних.

Цифровий підпис. Цей метод дозволяє підтвердити автентичність даних та особи, яка їх надіслала. Він базується на використанні приватного ключа для підпису даних та публічного ключа для перевірки підпису.

Використання цих методів дозволяє забезпечити високий рівень захисту конфіденційної інформації в інформаційній системі.

Реалізація цих методів дозволить знизити ризик інсайдерських атак та захистити інформацію від несанкціонованого доступу.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД ІНСАЙДЕРСЬКИХ АТАК

3.1 DeviceLock DLP

Програмний комплекс DeviceLock DLP складається з функціональних взаємодоповнюючих модулів - DeviceLock, NetworkLock, ContentLock, DeviceLock Search Server (DLSS) та DeviceLock Discovery, що ліцензуються опціонально в будь-яких коDмбінаціях для задоволення завдань служб інформаційної безпеки.

Базисний компонент DeviceLock є інфраструктурною платформою та ядром для іншихкомпонентів комплексу та реалізує всі функції його централізованого управління та адміністрування. DeviceLock підтримує повний набір механізмів контекстного контролю доступу користувачів, а також забезпечує подійне протоколювання (аудит) і тіньове копіювання даних для всіх локальних каналів введення-виведення на захищених комп'ютерах, включаючи периферійні пристрої та інтерфейси, системний буфер обміну, локально під'єднані смартфони та КПК, Media Transfer Protocol (MTP), а також канал друку документів на локальні та мережеві принтери. Крім того, компонент DeviceLock включає всі консолі централізованого управління.

Компонент NetworkLock™ забезпечує контекстний контроль каналів мережевих комунікацій на робочих комп'ютерах, включаючи розпізнавання мережевих протоколів незалежно від використовуваних портів, детектування комунікаційних додатків та їх селективну блокування, реконструкцію сесій з відновленням файлів, даних та параметрів, а також подієве протоколювання і тіньове копіювання даних, що передаються.

NetworkLock контролює більшість популярних мережевих протоколів та додатків, включаючи прості та SSL-захищені SMTP-сесії електронної

пошти (з роздільним контролем повідомлень та вкладень), взаємодія між клієнтом Microsoft Outlook та сервером Microsoft Exchange (протокол MAPI), IBM Notes, веб-доступ та інші HTTP програми, включаючи HTTPS сесії, веб-служби електронної пошти та соціальні мережі (AOL Mail, freenet.de, Gmail, GMX Mail, Hotmail (Outlook.com), Mail.ru, NAVER, Outlook Web App (OWA), Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail, Zimbra; Facebook, Google+, Instagram, LinkedIn, LiveJournal, MeinVZ, Myspace, Odnoklassniki, Pinterest, StudiVZ, Tumblr, Twitter, Vkontakte, XING, Disqus, LiveInternet.ru), служби миттєвих повідомлень (Skype, Telegram, Viber, WhatsApp, ICQ Messenger, Jabber, IRC, Mail.ru Агент), хмарні сховища (Amazon S3, Dropbox, Box, Google Drive, Microsoft OneDrive та ін), передачу файлів по протоколів FTP та FTP-SSL, передачу файлів у локальній мережі за SMB, а також сеанси Telnet та Торент.

Компонент ContentLock™ реалізує механізми контентного моніторингу та фільтрації файлів та даних, що передаються з/на змінні носії та в каналах мережевих комунікацій - веб-пошті та соціальних мережах, службах миттєвих повідомлень, файловому обміні протоколів FTP та FTP-SSL та ін. Крім того, технології контентної фільтрації в модулі ContentLock дозволяють встановити фільтрацію для даних тіньового копіювання, щоб зберігати лише ті файли та дані, які інформаційно значущі для завдань аудиту інформаційної безпеки, розслідувань позаштатних ситуацій та їх криміналістичного аналізу.

Компонент DeviceLock Search Server (DLSS) забезпечує повнотекстовий пошук по централізованих баз даних тіньового копіювання та подійного протоколювання.

Сервер DLSS дозволяє значно знизити трудомісткість та підвищити ефективність процесів аудиту та розслідування інцидентів інформаційної безпеки, пов'язаних з витоками інформації, їх криміналістичного аналізу та

збору доказової бази.

DeviceLock Search Server може автоматично розпізнавати, індексувати, знаходити та відображати документи багатьох форматів, таких як: Adobe Acrobat (включаючи зашифровані файли, якщо шифрування файлу виконано одним із наступних алгоритмів: 40-bit RC4, 128-bit RC4, 128-bit AES та 256-bit AES, і при цьому дозволи, встановлені на файл, не забороняють вилучення тексту) (PDF), Ami Pro, AutoCAD (DWG, DXF), Архіви (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Visio, Microsoft Word, Microsoft Works, OpenOffice (документи, таблиці та презентації), Quattro Pro, WordPerfect, WordStar та багато інших.

Компонент DeviceLock Discovery виконує сканування робочих станцій та корпоративних мережевих ресурсів, і на підставі заданих політик здатний виявляти документи та файли з критичним вмістом, здійснювати різні дії з виявленими документами, а також може ініціювати процедури керування інцидентами, спрямовуючи тривожні оповіщення у реальному режимі часу. Детальну інформацію про DeviceLock Discovery можна знайти у документі “Посібник користувача DeviceLock Discovery”.

Початок роботи з DeviceLock Group Policy Manager

DeviceLock Group Policy Manager інтегрується до редактора об'єктів групової політики Windows і не доступний як окрема програма. Щоб використовувати DeviceLock Group Policy Manager на вашому локальному комп'ютері, а не на контролері домену, на ваш комп'ютер необхідно встановити консоль "Управління груповою політикою" (Group Policy Management console, GPMC).

Для Windows Server 2003 або Windows XP консоль “Керування груповою політикою” можна скачати з сайту Microsoft

microsoft.com/download/details.aspx?id=21895. Для пізніших версій клієнтської операційної системи Windows необхідно встановити кошти віддаленого адміністрування сервера (Remote Server Administration Tools, RSAT). Інструкції щодо їх встановлення можна знайти у статті Microsoft support.microsoft.com/kb/2693643.

Для доступу до DeviceLock Group Policy Manager виконайте такі дії:

1. Запустити консоль “Керування груповою політикою”.

2. У дереві консолі обрати потрібний домен Active Directory.

3. На вкладці Пов'язані об'єкти групової політики на панелі відомостей клацнути правою кнопкою миші потрібний об'єкт групової політики та обрати команду Змінити.

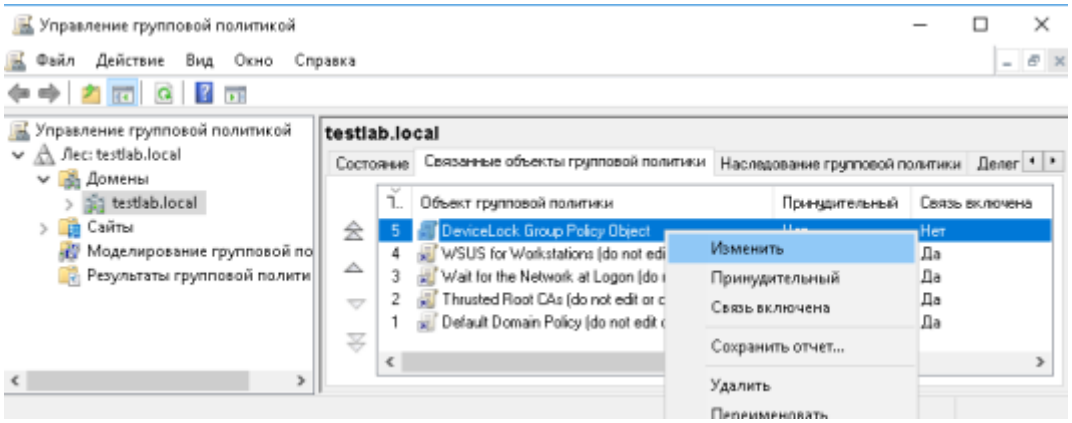


Рис. 3.1. Управління груповими політиками

Якщо потрібно створити новий об'єкт групової політики, клацнути правою кнопкою миші домен у дереві консолі та обрати команду. Створити об'єкт групової політики в цьому домені і зв'язати його.

4. Зачекати, доки запуститься редактор керування груповими політиками. Це може зайняти якийсь час.

5. У розділі Конфігурація комп'ютера обрати DeviceLock.

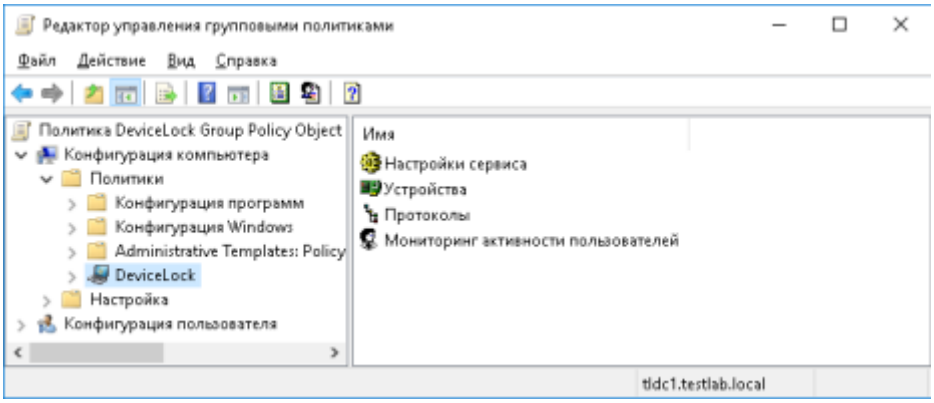


Рис. 3.2. Отримання доступу до DeviceLock через консоль

Можна також запустити консоль керування MMC і вручну додати оснащення Редактор управління груповими політиками:

1. Запусити mmc з командного рядка або використовувати команду Виконати.

2. Відкрити меню Файл і обрати команду Додати або видалити оснастку.

3. У діалоговому вікні, що з'явиться, обрати оснастку Редактор управління

груповими політиками та натиснути кнопку Додати.

Приклади правил IP-файрволу

Нижче наведено приклади правил, які можна створити для IP-файрволу.

IP-файрвол блокує підключення до віддаленого робочого столу на комп'ютери з працюючим сервісом DeviceLock:

1. У дереві консолі розкрити вузли Сервіс DeviceLock -> Протоколи.

2. У вузлі Протоколи клацнути правою кнопкою миші Базовий IP-файрвол, а потім обрати команду Керування.

3. У лівій частині діалогового вікна Базовий IP-файрвол в області

Користувачі натиснути кнопку Додати.

