Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Розробка модуля отримання інформації про процеси для ОС Windows.
Назва теми

КвРКІ.170284.17.02.15 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія»*
Назва

Виконав: студент IV курсу, група КІ–17–2 _____ В.В. Оліх
Підпис Ініціали, прізвище

Керівник _____ С.В. Мостовий
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ І.В. Муляр
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки та
комп'ютерних систем і мереж _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

«18» червня 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Програмування та комп'ютерних і телекомунікаційних систем

Кафедра Кібербезпеки та комп'ютерних систем і мереж

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри Ю.П.Кльоц

" 05 " 02 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Оліху Василю Володимировичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Розробка модуля отримання інформації про процеси для ОС Windows.

Керівник проекту (роботи) Мостовий Сергій Володимирович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

старший викладач

Затверджена наказом ректора університету від 05.02.2021 № 11 додаток №7

2. Строк подання студентом проекту (роботи) на кафедру 18.06.2021

3. Вихідні дані до проекту (роботи): розробка методики дослідження і аналізу засобів аудиту систем сімейства Windows з метою виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин, а також розробка програмного засобу на основі алгоритму, отриманого при розробці даної методики.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити): дослідження і аналіз засобів аудиту подій систем родини windows з метою виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин; Опис схем електричних (структурної,функційної, принципової) проєктованої системи; опис алгоритму роботи системи.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Схема електрична структурна (Е1)

Схема електрична функційна (Е2)

Схема електрична принципова (Е3)

Алгоритм роботи (Е8)

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання при
Нормоконтроль	Муляр І.В., доцент кафедри КбКСМ	-	
Антиплагіат	Муляр І.В., доцент кафедри КбКСМ	-	

7. Дата видачі завдання «_08_» _____02_____ 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Прим.
1.	Підготовка вступного розділу	Березень - 1 декада	
2.	Огляд існуючих методів, засобів	Березень - 2 декада	
3.	Обгрунтування обраних рішень	Березень - 3 декада	
4.	Підготовка опису електричних схем	Квітень - 1 декада	
5.	Виконання розрахункової частини	Квітень - 1 декада	
6.	Підготовка ескізів креслень	Квітень - 2 декада	
7.	Формулювання висновків	Квітень - 3 декада	
8.	Розробка додатків	Травень - 1 декада	
9.	Погодження розділів з консультантом з нормоконтролю	Травень - 1 декада	
10.	Оформлення графічного матеріалу	Травень - 2 декада	
11.	Оформлення пояснювальної записки	Травень - 2 декада	
12.	Попередній захист кваліфікаційної роботи	Травень - 3 декада	
13.	Доопрацювання кваліфікаційної роботи	Травень - 3 декада	
14.	Подання роботи для перевірки на плагіат	Травень - 3 декада	
15.	Захист кваліфікаційної роботи	Червень - 1 декада	

Студент _____ В.В. Оліх
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ С.В. Мостовий
Підпис

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Розробка модуля отримання інформації про процеси для ОС Windows».

Автор роботи: Оліх Василь Володимирович.

Керівник роботи: Мостовий Сергій Володимирович.

Пояснювальна записка: 60 с., 20 рис., 20 джерел, 2 додатка.

Графічна частина: 4 плакати.

Практична значимість дипломного проекту полягає в тому, що розробляється методика дослідження і аналізу засобів аудиту систем сімейства Windows з подальшою розробкою і впровадженням системи моніторингу та аналізу подій безпеки, дозволить підвищити рівень контролю і відстеження несанкціонованих дій програмного забезпечення, який подолав систему інформаційної безпеки підприємства. Необхідність такого контролю зумовлена, як правило, відсутністю в політиці безпеки підприємства приписів щодо розкриття факту несанкціонованого доступу, безпосередньо після того як несанкціонований доступ стався.