4. У діалоговому вікні Вибір: "Користувачі" або "Групи" у полі Ввести імена

вибраних об'єктів ввести ім'я облікового запису SYSTEM, а потім натиснути кнопку добре.

5. У лівій частині діалогового вікна Базовий IP-файрвол в області Користувачі обрати запис SYSTEM.

6. У правій частині діалогового вікна Базовий IP-файрвол в області Правила натиснути кнопку Додати.

7. У діалоговому вікні Додати правило виконати такі дії:

a) У полі Ім'я ввести ім'я правила файрвола, наприклад, Закрити доступ до RDP.

b) В області Протокол встановити прапорці TCP та UDP.

c) У розділі Тип обрати пункт Заборон.

d) В області Напрямок встановити прапорець Вхідні.

e) У полі Порти ввести 3389.

f) Натиснути кнопку OK.

8. Натиснути кнопку OK або Застосувати, щоб застосувати параметри правила файрволу та закрити діалогове вікно Базовий IP-файрвол. Файрвол дозволяє вхідні підключення за протоколом POP3 для вказаного користувача, блокуючи будь-які інші підключення до комп'ютера з працюючим сервісом DeviceLock:

1. У дереві консолі розкрити вузли Сервіс DeviceLock -> Протоколи.

2. У вузлі Протоколи клацнути правою кнопкою миші Базовий IP-файрвол, а потім обрати команду Керування.

3. У лівій частині діалогового вікна Базовий IP-файрвол в області Пользователи натиснути кнопку Додати.

4. У діалоговому вікні Вибір: "Користувачі" або "Групи" у полі Ввести імена

об'єктів, що обираються, ввести ім'я облікового запису Все, а потім натиснути кнопку OK.

5. У лівій частині діалогового вікна Базовий IP-файрвол в області Користувачі

Вибрати запис Все.

6. У правій частині діалогового вікна Базовий IP-файрвол в області Правила натиснути кнопку Додати.

7. У діалоговому вікні Додати правило виконати такі дії:

a) У полі Ім'я ввести ім'я правила файрвола, наприклад Закрити доступ.

b) В області Протокол встановити прапорці TCP та UDP.

c) У розділі Тип обрати пункт Заборон.

d) В області Напрямок встановити прапорець Вхідні.

e) У полі Порти ввести 0-65535.

f) Натиснути кнопку OK.

Створене правило з'явиться в області “Правила” у правій частині діалогового вікна "Базовий IP-файрвол". Це правило буде використовуватися для блокування всіх віддалених підключень до клієнтського комп'ютера.

8. У лівій частині діалогового вікна Базовий IP-файрвол в області Користувачі натиснути кнопку Додати.

9. У діалоговому вікні Вибір: "Користувачі" або "Групи" у полі Ввести імена об'єктів, що вибираються, ввести ім'я користувача або групи, яким дозволено використовувати POP3, а потім натиснути кнопку OK.

10. В лівій частині діалогового вікна Базовий IP-файрвол в області Пользователи обрати користувача або групу, яким можна використовувати протокол POP3.

11.У правій частині діалогового вікна Базовий IP-файрвол в області Правила натиснути кнопку Додати.

12.У діалоговому вікні Додати правило виконайте такі дії:

a) У полі Ім'я ввести ім'я правила файрвола, наприклад Відкрити доступ до POP3.

b) В області протоколу встановити прапорець TCP.

c) У розділі Тип виберати Роздільна здатність.

d) В області Напрямок встановити прапорець Вхідні.

e) У полі Порти ввести 110.

f) Натиснути кнопку OK.

Створене правило з'явиться в області “Правила” у правій частині діалогового вікна "Базовий IP-файрвол". Це правило буде використовуватися для розблокування в файрвол порту 110, щоб користувач міг створювати підключення по протоколу POP3.

13.Натиснути кнопку OK або Застосувати, щоб застосувати параметри правила файрволу та закрити діалогове вікно Базовий IP-файрвол.

Acronis DeviceLock DLP 9.0

Приклад: файрвол забороняє всі вхідні та вихідні TeamViewer-з'єднання з комп'ютером, на якому працює сервіс DeviceLock:

1. У дереві консолі розкрити вузли Сервіс DeviceLock -> Протоколи.

2. У вузлі Протоколи клацнути правою кнопкою миші Базовий IP-файрвол, а потім виберати команду Керування.

3. У лівій частині діалогового вікна Базовий IP-файрвол в області Пользователи натиснути кнопку Додати.

4. У діалоговому вікні Вибір: "Користувачі" або "Групи" у полі Ввести імена

об'єктів, що вибираються, ввести ім'я облікового запису Все, а потім

натиснути кнопку OK.

5. У лівій частині діалогового вікна Базовий IP-файрвол в області Пользователи обрати запис Все.

6. У правій частині діалогового вікна Базовий IP-файрвол в області Правила натиснути кнопку Додати.

7. У діалоговому вікні Додати правило виконати такі дії:

a) У полі Ім'я ввести ім'я правила файрвола, наприклад, Закрити доступ до

TeamViewer.

b) В області протоколу встановити прапорець TCP.

c) У розділі Тип обрати пункт Заборон.

d) В області Напрямок встановити прапорець Вихідні.

e) У полі Порти ввести 5938.

f) Натиснути кнопку OK.

Створене правило з'явиться в області “Правила” у правій частині діалогового вікна "Базовий IP-файрвол". Це правило буде використовуватися для блокування всіх підключень до серверів TeamViewer.

8. Натиснути кнопку OK або Застосувати, щоб застосувати параметри правила файрволу та закрити діалогове вікно Базовий IP-файрвол.

Моніторинг

Централізований моніторинг – функція сервера DeviceLock Enterprise Server, що дозволяє контролювати поточний стан сервісу DeviceLock на віддалених комп'ютерах шляхом періодичного опитування. Результати моніторингу відображаються в консолі керування режимі реального часу, а також зберігаються у спеціальному журналі для наступного перегляду та аналізу.

Крім того, DeviceLock Enterprise Server періодично порівнює поточні політики. безпеки (налаштування) агентів на вказаних адміністратором комп'ютерах з еталонними політиками, і фіксує інформацію про виявлені відхилення.

Функція моніторингу на сервері DeviceLock Enterprise Server дозволяє встановлювати сервіс DeviceLock на контрольовані комп'ютери, які можна розглядати як ще один спосіб розгортання сервісу DeviceLock на додаток до традиційних методів (інсталяція ПЗ) через GPO, Microsoft SCCM, через консолі управління DeviceLock, інтерактивну установку, та і т.д.). Для отримання додаткових відомостей див. Установка за допомогою DeviceLock Enterprise Server.

Також цю функцію можна використовувати як альтернативний спосіб розгортання налаштувань, дозволів, аудиту, правил тіньового копіювання та тривожних сповіщень на віддалені мережеві комп'ютери, що контролюються сервісом DeviceLock.

Усі дії, пов'язані з моніторингом, виконуються завданнями. Список завдань можна побачити на панелі відомостей під час вибору вузла Моніторинг у дереві консолі. Управління завданнями передбачає:

• Створення завдання - Клацнути вузол Моніторинг правою кнопкою миші та обрати команду Створити завдання.

• Редагування існуючого завдання - Клацнути правою кнопкою миші та обрати команду Редагувати завдання.

• Управління списком комп'ютерів існуючого завдання - Клацнути правою задачею кнопкою миші та обрати команду Редагувати список комп'ютерів. Ця команда з'являється у меню лише для завдань зі статичним списком комп'ютерів.

• Негайне виконання завдання - Клацнути правою кнопкою миші задачу

і обрати команду Запустити зараз.

• Перегляд комп'ютерів, які контролюються завданням - Розгорнути вузол Моніторинг та обрати завдання у дереві консолі. Список комп'ютерів з'явиться на панелі відомостей. При необхідності можна підключити консоль до сервісу DeviceLock на контрольованому комп'ютері: клацнути правою кнопкою миші комп'ютер у списку та виберати команду Підключитися до сервісу DeviceLock.

• Видалення завдання - Клацнути правою кнопкою миші задачу та обрати команду Видалити завдання.

Завдання моніторингу

Усі дії, пов'язані з моніторингом, виконуються завданнями. На одному сервері

DeviceLock Enterprise Server може створити будь-яку кількість завдань. Максимальна кількість завдань на сервері обмежено лише кількістю вільної пам'яті, швидкістю процесора та пропускною спроможністю мережі. Майте на увазі, що сервер повинен мати достатньо ресурсів, щоб одночасно підключатися щонайменше до 10 віддалених комп'ютерів. За промовчанням DeviceLock Enterprise Server може виконувати одночасно до 30 завдань. Це означає, що якщо у вас, наприклад, 40 завдань, і всі вони запускаються в один і той же час, то спочатку будуть запущені перші 30 завдань, а потім, у міру їх закінчення, по одному будуть запускатися 10 завдань, що залишилися. Тим не менш, максимальну кількість завдань, що одночасно запускаються, можна змінити. Для цього додайте наступне значення до реєстру комп'ютера, на якому працює сервер DeviceLock Enterprise Server:

• Ключ: HKEY_LOCAL_MACHINE\SOFTWARE\SmartLine Vision\DeviceLockEnterpriseServer

• Значення: ConcurrentJobs=dword:<кількість потоків>

Тут <кількість потоків> має бути цілим числом від 1 до 1000.

Під час виконання завдання пишуть корисну інформацію в журнал моніторингу. Ця інформація включає в себе поточні стану комп'ютерів та екземплярів сервісу DeviceLock, а також можливі помилки, які виникають у процесі сканування комп'ютерів та підключення до екземплярів сервісу DeviceLock.

Також завдання відображають списки комп'ютерів та їх поточні стани у консолі керування. Це дозволяє аналізувати ситуацію у режимі реального часу. Завдання та її контрольовані комп'ютери та завдання моніторингу відображаються у дереві консолі під вузлом DeviceLock Enterprise Server > Моніторинг > Завдання.