Підпис студента

18.06.21
Дата

№	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
	А4	КВРКІ. 170284.17.02.15 ПЗ	Пояснювальна записка	60		
			Графічні матеріали			
	А2	КВРКІ. 170284.17.02.15 Е1	Схема електрична	1		
			структурна			
	А2	КВРКІ. 170284.17.02.15 Е2	Схема електрична	1		
			функціональна			
	А2	КВРКІ. 170284.17.02.15 Е3	Схема електрична	1		
			принципова -			
	А2	КВРКІ. 170284.17.02.15 Е8	Алгоритм роботи	1		

КВРКІ. 170284.17.02.15 ВП

Арк	№ докум	Підпис	Дата
Розробив	Оліх В.В.		
Перевір.	Мостовий С.В.		
Н.контр.	Муляр І.В.		
Затв.	Кльоц Ю.П.		18.06.21

Розробка модуля отримання інформації про процеси для ОС Windows. Відомість проекту

Літера	Аркуш	Аркушів
У		1

ХНУ, КІ-17-2

ЗМІСТ

				КвРКІ. 170284.17.02.15 ПЗ			
Арк.	№докум.	Підпис	Дата				
конав	Оліх В.В.			Розробка модуля отримання інформації про процеси для ОС Windows. Пояснювальна записка	Літера	Аркуш	Аркушів
ревір.	Мостовий С.В.				у	2	60
онтр.	Муляр І.В.				ХНУ КІ-17-2		
вер.	Кльоц Ю.И.						

ВСТУП

Актуальність теми пов'язана з тим, що в останні роки різко зросла кількість можливих способів впливу на конфіденційність, цілісність і доступність інформації, що обробляється в приватних і корпоративних мережах. Причин цього явища кілька. Перш за все, зросла кількість вразливостей, щодня виявляються в програмному забезпеченні інформаційних систем. З ускладненням систем інформаційної безпеки з'являються все більш витончені методи проникнення в систему за допомогою програмного забезпечення. В наш час основними напрямками захисту інформації є: забезпечення доступності необхідної інформації з будь-якої точки мережі, забезпечення її конфіденційності і цілісності.

Однак, доступність мережевих інформаційних ресурсів також спрощує завдання зловмисника по здійсненню успішної спроби несанкціонованого доступу (НСД) до цих ресурсів через мережу, що призводить до порушення конфіденційності. У той же час, недосконалі організаційні заходи дозволяють як внутрішнім, так і зовнішнім зловмисникам запускати шкідливий код на комп'ютерах організацій. Для протидії спробам несанкціонованого доступу розробники програмних і апаратних засобів комп'ютерних мереж розвивають засоби ідентифікації і аутентифікації користувачів, засоби розмежування доступу до мережевих інформаційних ресурсів, криптографічні засоби захисту інформації, а для захисту комп'ютерів кінцевих користувачів від несанкціонованого доступу програмного забезпечення - антивірусні програми і персональні міжмережеві екрани. Зазначені традиційні засоби захисту інформаційних систем від несанкціонованого доступу є досить ефективними, проте їх надмірне ускладнення часто негативно позначається на доступності інформації в мережі. Таким чином, виникає проблема розробки методів і засобів підвищення захищеності інформаційних ресурсів від несанкціонова-

ного доступу в комп'ютерних мережах без погіршення властивостей доступності цих ресурсів. Одним з найбільш ефективних рішень цієї проблеми є використання засобів реєстрації та оперативного аналізу подій, що впливають на інформаційну безпеку комп'ютерних мереж. виникає проблема розробки методів і засобів підвищення захищеності інформаційних ресурсів від несанкціонованого доступу в комп'ютерних мережах без погіршення властивостей доступності цих ресурсів. Одним з найбільш ефективних рішень цієї проблеми є використання засобів реєстрації та оперативного аналізу подій, що впливають на інформаційну безпеку комп'ютерних мереж. виникає проблема розробки методів і засобів підвищення захищеності інформаційних ресурсів від несанкціонованого доступу в комп'ютерних мережах без погіршення властивостей доступності цих ресурсів. Одним з найбільш ефективних рішень цієї проблеми є використання засобів реєстрації та оперативного аналізу подій, що впливають на інформаційну безпеку комп'ютерних мереж.

В даний час завдання реєстрації подій безпеки вирішуються досить ефективно за допомогою засобів аудиту, вбудованих в системне і прикладне програмне забезпечення. Політику аудиту подій можна налаштувати таким чином, щоб створювалися записи про дії користувача або активності системи в зазначеній категорії подій. Можна вести спостереження за активністю, пов'язаної з безпекою, наприклад за тим, хто отримує доступ до об'єкту, за входом користувача в систему і виходом із системи, або за зміною параметрів політики аудиту. Однак завданням ефективної організації оперативного аналізу зареєстрованих подій безпеки не приділяється належної уваги. Для забезпечення оперативного аналізу подій безпеки в комп'ютерній мережі доцільно розробляти і впроваджувати системи моніторингу та аналізу подій безпеки,

Практична значимість дипломного проекту полягає в тому, що розробляється методика дослідження і аналізу засобів аудиту систем сімейства Windows з подальшою розробкою і впровадженням системи моніторингу та

аналізу подій безпеки, дозволить підвищити рівень контролю і відстеження несанкціонованих дій програмного забезпечення, який подолав систему інформаційної безпеки підприємства. Необхідність такого контролю зумовлена, як правило, відсутністю в політиці безпеки підприємства приписів щодо розкриття факту несанкціонованого доступу, безпосередньо після того як несанкціонований доступ стався.

Метою проекту є розробка методики дослідження і аналізу засобів аудиту систем сімейства Windows з метою виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин, а також розробка програмного засобу на основі алгоритму, отриманого при розробці даної методики. Створення системи моніторингу та аналізу подій безпеки на основі розробленої методики дозволить фахівцеві з інформаційної безпеки на підприємстві проводити жорсткий контроль доступу до критичних об'єктів інформаційної системи, дозволить своєчасно виявляти факти несанкціонованого доступу до ресурсів обчислювальної машини і проводити розслідування даних фактів.

Проект складається з 4 розділів.

У першому розділі розробляється методика дослідження і аналізу засобів аудиту систем сімейства Windows з метою виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин на основі аналізу архітектури та функціональних можливостей системи аудиту Windows.

У другому розділі розробляється програмний засіб на основі розробленої методики дослідження і аналізу засобів аудиту систем сімейства Windows з метою виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин

У третьому розділі розглядається інформаційна структура підприємства, аналізуються загрози інформаційній безпеці, і робляться висновки про необ-

хідність додаткового захисту, описується докладний алгоритм роботи програмного засобу та результати впровадження програмного засобу в виділений сегмент інформаційної структури підприємства. У четвертому розділі розраховується техніко-економічна ефективність проекту.

1 ДОСЛІДЖЕННЯ І АНАЛІЗ ЗАСОБІВ АУДИТУ ПОДІЙ СИСТЕМ РОДИНИ WINDOWS З МЕТОЮ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДО РЕСУРСІВ ОБЧИСЛЮВАЛЬНИХ МАШИН

1.1 Дослідження архітектури та функціональних можливостей засобів аудиту систем родини windows

1.1.1 Актуальність реєстрації та аналізу подій безпеки

Підсистеми реєстрації подій безпеки є на сьогоднішній день важливими і невід'ємними компонентами систем забезпечення інформаційної безпеки практично в будь-який мережевий операційній системі. Реєстрацію подій безпеки також часто називають аудитом подій безпеки. Можливості реєстрації подій безпеки реалізовані в мережевих операційних системах і прикладному програмному забезпеченні. Однак, відчутний ефект від використання коштів аудиту досягається лише тоді, коли зареєстровані дані про події безпеки можуть бути проаналізовані. Тільки в цьому випадку стає можливим своєчасне виявлення шкідливих впливів на елементи мережевої інформаційної системи - комп'ютери, програмне забезпечення, що передаються і зберігаються дані і т.д.

Наявність підсистем реєстрації подій безпеки є одним з основних вимог, яке присутнє у всіх сучасних стандартах і керівних документах з інформаційної безпеки комп'ютерних систем. Зазначені стандарти також визначають класи подій, що підлягають реєстрації. Вимоги до наявності коштів реєстрації подій безпеки відносяться до технічних вимог, тому вони, як правило, виконуються виробниками базового програмного забезпечення, використовуваного для побудови мережевих інформаційних систем [1].