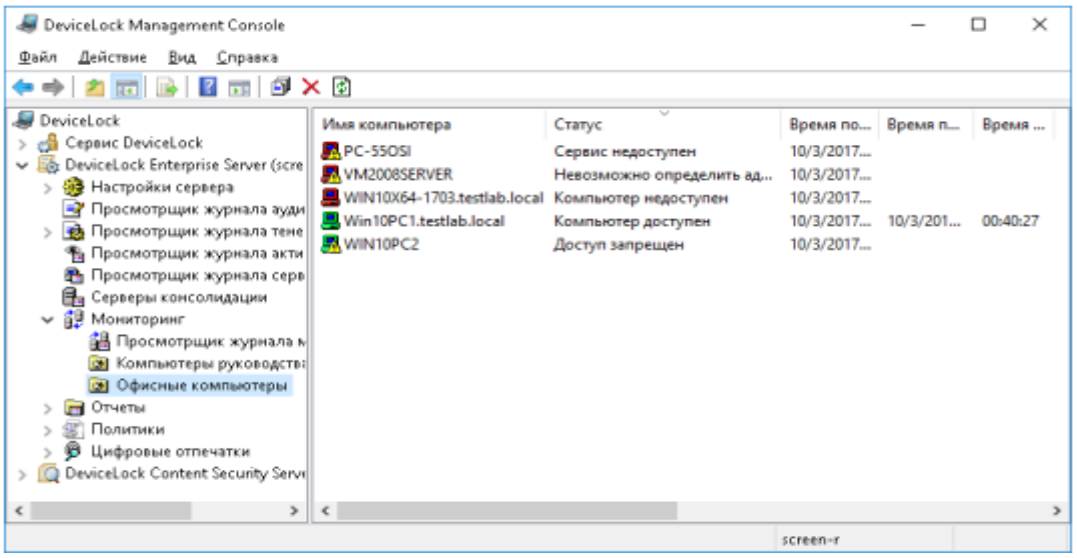


Рис. 3.3. Розділ моніторингу

Вибравши завдання у дереві консолі, можна побачити список усіх комп'ютерів, що контролюються цим завданням. Щоб оновити інформацію у списку комп'ютерів, клацнути правою задачею кнопкою миші та обрати команду Оновити.

Панель відомостей консолі відображає список контрольованих комп'ютерів з наступними відомостями щодо кожного комп'ютера:

• Ім'я комп'ютера - Ім'я, яке ідентифікує комп'ютер.

• Статус - Поточний стан комп'ютера та сервісу DeviceLock на цьому комп'ютері.

Для індикації статусу слугує також значок поруч із ім'ям комп'ютера:

• Зелений комп'ютер – означає, що комп'ютер та сервіс DeviceLock працюють.

• Червоний комп'ютер - означає, що комп'ютер не працює (або не знайдено), або працює, але сервіс DeviceLock не працює.

• Комп'ютер із знаком оклику - Виявлено проблеми або з самим комп'ютером або з сервісом DeviceLock на цьому комп'ютері.

Передбачено вісім різних станів (статусів):

• Комп'ютер доступний - Комп'ютер працює та сервіс DeviceLock на ньому запущено.

Також, якщо це завдання перевіряє цілісність політики, то ця перевірка пройшла без поялок. Значок комп'ютера у разі - “зелений комп'ютер”. Якщо це завдання відновлює змінену політику, іконка комп'ютера буде - "Зелений комп'ютер із знаком оклику".

• Комп'ютер недоступний - DeviceLock Enterprise Server не може виконати

сканування комп'ютера. Це відбувається, коли комп'ютер вимкнено або з'єднання блокуються файрволом, але при цьому ім'я комп'ютера або його IP-адресу можуть бути отримані через DNS. Значок комп'ютера в цьому випадку - "червоний комп'ютер".

• Сервіс недоступний - DeviceLock Enterprise Server не може

підключитися до

сервісу DeviceLock Це відбувається, коли комп'ютер працює, але сервіс DeviceLock на ньому не запущено. Також це може відбуватися через те, що сервіс DeviceLock запущений не на тому TCP-порту, який вказаний у налаштуваннях завдання, або з'єднання блокуються файрволом. Значок комп'ютера в цьому випадку - "червоний комп'ютер із знаком оклику".

• Налаштування пошкоджено - Комп'ютер працює та сервіс DeviceLock на ньому запущено, але деякі налаштування сервісу DeviceLock на цьому комп'ютері відрізняються від еталонної політики, заданої завдання моніторингу. Значок комп'ютера в цьому випадку -зелений комп'ютер з знак оклику. Клацнути правою кнопкою миші комп'ютер і обрати пункт Перегляд деталей для перегляду налаштувань сервісу DeviceLock на контрольованому комп'ютері, які від еталонної політики. Команда Перегляд деталей відображає діалогове вікно зі списком налаштувань, що не відповідають еталонному політиці. Кожне таке налаштування супроводжується описом невідповідності,

наприклад:

• відсутня - Налаштування встановлено в еталонній політиці, але відсутнє на

контрольований комп'ютер.

• відрізняється - Налаштування задане по-різному в еталонній політиці та на

контрольований комп'ютер.

• надмірно - Налаштування відзначено як віддалену в еталонній політиці, але

задана на контрольованому комп'ютері.

- Неможливо визначити адресу комп'ютера - DeviceLock Enterprise

Server не може отримати ім'я/адресу комп'ютера. Це відбувається, коли задано ім'я комп'ютера, що не існує в DNS. Також це може відбуватися через те, що комп'ютер в даний момент не включений, а в мережі немає сервера DNS. В такому випадку статус Неможливо визначити адресу комп'ютера повинен трактуватися вами як Комп'ютер недоступний. Значок комп'ютера в цьому випадку – червоний комп'ютер із знаком оклику".

• Непідтримувана версія сервісу – DeviceLock Enterprise Server намагається отримати політику (налаштування) від сервісу DeviceLock версії 6.2 та нижче. Перевірка цілісності політика підтримується тільки для версій 6.2.1 і вище. Значок комп'ютера в цьому випадку - "зелений комп'ютер із оклику знаком".

• Доступ заборонено - DeviceLock Enterprise Server не може підключитися до

сервісу DeviceLock через нестачу привілеїв. Це відбувається, коли обліковий запис, під яким запущено службу DeviceLock Enterprise Server, не має прав доступу для підключення до DeviceLock. Значок комп'ютера у цьому випадку - "Зелений комп'ютер із знаком оклику".

• Ліцензія недоступна - через брак ліцензій DeviceLock Enterprise Server не

може провести моніторинг комп'ютера з сервісом DeviceLock . DeviceLock Enterprise Server контролює стільки екземплярів сервісу DeviceLock, скільки ліцензій встановлено на DeviceLock Enterprise Server.

Значок комп'ютера в цьому випадку - "зелений комп'ютер із знаком оклику". Ці статуси (за винятком статусу Комп'ютер доступний) також записуються в журнал моніторингу та можуть бути проаналізовано пізніше.

• Час останнього сканування - Дата та час останньої спроби сканування.

Спроба сканування може бути успішною чи невдалою.

• Час останнього успішного сканування - Дата та час останньої успішної спроби сканування.

• Час роботи сервісу – Час безперервної роботи сервісу DeviceLock.

• Час роботи комп'ютера - Час безперервної роботи комп'ютера

відстежується. Порівнявши час безперервної роботи комп'ютера з часом роботи сервісу, можна визначити, чи зупинявся сервіс DeviceLock у поточному сеанс.

• Версія сервісу – Версія сервісу DeviceLock. Останні п'ять цифр означають номер збирання.

Створення/Редагування задачі

Кожне завдання містить власний список комп'ютерів та налаштування.

Щоб створити нове завдання, використовуйте команду Створити завдання з контекстного меню, доступного для пункту Моніторинг. Щоб відредагувати існуюче завдання, використовуйте команду **Редагувати завдання** з контекстного меню. Якщо необхідно безповоротно видалити завдання, виділити це завдання в дереві консолі та обрати команду **Видалити завдання** із контекстного меню.

Для створення або редагування завдання використовується таке діалогове вікно:

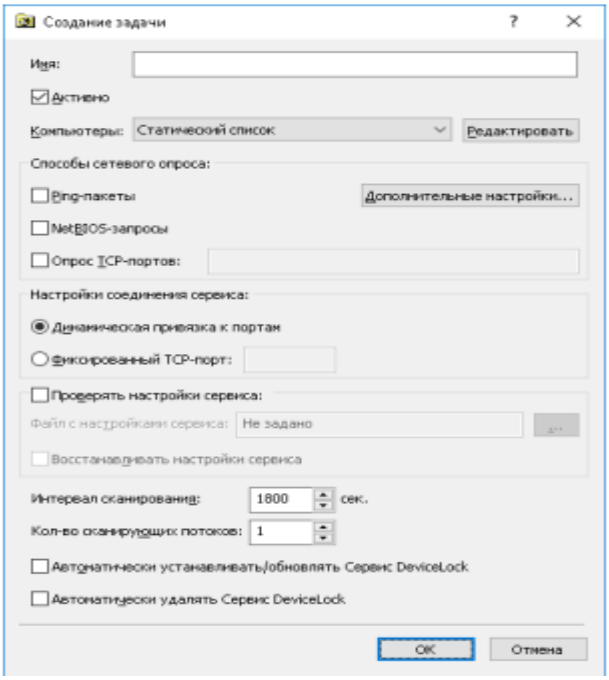


Рис. 3.4. Створення задачі

• Ім'я - Ім'я завдання, яке служить для її ідентифікації у списку завдань та журналі моніторингу.

• Активно - якщо цей прапорець встановлений, DeviceLock Enterprise Server буде виконувати завдання. Зняти цей прапорець, якщо потрібно вимкнути виконання цієї задачі без її видалення.

• Комп'ютери - Тип списку комп'ютерів, який використовується для завдання комп'ютерів, які контролюватимуться даним завданням.

Натиснути кнопку Редагувати, щоб настроїти список, тип якого вибраний у полі Комп'ютери.

Підтримуються два типи списків комп'ютерів:

1. Статичний список - Всі комп'ютери задаються у списку за іменами та/або IP-адресами. Оскільки цей список статичний, то навіть якщо якийсь комп'ютер більше не існує в мережі, він буде контролюватись завданням, поки запис про ньому не буде видалено вручну з цього списку.

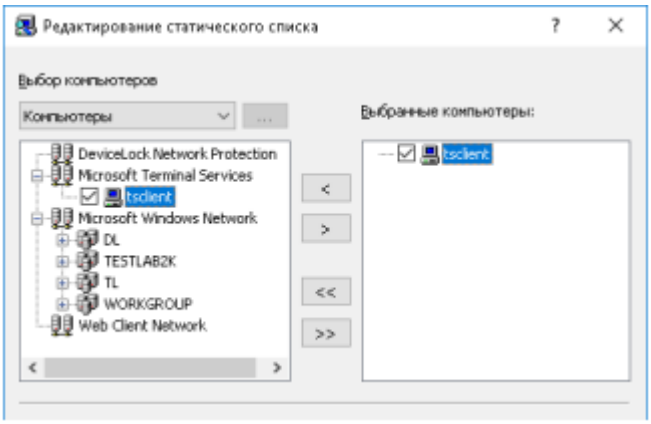


Рис. 3.5. Редагування статичного списку

Комп'ютери, що контролюються, задаються в правому списку. Обрати необхідні комп'ютери в лівому списку, а потім перемістити їх у правий список, натиснувши кнопку.