Регулярний аналіз зареєстрованих подій безпеки зазвичай відносять до організаційних заходів, що є основною причиною недостатньої уваги виробників програмного забезпечення до проблем організації оперативного аналізу подій безпеки в мережі. Іншими словами, для того, щоб атестувати програмне забезпечення мережевої інформаційної системи на відповідність вимогам стандартів безпеки зазвичай досить реалізувати в ній лише кошти реєстрації подій безпеки.

Облік типових обсягів даних про події безпеки, а саме сотні і тисячі записів в день на одному комп'ютері в мережі, дозволяє стверджувати, що при відсутності спеціальних автоматизують програмних засобів аналіз подій безпеки стає малоефективним. З цієї причини і обслуговуючий персонал мережевих інформаційних систем часто зневажливо ставиться до завдань аналізу зареєстрованих даних про події безпеки.

Все це в значній мірі знижує ефективність реєстрації подій безпеки, яка дає можливість виявити помилки і недоліки в реалізації політики безпеки мережевої інформаційної системи до того, як вони будуть використані в зловмисних цілях.

Засоби управління доступом, існуючі в програмному забезпеченні кожної мережевої інформаційної системи часто не можуть забезпечити безпеку в повній мірі, оскільки вони не призначені для запобігання некваліфікованих або зловмисних дій з боку користувачів мають необхідні повноваження доступу. Своєчасний аналіз подій безпеки дозволяє оперативно виявляти небезпечні ситуації, що виникають внаслідок недостатньо суворого розмежування доступу і вживати заходів протидії [2].

Під час налаштування засобів управління доступом можуть бути допущені помилки, які найчастіше важко помітити при тестуванні, проте ці помилки стають помітні від халепи мережевої інформаційної системи. Своєчасний аналіз подій безпеки дозволяє виявити такі помилки до того, як вони стануть причиною порушення безпеки.

Таким чином, оперативний аналіз зареєстрованих подій безпеки в комп'ютерній мережі дозволяє підвищити захищеність мережевої інформаційної системи від різних загроз інформаційній безпеці за рахунок своєчасного виявлення вразливостей в системі захисту інформації та політики безпеки.

1.1.2 Інструменти аудиту та журнали подій

Аудит безпеки забезпечує моніторинг різних подій, що впливають на безпеку вашої операційної системи. Перегляд системних подій необхідний для виявлення зловмисника і компрометації системних даних. Прикладом події, яке піддається аудиту, є невдала спроба доступу.

Найбільш поширені типи подій аудиту:

-Доступ до таких об'єктів, як файли і папки.

-Управління обліковими записами користувачів, групами, програмами та інтернет-ресурсами.

-Користувальницькі логін і логін

-Доступ і управління процесами.

Під час аудиту подій безпеки створюється журнал безпеки, який дозволяє переглядати ці події. Тому система аудиту - незамінний інструмент інформаційної безпеки. Як приклад наведемо екранний формат звичайної реалізації відображення подій в Windows 10 (рис. 1.1).