Якщо потрібно виключити деякі комп'ютери з процесу моніторингу, то виділити їх у правому списку та натиснути кнопку.

Використовуючи кнопки та, можна додавати та видаляти всі доступні комп'ютери за один раз (не потрібно окремо виділяти комп'ютери у списках).

Є кілька варіантів вибору комп'ютерів у списку:

• Active Directory - Переглянути та вибрати комп'ютери з підрозділів служби каталогів Active Directory.

• Комп'ютери - Переглянути та вибрати комп'ютери з дерева мережі.

• LDAP - Переглянути та вибрати комп'ютери з дерева LDAP-сумісної служби каталогів.

• З файлу - Завантажити заздалегідь підготовлений список комп'ютерів з

зовнішній текстовий файл, а потім вибрати комп'ютери. Щоб відкрити

Зовнішній файл, натиснути кнопку . Текстовий файл може містити імена

комп'ютерів та/або IP-адреси, кожен з яких повинен бути записаний на

окремому рядку.

• Вручну - Ввести імена комп'ютерів вручну, а потім обрати комп'ютери із отриманого списку. Кожне імена або IP-адреса комп'ютера

необхідно вводити на окремому рядку.

2. Динамічний список - Замість імен комп'ютерів або IP-адрес, динамічний список містить шлях до контейнера (наприклад, до підрозділу) дереві служби каталогів (такі як Active Directory, Novell eDirectory, OpenLDAP та т.п.). Щоразу на момент виконання завдання DeviceLock Enterprise Server отримує всі комп'ютери, які зараз існують в контейнер. Таким чином, якщо деякий комп'ютер був вилучений зі служби каталогів або був переміщений в інший контейнер, то він не буде більше контролюватись завданням. І навпаки, якщо з'явився новий комп'ютер не існував у контейнері на момент створення/редагування завдання, а був доданий туди пізніше, то цей новий комп'ютер буде контролюватись у момент виконання завдання. Можна вибрати один або кілька контейнерів.

Шлях до вибраних контейнерів вказується у полі Шлях. Обрати контейнери в дерево клацанням миші, утримуючи натиснутою клавішу Shift або Ctrl. Потім натиснути кнопку Вибрати. Щоб скасувати вибір контейнера, натиснути червоний хрестик у поле Шлях.

Встановити прапорець Переглянути вкладені контейнери, щоб дозволити задачі отримувати комп'ютери з усіх вкладених контейнерів, що знаходяться всередині вибраного контейнера. Якщо цей прапорець знято, то всі вкладені контейнери ігноруються та комп'ютери виходять тільки безпосередньо з вибраного контейнера.

Передбачено два режими роботи зі службою каталогів:

• Active Directory - Перегляд та вибір контейнера з дерева служби каталогів Active Directory.

Хоча дерево Active Directory може відображатись і в режимі LDAP, рекомендовано використовувати цей спеціальний режим ActiveDirectory, т.к. у цьому випадку DeviceLock Enterprise Server працює зі службою каталогів ефективніше і споживає менше ресурсів.

Якщо для доступу до Active Directory вам потрібно встановити дані альтернативного облікового запису (ім'я користувача та пароль), натиснути кнопку і вказати у діалоговому вікні Параметри доступу необхідне ім'я користувача та відповідний пароль.

Встановити прапорець Синхронізація, щоб дозволити серверу DeviceLock Enterprise Server використовувати внутрішній механізм синхронізації, наданий Active Directory. Використання цього механізму дозволяє значно знизити навантаження на контролер домену та швидше отримувати комп'ютери під час виконання завдання.

• LDAP - Перегляд та вибір контейнера з дерева LDAP-сумісної служби каталогів.

Щоб налаштувати підключення до LDAP-сервера, натиснути кнопку та вказати у діалоговому вікні Параметри LDAP.

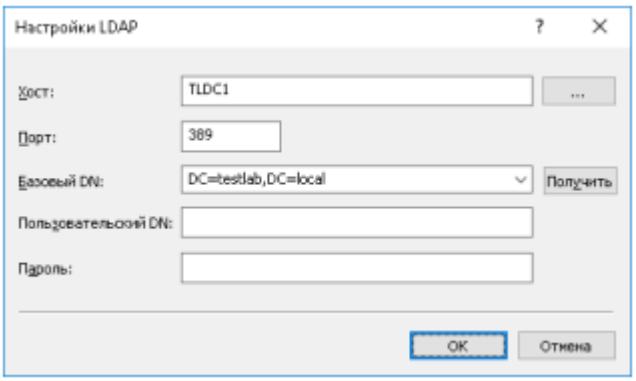


Рис. 3.6. Налаштування LDAP.

• Хост - Ім'я або IP-адреса LDAP-сервера, до якого виконується

підключення.

• Порт - Номер порту, за яким LDAP-сервер приймає

підключення. За промовчанням це порт 389.

• Базовий DN – початкова точка для перегляду дерева каталогу. Ви

повинні використовувати рядок у форматі LDAP (наприклад,

cn=qa,o=SMARTLINE,c=US). Залишити це поле порожнім для перегляду з

коріння дерева.

Отримати всі доступні контексти можна за допомогою кнопки Отримати.

• DN користувача - Ім'я користувача, під яким

виконується підключення до каталогу. Ви повинні використовувати

рядок у форматі LDAP (наприклад, cn=admin,o=SMARTLINE,c=US).

• Пароль – Пароль користувача.

• Способи мережного опитування - Різні методи мережного сканування, які використовуються для визначення статусів (доступний або недоступний) комп'ютерів, що перевіряються. У момент виконання завдання сервер DeviceLock Enterprise Server використовує все вибрані методи сканування в перерахованому порядку, поки один із них не поверне статус доступний для комп'ютера. Якщо жоден з методів не повернув статус доступний, цей комп'ютер отримує статус недоступний. Підтримується три методи мережного сканування:

• Ping-пакети - Сервер надсилає звичайний ICMP-пакет (“пінг”) до комп'ютера та чекає від нього відповіді.

• NetBIOS-запити - Якщо компонент “Клієнт для мереж Microsoft встановлено на комп'ютері, то цей комп'ютер відповість на NetBIOS-запит, надісланий сервером.

• Опитування TCP-портів - Сервер перевіряє перелічені TCP-порти на комп'ютері та шукає перший відкритий порт. Використовуючи кому (,) або точку з комою (;) як роздільник, ви можете вказати кілька портів одночасно. Щоб встановити додаткові параметри сканування, натиснути кнопку Додаткові налаштування та вказати наступні параметри у діалоговому вікні

Налаштування мережевого опитування.

• Кількість повторів - Визначає, скільки разів DeviceLock Enterprise

Server повторно виконуватиме кожен метод сканування, коли він

повертає статус недоступний. Нуль (0) у цьому полі означає, що повторних

спроб сканування цим же методом робитися не буде (для цього

комп'ютера на даний момент виконання завдання).

• Очікування відповіді - Час у секундах протягом DeviceLock Enterprise

Server очікує відповідь від комп'ютера для кожного методу сканування. Якщо

DeviceLock Enterprise Server працює в повільній або надмірно завантаженій

мережі, можливо, потрібно збільшити це значення.

• Налаштування з'єднання сервісу - Ці параметри визначають як DeviceLock

Enterprise Server повинен підключатися до сервісу DeviceLock на контрольованих

комп'ютерах для отримання номера версії, налаштувань тощо. Якщо параметри з'єднання задані неправильно, то DeviceLock Enterprise Server не зможе підключитися до сервісу DeviceLock і комп'ютери, на яких він працює, отримають статус Сервіс недоступний.

Сервіс DeviceLock може бути налаштований на використання

фіксованого порту або динамічних портів під час встановлення на комп'ютер. Додаткову інформацію.

Передбачено два способи підключення:

• Динамічна прив'язка до портів - Обрати цю опцію для використання сервером DeviceLock Enterprise Server динамічних портів при підключенні до сервісу DeviceLock.

• Фіксований TCP-порт - Якщо сервіс DeviceLock налаштований на використання фіксованого TCP-порту, слід обрати цю опцію і вказати номер порту.

• Перевірка установок сервісу - встановити цей прапорець, якщо потрібно, щоб дане завдання моніторингу виконувало перевірку налаштувань сервісу DeviceLock шляхом їхнього порівняння з певними еталонними налаштуваннями.

Якщо цей прапорець встановлений, то на кожному контрольованому комп'ютері завдання моніторингу перевіряє налаштування сервісу DeviceLock, порівнюючи їх із еталонними. При виявленні налаштувань, що відрізняються від еталонних, комп'ютеру надається статус

"Налаштування пошкоджено". Крім того, подія “Налаштування пошкоджено” реєструється у журналі моніторингу. Список налаштувань, що відрізняються від еталонних, міститься в записи про подію. Його можна переглянути за допомогою команди Перегляд деталей на подію “Налаштування пошкоджено” у журналі моніторингу. Ще один спосіб перегляду налаштувань, що не збігаються з еталонними, - використовувати команду Перегляд деталей на контрольованому комп'ютері зі статусом “Налаштування пошкоджено”.

• Файл із налаштуваннями сервісу - Шлях та ім'я файлу налаштувань сервісу DeviceLock, які вважаються еталонною політикою. Для вибору файлу

служить кнопка поруч із цим полем. Еталонна політика призначається задачі шляхом завантаження певного файлу налаштувань сервісу DeviceLock. Цей файл можна створити у консолі DeviceLock Service Settings Editor, DeviceLock Management Console або DeviceLock Group Policy Manager. У ході перевірки завдання отримує налаштування з контрольованих комп'ютерів та порівнює їх із файлом налаштувань, призначеним як еталонна політика для цього завдання. Усі настройки, не визначені в еталонній політиці (параметри, що знаходяться у стані “не визначено”), під час перевірки не враховуються. Ця функція може використовуватися для вибіркової перевірки параметрів, що цікавлять, дозволяючи іншим параметрам відрізнятиметься від еталонної політики. Щоб завантажити файл, натиснути кнопку . Оскільки цифровий підпис на даному не перевіряється, можна вибрати підписаний або непідписаний файл. Ім'я та шлях вибраного файлу відображається у полі Файл з налаштуваннями сервісу. У разі підписаного файлу його ім'я та шлях полягає в круглі дужки. При редагуванні завдання, якому вже призначено еталонну політику, параметри еталонної політики можна експортувати до файлу, натиснувши кнопку “Зберегти”.