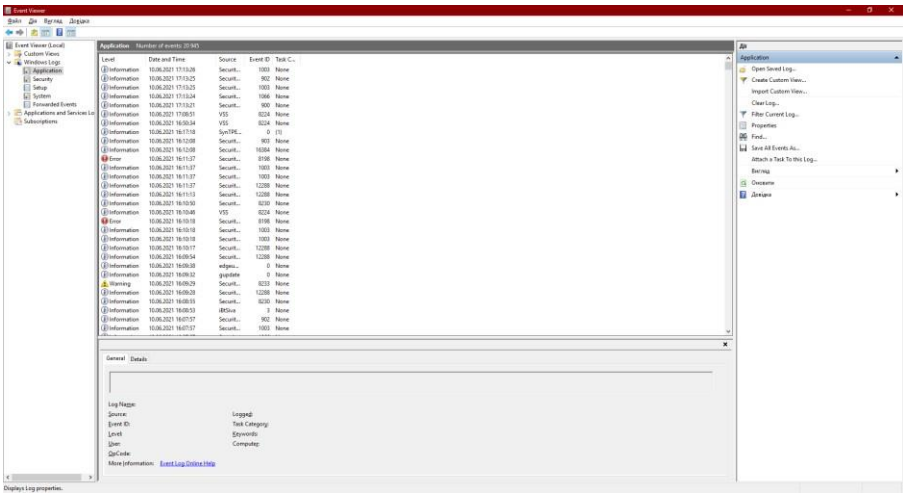


Рисунок 1.1 - Перегляд подій в Windows 10

Журнал подій - цінний інструмент для контролю якості роботи і безпеки мережі, який часто використовується недостатньо ефективно через складність читання логів і їх обсягу. Управління логами подій і їх зберігання вимагають структурованого підходу [3].

1.1.3. Категорія подій системного аудиту

Перед виконанням аудиту необхідно вибрати політику аудиту. По-перше, вам необхідно опублікувати подія безпеки в політиці безпеки аудиту (compmgmt.msc-Utility-Event Viewer-Security). Щоб зареєструватися на такі події, необхідно налаштувати параметри безпеки політики аудиту.

Для виявлення випадків несанкціонованого доступу ПО обов'язковий аудит доступу до об'єктів (файлів, ключів реєстру).

1.1.4 Формат події системи

Журнал аудиту складається з подій системи. При обробці журналу аудиту відбувається аналіз окремих подій. Для аналізу необхідно знати, де можна отримати інформацію про подію, і мати чітке уявлення про структуру самої події.

Щоб переглянути відомості про подію

- необхідно відкрити вікно Перегляд подій;
- в дереві консолі вибрати потрібний журнал;
- в області відомостей вибрати потрібну подію;
- в меню Дія виберіть команду Властивості.

Рисунок 1.2 - Відомості про подію

Далі наведена структура події журналу аудиту.

10.06.2021 16:12:08 Security

Відкриття об'єкту:

Сервер об'єкта: Security

Тип об'єкта: File

Код дескриптора: 2864

Код операції: {0,5246970}

Код процесу: 1428

Файл малюнка: C: \ WINDOWS \ explorer.exe

Основний користувач: Destreizel

Домен: Destreizel

Код входу: (0x0,0x13DAB)

Користувач-клієнт: -

Код входу клієнта: -

доступ READ_CONTROL

SYNCHRONIZE

Читання даних (або перерахування каталогів)

Запис даних (або додавання файлу)

ReadEA

WriteEA

привілеї

Лічильник обмеженого SID: 0

1.2 Розробка методики аналізу засобів аудиту подій систем родини windows для виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин

1.2.1 Розробка структури системи моніторингу подій безпеки

Розробка структури системи аналізу подій безпеки і розподіл функцій між її компонентами повинні проводитися з урахуванням основних вимог до системи. Можна сформулювати такі вимоги, що впливають на структуру системи:

1. Система повинна обробляти дані про події безпеки, які добувають із журналів аудиту кінцевого безлічі комп'ютерів в мережі.

2. Результати обробки подій безпеки повинні зберігається в єдиній базі даних подій безпеки.

3. Функції системи повинні розподілятися між компонентами, що функціонують на різних комп'ютерах мережі.

Пропонована структура системи, яка задовольняє зазначеним вимогам, (рис. 1.3).

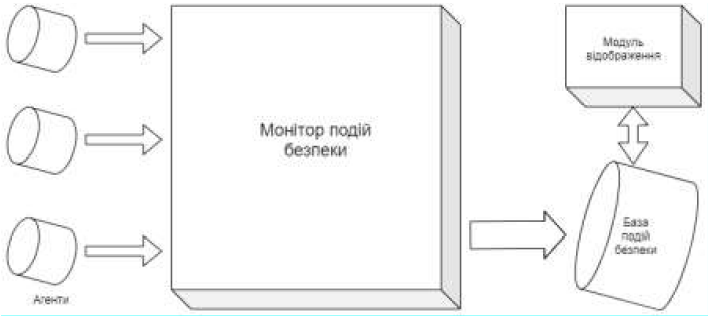


Рисунок 1.3 - Структура системи моніторингу подій безпеки

Розглянемо докладніше призначення і основні функції компонентів системи, користуючись схемою, представленої на (рис. 1.3).