• Відновлювати установки сервісу - Встановити прапорець, якщо потрібно, щоб завдання моніторингу замінювало пошкоджені налаштування на контрольованих комп'ютери налаштування з еталонної політики. Завдання, у якого даний прапорець встановлений, не тільки перевіряє, а й відновлює налаштування сервісу DeviceLock у разі їх зміни чи пошкодження.

• Інтервал сканування - Час у секундах, який має пройти після закінчення

виконання завдання та перед початком виконання цієї задачі знову.

• Кількість скануючих потоків - Максимальна кількість потоків, яка може бути задіяно даним завданням у процесі виконання. Можна збільшити

це значення, щоб розділити процес сканування комп'ютерів. Тим не менш, більша кількість потоків вимагає більшої кількості ресурсів (особливого пам'яті та мережного трафіку) для сервера DeviceLock Enterprise Server.

• Автоматично встановлювати/оновлювати Сервіс DeviceLock - встановити цей прапорець для автоматичного встановлення сервісу DeviceLock на комп'ютери, включені завдання моніторингу.

• Автоматично видаляти Сервіс DeviceLock - встановити цей прапорець для

автоматичного видалення сервісу DeviceLock із комп'ютерів, включених у завдання моніторингу.

Правила протоколів

Контекстно-залежні правила розширюють базову функціональність контролю доступу до мережевим протоколам у DeviceLock DLP, забезпечуючи високотехнологічний рівень захисту конфіденційних документів організації через використання технологій контентного аналізу та фільтрації вмісту файлів та даних. Вони забезпечують автоматичну перевірку вмісту даних/файлів, що передаються по мережі, виявлення конфіденційних даних та застосування необхідних політик безпеки. За допомогою контентно-залежних правил можна вибірково дозволити чи заборонити доступ до зазначеному вмісту даних, що передаються по мережі, незалежно від дозволів, встановлених на протокол. Контентно-залежні правила також можна використовувати, щоб дозволити або заборонити тіньове копіювання зазначеного вмісту або для виявлення спроб прийому та передачі даних з певним вмістом без блокування доступу та без створення тіньових копій. Правила можна задавати стосовно тих чи інших протоколи індивідуальні для різних користувачів та/або груп. Контентно-залежні правила можуть бути

задані для операцій контролю доступу, тіньового копіювання, виявлення вмісту або для будь-якої комбінації цих операцій.

Наступні приклади показують використання контентно-залежних правил.

• Приклад 1 - Використання контентно-залежних правил для операцій контролю доступу. Можна заборонити окремим користувачам або групам надсилання файлів, що містять номери кредитних карток, номери телефонів та поштові адреси, на FTP сервер.

• Приклад 2 - Використання контентно-залежних правил для операцій тіньового копіювання. Для проведення аудиту інформаційної безпеки та з метою розслідування інцидентів інформаційної безпеки можна зазначити, що тіньові копії будуть створені для миттєвих повідомлень, що містять номери кредитних карток та адреси електронної пошти.

• Приклад 3 - Використання контентно-залежних правил для операцій виявлення. Можна задати правило, що передбачає протоколювання та відправлення тривожного оповіщення при спробах передачі виконуваних файлів, без блокування передачі або створення тіньових копій таких файлів.

Вузол "Контекстно-залежні правила"

Під вузлом Протоколи > Контентно-залежні правила у дереві консолі перераховуються користувачі та групи, для яких задані контентно-залежні правила, що стосуються протоколів. Контентно-залежні правила можуть бути задані індивідуально для кожного користувача та групи.

Контекстне меню вузла Контентно-залежні правила містять такі команди:

• Керування - Відкриває діалогове вікно, яке дозволяє встановити або редагувати контентно залежні правила для оперативного режиму.

• Керування офлайновими налаштуваннями - Відкриває діалогове вікно, що дозволяє встановити або редагувати контентно-залежні правила для автономного режиму.

• Завантажити - Дозволяє імпортувати раніше збережений файл із контентзалежними правилами для оперативного режиму.

• Завантажити офлайнові налаштування - Дозволяє імпортувати раніше збережений файл із контентно-залежними правилами для автономного режиму.

• Зберегти - дозволяє експортувати контентно-залежні правила, задані для оперативного режиму, файл з розширенням .cwl, який потім можна імпортувати та використовувати на іншому комп'ютері.

• Зберегти офлайнові налаштування - Дозволяє експортувати контентно залежні правила, задані для автономного режиму, файл з розширенням .cwl, який потім можна імпортувати та використовувати на іншому комп'ютері.

• Скинути - скидає контентно-залежні правила для оперативного режиму

стан "не задано". Ця команда доступна лише в DeviceLock Group Policy Manager та DeviceLock Service Settings Editor.

• Скинути офлайнові налаштування - Скидає контентно-залежні правила для

автономного режиму стан “не задано”. Якщо такі правила не задані, клієнтським комп'ютерам, що знаходяться не в мережі, застосовуються правила, задані для оперативного режиму.

• Видалити офлайнові налаштування - Блокує успадкування контентно-залежних правил, заданих для автономного режиму, та примусово застосовує правила, поставлені для оперативного режиму. Ця команда доступна лише у DeviceLock Group Policy Manager та DeviceLock Service Settings Editor.

Користувачі та групи, для яких задані контентно-залежні правила, відображаються під вузлом Контентно-залежні правила у дереві консолі та мають таке ж контекстне меню, що і цей вузол, за винятком команди Скинути офлайнові налаштування та з додаванням команди Видалити користувача, яка видаляє контентно-залежні правила для вибраного користувача чи групи.

Примітка: Можна задавати різні контентно-залежні правила для різних режимів роботи (оперативного та автономного) для тих самих користувачів чи груп. Контентно-залежні правила для оперативного режиму (звичайний профіль) застосовуються, коли клієнтські комп'ютери знаходяться у мережі. Контентно-залежні правила для автономного режиму (офлайн-профіль) застосовуються, коли клієнтські комп'ютери працюють автономно. За замовчуванням DeviceLock працює в автономному режимі, коли мережевий кабель не підключено до клієнтського комп'ютера. Опис політик DeviceLock для автономного режиму можна знайти у розділі Політики безпеки DeviceLock (офлайнпрофіль). Інструкції з налаштування контентно-залежних правил див. у розділі Керування контентно залежними правилами для автономного режиму.

Список контентно-залежних правил для протоколів

Користувачі та групи, для яких задані контентно-залежні правила, що стосуються протоколів, що відображаються під вузлом Протоколи > Контентно-залежні правила в дереві консолі.

Якщо вибрати користувача або групу під вузлом Контентно-залежні правила у дереві консолі, на панелі відомостей відображаються контентно-залежні правила, задані для цього користувача чи групи. Для кожного правила список містить такі відомості:

• Ім'я – Ім'я правила. За умовчанням контентно-залежне правило має те саме ім'я, що й зазначена у правилі контентна група.

• Тип – тип аналізу вмісту файлу. Можливі значення:

• Визначення типу файлу – означає, що ідентифікація файлів ведеться за сигнатур.

• Ключові слова - означає, що ідентифікація даних/файлів здійснюється за заданим ключовим словам та виразам.

• Шаблон - означає, що ідентифікація даних/файлів ведеться на основі заданих шаблонів регулярних виразів Perl.

• Властивості документа - означає, що ідентифікація файлів ведеться за їх властивостям.

• Цифрові відбитки - означає, що ідентифікація даних/файлів ведеться їх цифровим відбиткам.

• Складене – означає, що ідентифікація даних/файлів ведеться за заданим контенту, описаному логічним виразом.

• Дія - Вказує, які дії з протоколами користувачеві дозволені або заборонені, а також які дії користувача записуватимуться в журналі тіньового копіювання.

• Застосовується до - Можливі значення:

• Дозволи - означає, що правило застосовується для операцій контролю доступу.

• Тіньове копіювання - означає, що правило застосовується до операцій виборчого тіньового копіювання

• Виявлення - означає, що правило застосовується до операцій виявлення.

• Дозвіл+Тіньове копіювання - означає, що правило застосовується до операцій контролю доступу та операцій виборчого тіньового копіювання.

• Роздільна здатність + Виявлення - означає, що правило застосовується до операцій контролю доступу та операцій виявлення.

• Тіньове копіювання+Виявлення - означає, що правило застосовується до операціям виборчого тіньового копіювання та операціям виявлення.

• Дозвіл+Тіньове копіювання+Виявлення - означає, що правило застосовується до всіх можливих видів операцій: контролю доступу, виборчого тіньового копіювання та виявлення вмісту.

• Протокол(и) - Протоколи, до яких застосовується правило.

• Надіслати алерт - Відображає, чи увімкнені оповіщення для цього правила.

• Протоколувати подію - Відображає, чи увімкнено реєстрацію подій.

• Тіньове копіювання - Відображає, чи буде створено тіньову копію в результаті спрацьовування цього правила.

• Профіль - Можливі значення: Звичайний та Офлайн. Значення Звичайний вказує, що правило застосовується до комп'ютерів, що у мережі. Значення Офлайн показує, що правило застосовується до комп'ютерів, які працюють автономно.

Одним і тим же користувачам або групам можна задавати різні правила для різних профілів. Про роботу з правилами офлайн-профілю див. Управління контентзалежними правилами для протоколів в автономному режимі.

Контекстне меню правила у списку на панелі відомостей містить такі команди:

• Управління - Залежно від профілю цього правила (звичайний або офлайн),

відкриває діалогове вікно, в якому можна задати контентно-залежні правила для оперативного чи автономного режиму.

• Редагувати - Відкриває діалогове вікно, в якому можна переглянути або змінити це правило.

• Надіслати алерт - Вмикає або вимикає надсилання сповіщень для цього
правила.

• Протоколувати подію - Вмикає або вимикає протоколювання подій для
цього правила.

• Тіньове копіювання - Включає або вимикає тіньове копіювання контенту,
що викликає спрацьовування цього правила.

• Видалити - Видалення цього правила.

Управління доступом до контенту Контентно-залежні правила для протоколів дозволяють:

• Надати доступ до зазначеного контенту, коли доступ заборонено на рівні
протоколу.

- Заборонити доступ до зазначеного контенту, коли доступ дозволено на рівні типу протоколу.

Контенстно-залежні правила застосовуються до сесій, дозволених за білим списком протоколів, лише якщо встановлено прапорець Контентний аналіз. В іншому випадку контентно залежні правила не впливають на такі сесії. Наступна таблиця містить відомості про права доступу, які використовуються під час створення контентно-залежних правил протоколів.

Налаштування безпеки для протоколів

Використовуючи вузол Протоколи > Установки безпеки, можна увімкнути додаткові параметри безпеки, які впливають на встановлені дозволи та правила аудиту для протоколів. Опис цих параметрів див. у розділі

Опис параметрів безпеки.

Контекстне меню вузла Установки безпеки містять такі команди:

• Керування - Відкриває діалогове вікно, яке дозволяє спільно вмикати або

вимикати параметри безпеки для оперативного режиму.

• Керування офлайновими налаштуваннями - Відкриває діалогове вікно, що дозволяє спільно вмикати або вимикати параметри безпеки для автономного режиму.

Якщо в дереві консолі вибрано вузол Налаштування безпеки, на панелі відомостей відображається список налаштувань. Щоб керувати налаштуванням, клацнути її правою кнопкою миші на панелі відомостей та використати команди контекстного меню:

• Увімкнути - Вмикає параметри безпеки для оперативного режиму.

• Вимкнути - Вимикає параметри безпеки для оперативного режиму.

• Скинути - Скидає налаштування для оперативного режиму у стан “не встановлено”.

Ця команда доступна лише в DeviceLock Group Policy Manager та DeviceLock Service Settings Editor.

• Увімкнути офлайн - Вмикає параметри безпеки для автономного режиму.

• Вимкнути офлайн - Вимикає параметри безпеки для автономного режиму.

• Скинути офлайнові налаштування - Скидає всі налаштування, що були раніше задані.

автономного режиму стан “не задано”. Якщо налаштування безпеки для

автономного режиму не задані, до клієнтських комп'ютерів, що не в мережі,

застосовуються параметри безпеки для оперативного режиму.

• Керування - Відкриває діалогове вікно, яке дозволяє спільно вмикати або

вимикати параметри безпеки для оперативного режиму.

• Керування офлайновими налаштуваннями - Відкриває діалогове вікно, що дозволяє

спільно вмикати або вимикати параметри безпеки для автономного режиму.

• Видалити налаштування офлайну - Блокує успадкування налаштувань безпеки

для автономного режиму та примусово застосовує налаштування, задані для

оперативний режим. Ця команда доступна лише в DeviceLock Group Policy Manager та DeviceLock Service Settings Editor.

Щоб змінити налаштування оперативного режиму (звичайний профіль), можна двічі клацнути відповідне налаштування на панелі відомостей для зміни її стану (Увімкнено / Вимкнено). Також можна клацнути налаштування правою кнопкою миші та вибрати пункт управління в контекстному меню або натиснути відповідну кнопку на панелі інструментів.

Опис налаштувань безпеки

DeviceLock надає такі параметри безпеки для протоколів:

• Блокувати нерозпізнаний вихідний SSL-трафік - Якщо увімкнено, то сервіс

DeviceLock проводить аудит та блокує весь нерозпізнаний вихідний SSL-трафік.

Якщо налаштування вимкнено, навіть при заблокованих протоколах нерозпізнаний вихідний SSL-трафік не блокується та аудит для нього не виконується.

• Блокувати URL-адреси, що містять IP-адреси - Якщо увімкнено, то сервіс DeviceLock блокує з'єднання по будь-яких URL, що містять IP-адресу, навіть якщо користувачеві можна використовувати протокол. Ця установка впливає на всі протоколи, крім наступних: FTP, IBM Notes, IRC, Jabber, MAPI, SMB, SMTP, Telnet та Торрент. За замовчуванням вона вимкнена.

Стосовно протоколів, на які впливає це налаштування, контроль доступу, аудит та тіньове копіювання для URL, що містять IP-адресу, виконуються на рівні протоколу HTTP. При забороні доступу за протоколом HTTP з'єднання з використанням що містять IP-адресу URL блокуються для всіх таких протоколів, навіть якщо налаштування блокувати URL-адреси, що містять IP-адреси, не включено.

• Блокувати проксі трафік - Якщо увімкнено, то сервіс DeviceLock реєструє та
блокує весь трафік через проксі-сервер. Підтримуються такі типи проксі-серверів: HTTP, SOCKS4 та SOCKS5.

• Блокувати мережу, якщо BFE зупинено (для Windows 8 і вище) – Якщо включено, то сервіс DeviceLock блокує весь мережевий трафік при зупиненій системної служби базової фільтрації (BFE) Якщо це налаштування вимкнено та служба базової фільтрації зупинено, модуль NetworkLock не зможе контролювати мережевий трафік на комп'ютерах під керуванням Windows 8 і пізніших версій.

Щоб увімкнути цю установку, необхідно, щоб була задана політика NetworkLock (будь-які пов'язані з протоколами дозволу або правила сервісу DeviceLock). В іншому випадку це налаштування не діє.

• Перехоплювати з'єднання MS Lync - Якщо увімкнено, дозволяє сервісу DeviceLock перехоплювати мережевий трафік програми Microsoft Lync 2010 або Microsoft Office Communicator. Для ввімкнення даного налаштування необхідно, щоб було встановлено політика NetworkLock (будь-які пов'язані з протоколами дозволу або правила сервісу DeviceLock). В іншому випадку це налаштування не діє.

• Блокувати трафік Tor-браузера - Якщо увімкнено, сервіс DeviceLock блокує підключення до мережі Tor, запобігаючи використанню Tor-браузера. Для включення даної настройки необхідно, щоб була задана політика NetworkLock (будь-які пов'язані з протоколами дозволу або правила сервісу DeviceLock). Інакше у разі ця настройка не діє. Коли ця настройка діє, спроби використовувати Tor-браузер реєструються в журналі аудиту як події заборони підключення, де як джерело зазначений Torбраузер, і враховуються як заборонені спроби доступу до протоколу Інші (Other) в звіти за даними журналу аудиту (звіти категорії Audit Log).

Приклади дозволів

Для всіх користувачів заборонені всі пристрої USB, крім клавіатури та миші:

1. Обрати запис USB-порту зі списку типів пристроїв у розділі Дозволи, потім обрати встановити роздільну здатність із контекстного меню, доступного за натисканням правою кнопкою миші.

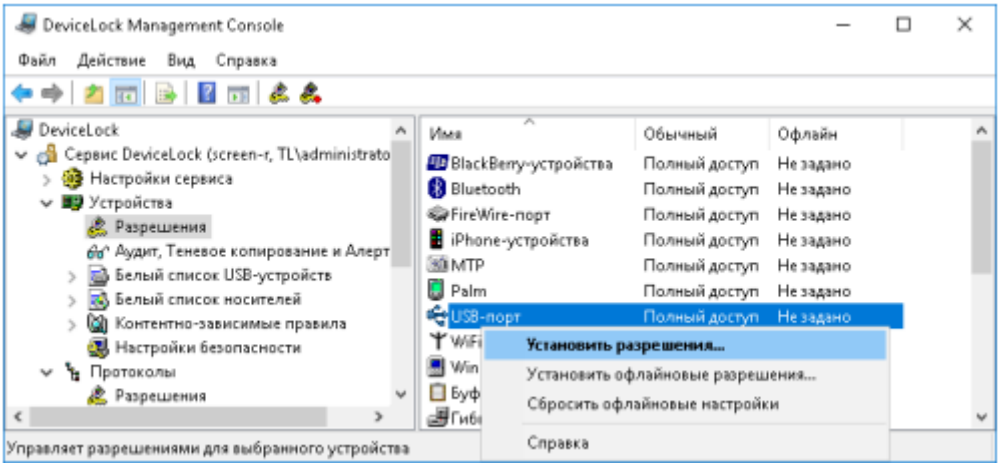


Рис. 3.7. Встановлення дозволу.

2. Натиснути кнопку Додати в діалоговому вікні Роздільна здатність, додайте обліковий запис всі (Everyone), натиснути OK, щоб закрити діалогове вікно вибору користувача, виділити запис Все та відключити для неї всі права у списку Права користувача.

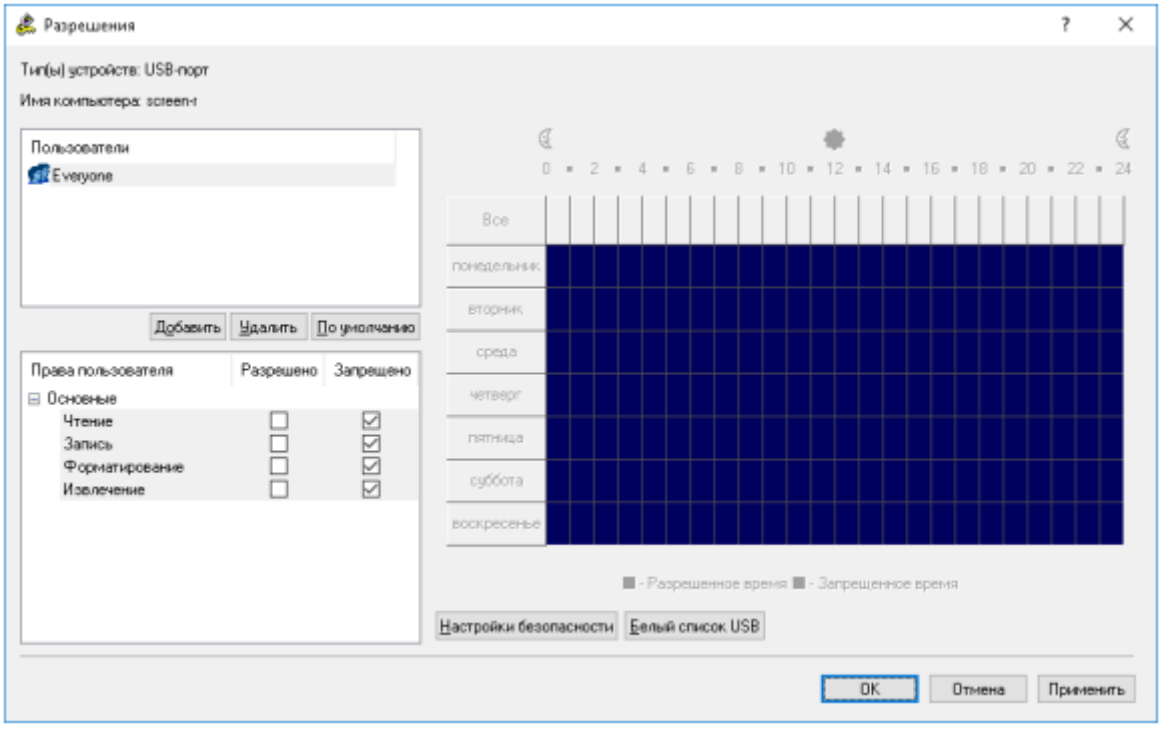


Рис. 3.8. Додавання облікового запису ВСІ.

3. Натиснути кнопку Налаштування безпеки у діалоговому вікні Роздільна здатність, а потім зняти прапорець Керувати доступом до USB HID (миша, клавіатура, тощо) діалоговому вікні Налаштування безпеки.

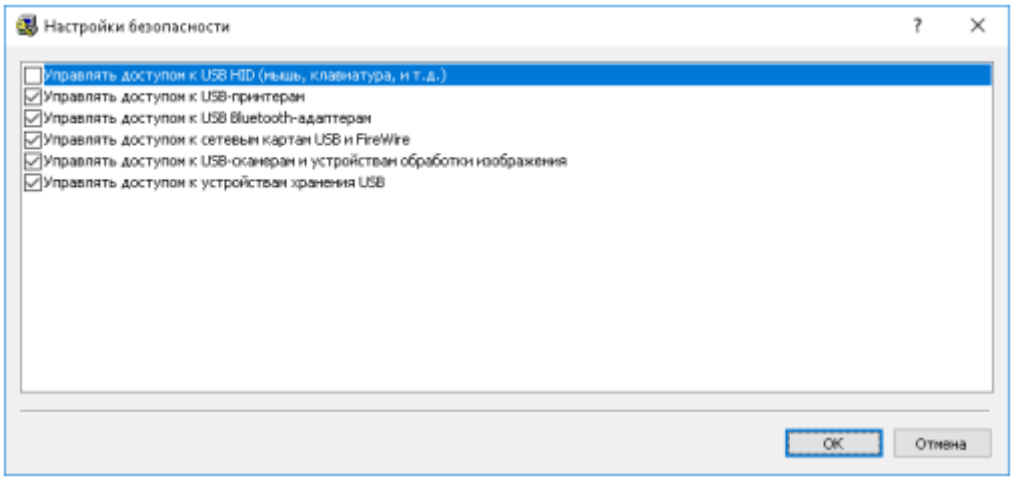


Рис. 3.9. Налаштування безпеки.

4. Натиснути OK, щоб закрити діалогове вікно Установки безпеки, натиснути OK, щоб застосувати налаштування та закрити діалогове вікно Дозволи, потім натиснути “так”, щоб підтвердити.

Категорії та типи звітів

Графи зв'язків: використовуються для інтерактивного аналізу комунікаційних взаємодій працівників організації. Аналіз здійснюється за допомогою наочних графічних зв'язків, які будуються на основі даних про канали комунікації та частоту їх використання.

Користувацькі профілі: дозволяють уповноваженим особам відстежувати комп'ютерну активність користувачів за допомогою зручного графічного подання статистики їх дій на комп'ютері. У цих звітах надаються статистичні показники для моніторингу та оцінки різних аспектів поведінки користувачів, таких як частота спроб виконати недозволені дії або передача

великих обсягів даних, зміна мережевої активності користувача і т. д.

Звіти на основі журналу аудиту: базуються на даних журналів подій, які збирає та зберігає DeviceLock Enterprise Server. Можна створювати тільки звіти попередньо визначених типів, зміна або створення нових (користувацьких) типів не передбачено.

Звіти на основі журналу тіньового копіювання: використовуються для аналізу журналів тіньового копіювання, що зберігаються на сервері DeviceLock Enterprise Server. Всі такі звіти базуються на даних з журналу тіньового копіювання та журналу видалених даних тіньового копіювання. Можна створювати тільки звіти попередньо визначених типів, зміна або створення нових (користувацьких) типів не передбачено.

Графи зв'язків дозволяють досліджувати статистику мережевої комунікації користувачів шляхом аналізу інтерактивного графічного подання даних, що зберігаються в журналах аудиту (протоколування подій), тіньового копіювання та віддалених даних тіньового копіювання. Звіти відображаються у формі графів. Для побудови графів використовуються різні типи даних, включаючи дані про чати, дзвінки та передані файли в сервісах миттєвих повідомлень і соціальних мережах, а також дані про повідомлення, які передаються електронною поштою, включаючи вкладення. Аналіз даних проводиться для наступних мережевих протоколів: IBM Notes, Skype, SMTP, соціальні мережі, Telegram, Viber, веб-пошта, WhatsApp та Zoom. При побудові графів можуть не враховуватись віддалені дані тіньового копіювання, що стосуються розмірів файлів, що передаються через сервіси миттєвих повідомлень, або у вигляді вкладень, що передаються електронною поштою.

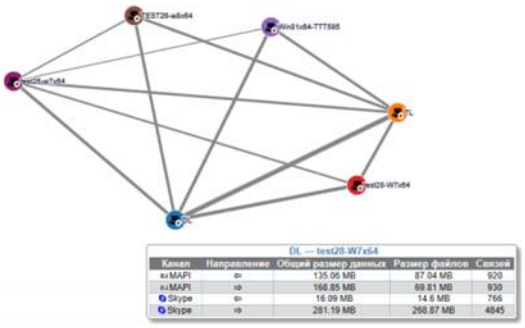


Рис. 3.10. Приклад графу.

Висновок до частини 2:

Під час дослідження методів за засобів захисту від інсайдерських атак було детально проаналізовано інструмент Device Lock DLP. Було встановлено, що цей інструмент дозволяє забезпечити захист конфіденційної інформації від інсайдерських загроз шляхом контролю за використанням різних пристроїв зберігання даних та моніторингом дій користувачів в мережі.

Device Lock DLP має декілька ключових функцій, таких як блокування доступу до конфіденційної інформації, контроль використання зовнішніх пристроїв зберігання даних, аудит дій користувачів та аналіз файлів на вміст конфіденційної інформації. Такі функції дозволяють підвищити рівень захисту від інсайдерських атак та зменшити ризики витоку конфіденційної інформації.

Отже, Device Lock DLP є ефективним інструментом для захисту від інсайдерських атак. Дослідження методів захисту від інсайдерських атак є важливим етапом розробки рекомендацій щодо захисту інформаційних систем від таких загроз.

3.2 Рекомендації щодо захисту від інсайдерських атак

Аналіз ефективності застосованих методів захисту від інсайдерських атак є важливим кроком у забезпеченні безпеки інформації в організації. Під час аналізу необхідно перевірити, наскільки ефективні застосовані методи захисту та на якому рівні є ризик інсайдерських атак.

Один з ключових методів захисту від інсайдерських атак - це розробка системи контролю доступу до інформації та ресурсів системи. Ефективність цього методу залежить від того, наскільки точно визначені права доступу до різних ресурсів інформаційної системи та наскільки добре контролюється доступ користувачів до цих ресурсів. Також важливо, щоб система контролю доступу мала можливість визначати та реагувати на ненормальну поведінку користувачів, наприклад, на спроби доступу до ресурсів, до яких вони не мають права.

Ще один ефективний метод захисту - використання системи моніторингу активності користувачів. Ця система дозволяє відстежувати дії користувачів в системі та спостерігати за змінами їх активності, що може свідчити про потенційну загрозу безпеці інформації. Якщо система виявляє підозрілу активність користувача, вона може автоматично заблокувати доступ до системи або сповістити адміністратора системи для подальшої перевірки.

Також можна використовувати процедури автентифікації та авторизації користувачів, які дозволяють перевіряти ідентифікацію користувача та його права доступу до ресурсів системи. Однак, якщо користувачі використовують слабкі паролі.

Надійність системи автентифікації та авторизації може бути компрометована. Тому важливо надавати рекомендації щодо використання надійних паролів та регулярної зміни їх, а також рекомендувати використовувати інші методи автентифікації, такі як двофакторна

автентифікація.

Крім того, використання криптографічних методів захисту даних, таких як шифрування та цифрові підписи, може забезпечити додатковий рівень захисту від інсайдерських атак.

Також, система моніторингу активності користувачів може допомогти виявляти незвичайну поведінку користувачів та надавати можливість швидко реагувати на потенційні загрози.

Однак, важливо розуміти, що жоден метод захисту не є 100% надійним. Тому потрібно постійно моніторити стан безпеки системи та регулярно оновлювати заходи захисту.

ВИСНОВКИ

У цій роботі було проаналізовано можливі загрози та ризики, пов'язані з інсайдерськими атаками, а також було запропоновано низку заходів для покращення захисту від цих атак.

Було виявлено, що деякі з методів захисту, такі як процедури автентифікації та авторизації, шифрування даних та мережеві фірмові стіни, є дуже ефективними в запобіганні несанкціонованому доступу до інформації. Однак, існує також ризик інсайдерських атак, які можуть обійти ці методи захисту.

Запропоновані рекомендації, такі як збільшення свідомості користувачів про загрози, встановлення системи контролю доступу до ресурсів, аудит безпеки та моніторинг діяльності користувачів, можуть допомогти покращити захист від інсайдерських атак.

Для перевірки ефективності запропонованих рекомендацій можна провести експериментальні дослідження, що включають тестування системи на наявність уразливостей, симуляцію інсайдерських атак та вимірювання впливу запропонованих заходів на покращення безпеки системи.

Отже, важливо розуміти, що захист інформаційної системи є постійним процесом, і потребує не тільки застосування ефективних методів захисту, але й постійного аналізу загроз та ризиків, а також удосконалення заходів захисту.

Враховуючи недоліки, бакалаврська робота заслуговує оцінку **відмінно**, а студент **Поліщук А.С.** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

ПЕРЕЛІК ПОСИЛАНЬ

1. Інсайдерські атаки: розуміння, виявлення та запобігання URL: https://www.cisa.gov/sites/default/files/publications/Insider_Attacks_508.pdf (дата звернення 26.04.2023)

2. Гарісон Д. Інсайдерські атаки: виявлення, запобігання та розслідування [Insider Threats: Detection, Prevention, and Mitigation] / Д. Гаррісон. / *Комп'ютерна безпека*. 2018. №73. С. 55–58.

3. Карлтон Д. Захист від інсайдерських загроз: перспективи та стратегії [Protection Against Insider Threats: Perspectives and Strategies] / Д. Карлтон. / *Журнал кібербезпеки*. 2019. №6. С. 27–35.

4. Бернштейн Д. Інсайдерські атаки: визначення, класифікація та заходи безпеки [Insider Threats: Definitions, Classifications, and Security Measures] / Д. Бернштейн, А. Мартінес, М. Ван-Счайк. / *Міжнародний журнал інформаційної безпеки*. 2018. №17. С. 16–29.

5. Абрамсон Д. Інсайдерські атаки: аналіз загроз та рекомендації з запобігання [Insider Threats: Threat Analysis and Prevention Recommendations] / Джеймс Абрамсон. / *Журнал кібербезпеки*. 2017. №4. С. 14–21.

6. Шубхрадж С. Ефективний підхід до виявлення інсайдерських атак з використанням машинного навчання [Effective Approach to Insider Attack Detection Using Machine Learning] / С. Шубхрадж, М. Сюн, І. Такефумі. / *Міжнародний журнал кібербезпеки та інформаційної безпеки*. 2019. №7. С. 1–13.

7. Джеремі В. Запобігання інсайдерським атакам: огляд підходів та технологій [Preventing Insider Attacks: Review of Approaches and Technologies] / В. Джеремі, К. Роберт. / Журнал безпеки і захисту інформації. 2018. №3. С. 11–22.

8. Лок М. Методи боротьби з інсайдерськими загрозами: огляд досліджень та практики [Methods for Combating Insider Threats: Review of Research and Practice] / М. Лок, Д. Чейм. / *Журнал кібербезпеки та захисту інформації*. 2019.

№6. С. 24–32.

9. Маркс Д. Управління ризиками інсайдерських загроз: моделі та методи [Managing Insider Threat Risks: Models and Methods] / Д. Маркс, Ф. Штайнер. / *Журнал кібербезпеки*. 2017. №4. С. 9–15.

10. Сандерсон Д. Захист від інсайдерських атак: практичний підхід [Protection Against Insider Attacks: A Practical Approach] / Д. Сандерсон, Е. Форд. // *Комп'ютерна безпека*. 2018. №74. С. 45–50.

11. Кавахара М. Розробка системи виявлення інсайдерських атак на основі машинного навчання [Development of an Insider Attack Detection System Based on Machine Learning] / М. Кавахара, Т. Нішида, К. Івасакі. // *Міжнародний журнал кібербезпеки та інформаційної безпеки*. 2020. №8. С. 16–28.

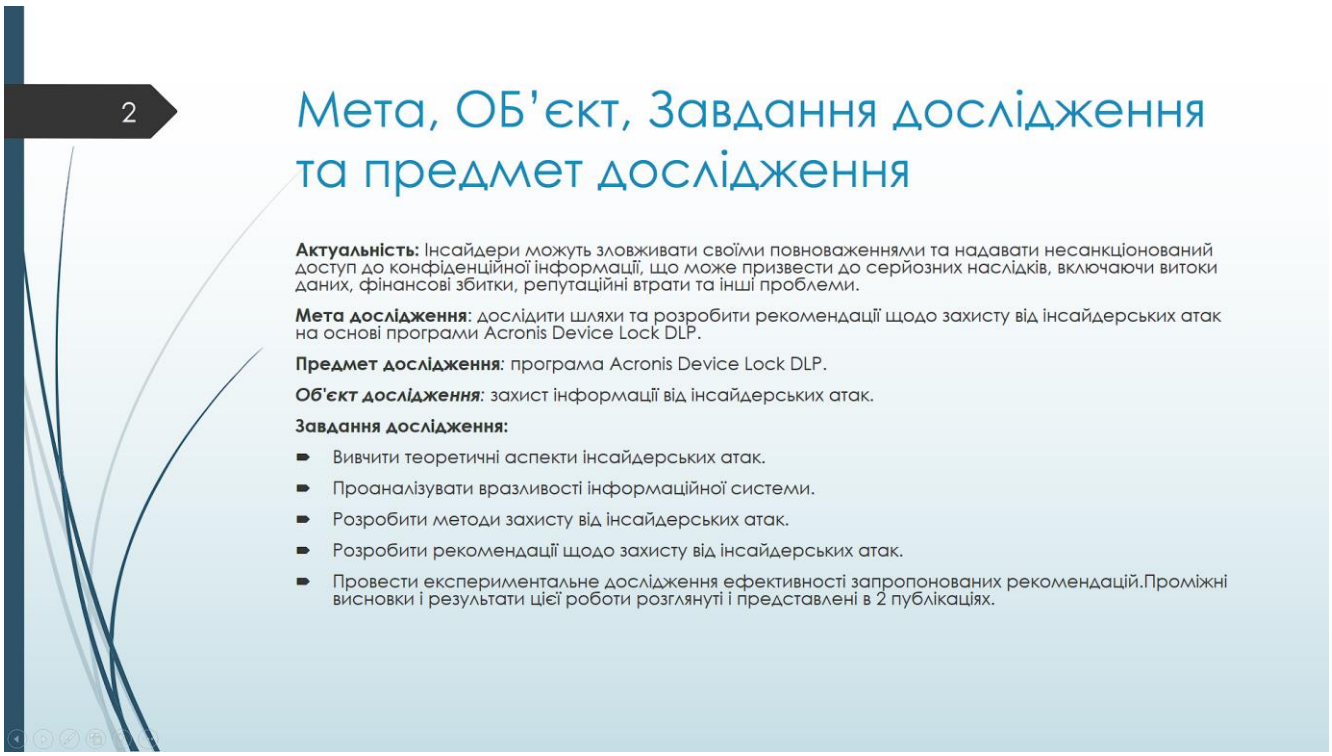
12. Рекомендації щодо запобігання та виявлення інсайдерських атак [Recommendations for Preventing and Detecting Insider Attacks]. URL: https://www.sec.gov/files/insider-threat-guidance.pdf (дата звернення 26.04.2023)

13. Керівництво з управління ризиками інсайдерських загроз [Insider Threat Risk Management Guidance]. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (дата звернення 26.04.2023)

14. Ліберман Д. Розробка стратегій виявлення інсайдерських загроз на основі аналізу даних [Developing Insider Threat Detection Strategies Based on Data Analysis] / Д. Ліберман, С. Блейн. / *Комп'ютерна безпека*. 2020. №80. С. 35–40.

15. Шаталін О. О, Коваленко С. М, Чередніченко В. І. Методи і технології захисту інформації в сучасних умовах. Харків: Факт, 2018. 438 с.

ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ (ПРЕЗЕНТАЦІЯ)



3

Види інсайдерських атак

- Активна інсайдерська атака - це випадки, коли працівник організації зловживає своїми повноваженнями та вчиняє дії, які завдають шкоди інформаційній системі. Наприклад, працівник може зламати систему безпеки та отримати доступ до конфіденційної інформації або видалити важливі дані.
- Пасивна інсайдерська атака - це випадки, коли працівник організації отримує конфіденційну інформацію, не вчиняючи активних дій, які можуть завдати шкоди організації. Наприклад, працівник може неправильно зберігати чутливу інформацію або не захистити свій пристрій з інформацією від несанкціонованого доступу.

4

Рішення для захисту від інсайдерських атак

- DLP система (англ. Data Loss Prevention system) - це комплекс технологій та інструментів, що призначений для запобігання втрати конфіденційної інформації організації або її неправомірному використанню.
- UEBA - UEBA аналізує не тільки дії користувачів, але й поведінку різних сутностей в комп'ютерних системах, таких як програми, пристрої та сервіси. Вона забезпечує пошук аномалій у поведінці, які можуть вказувати на загрози безпеці, такі як несподівана активність на рівні мережі, вивантаження даних на зовнішніх серверах або використання даних у незвичайний спосіб.

DIGITAL GUARDIAN®

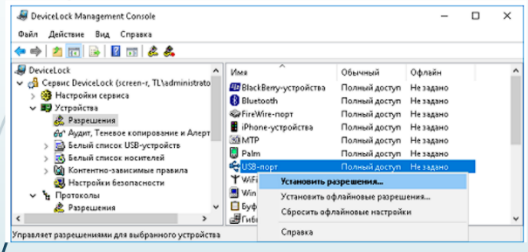
Acronis

DeviceLock DLP

5

Приклади надання дозволів в acronis device lockdlp

- Для всіх користувачів заборонені всі пристрої USB, крім клавіатури та миші:

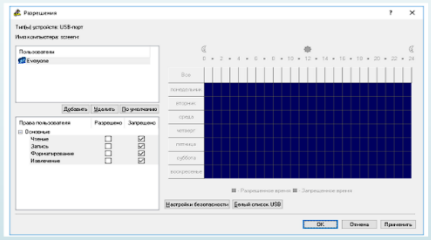


Встановлення дозволу на доступ до USB пристроїв.

6

Додавання облікового запису.

- Натисніть кнопку Додати в діалоговому вікні Роздільна здатність, додайте обліковий запис всі (Everyone), натисніть OK, щоб закрити діалогове вікно вибору користувача, виділіть запис Все та відключіть для неї всі права у списку Права користувача.



Додавання облікового запису ВСІ.

7

Приклад графічного звіту

- Графи зв'язків використовуються для інтерактивного аналізу комунікаційних взаємодій працівників організації. Аналіз здійснюється за допомогою наочних графічних зв'язків, які будуються на основі даних про канали комунікації та частоту їх використання.

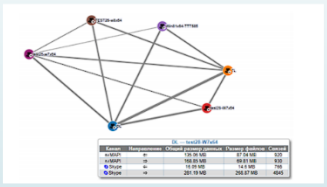


Рис. 2.10 Приклад графічного звіту

8

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД ІНСАЙДЕРСЬКИХ АТАК

- Один з ключових методів захисту від інсайдерських атак - це розробка системи контролю доступу до інформації та ресурсів системи. Ефективність цього методу залежить від того, наскільки точно визначені права доступу до різних ресурсів інформаційної системи та наскільки добре контролюється доступ користувачів до цих ресурсів. Також важливо, щоб система контролю доступу мала можливість визначати та реагувати на ненормальну поведінку користувачів, наприклад, на спроби доступу до ресурсів, до яких вони не мають права.
- Ще один ефективний метод захисту - використання системи моніторингу активності користувачів. Ця система дозволяє відстежувати дії користувачів в системі та спостерігати за змінами їх активності, що може свідчити про потенційну загрозу безпеці інформації. Якщо система виявляє підозрілу активність користувача, вона може автоматично заблокувати доступ до системи або сповістити адміністратора системи для подальшої перевірки.
- Також можна використовувати процедури автентифікації та авторизації користувачів, які дозволяють перевіряти ідентифікацію користувача та його права доступу до ресурсів системи. Однак, якщо користувачі використовують слабкі паролі.

9

Висновки

- Розроблено рекомендації щодо щодо захисту від інсайдерських атак.
- Показано на практиці як в программі можна керувати доступом наприклад до USB пристроїв.

10

Апробація результатів

Науково-практична конференція «цифрова трансформація кібербезпеки», навчально-наукового інституту захисту інформації, 27 квітня 2023 р.

Дякую з увагу!