Агенти системи функціонують на комп'ютерах мережі і витягають дані про події безпеки і направляють їх монітора подій безпеки для обробки. Агенти системи можуть виконувати свої функції двома основними способами, а значить можна виділити два основних можливих варіанти реалізації функцій агентів.

Активні агенти. Агенти такого типу направляють нові дані монітора подій безпеки в міру їх виявлення в журналах аудиту.

Пасивні агенти. Агенти такого типу надають монітора дані про події безпеки за запитом, виконуючи, фактично, функції сервісів віддаленого доступу до журналів аудиту комп'ютерів мережі.

Пасивні агенти, можуть забезпечувати як послідовне, так і довільне читання даних з журналів аудиту. Наявність можливості довільного читання даних значно спрощує і прискорює процедури пошуку і вибірки нових даних. Складність і ефективність реалізації довільного читання журналів аудиту залежить від способу зберігання подій в них. Широко поширений текстовий формат зберігання подій ускладнює завдання довільного читання даних у порівнянні зі структурованими форматами.

Монітор подій безпеки (МСБ) - це основний модуль системи, який забезпечує обробку даних про події безпеки, що надходять з комп'ютерів мережі. Основні етапи, методи і алгоритми обробки подій безпеки розглядаються далі. МСБ вирішує завдання автоматизованого аналізу і фільтрації надходять подій згідно із заданими правилами і збереження їх в основній базі даних подій безпеки. Таким чином, МСБ вирішує значну частину завдань системи, забезпечуючи виявлення ознак загроз порушення інформаційної безпеки в комп'ютерній мережі і оповіщення персоналу, відповідального за безпеку мережі.

Модуль відображення призначений для відображення і дослідження результатів роботи монітора подій безпеки.

Таким чином, монітор подій безпеки є основним модулем системи, вирішальним більшість завдань, що стоять перед системою моніторингу подій безпеки, шляхом взаємодії з іншими компонентами системи. Узагальнюючи, можна сказати, що монітор подій безпеки повинен ефективно вирішувати одна основне завдання системи - швидко і надійно виконувати обробку подій безпеки. Ефективність вирішення цього завдання багато в чому залежить від організації процесу обробки подій безпеки, структури монітора подій безпеки, поділу функцій обробки подій безпеки між монітором подій безпеки і агентами системи, що функціонують на комп'ютерах мережі. Ефективність обробки подій також залежить від методів і алгоритмів, що виконують різні етапи обробки подій безпеки.

Обов'язковою складовою методики повинен бути аудит критично важливих об'єктів і процесів операційної системи, таких як:

- кореневої системний каталог Windows, його підкаталоги;
- реєстр Windows;
- системні файли;
- кореневе системне сховище System Volume Information;
- об'єкти автозапуску;
- спроби входу в систему;
- зміна облікових політик;
- інших критичних процесів і об'єктів.

Найбільш поширеним місцем розміщення виконуваних файлів шкідливого програмного забезпечення є кореневої системний каталог Windows, внаслідок чого необхідно проводити аудит змін файлів в даному каталозі, зокрема на предмет появи нових виконуваних файлів.

Діяльність шкідливого програмного забезпечення часто супроводжується записом власних параметрів до реєстру операційної системи, зокрема в гілку автозапуску.

Діяльність шкідливого програмного забезпечення зачіпає системні файли, дописуючи шкідливий код в вихідний код файлу. Внаслідок цього змінюється розмір і контрольна сума заражених файлів.

1.2.2 Аналіз основних етапів обробки подій безпеки в системі

Процес обробки даних аудиту подій безпеки, одержуваних від будь-якого з джерел - журналів аудиту комп'ютерів мережі, може бути описаний узагальненим алгоритмом, блок-схема якого представлена на (рис. 1.4). Згідно з цим алгоритмом, в процесі обробки даних аудиту подій безпеки можна виділити чотири основні етапи.

1. Витяг даних з журналу аудиту.
2. Формалізація даних.
3. Аналіз і фільтрація подій безпеки.
4. Оповіщення про виявлені загрози і запис подій безпеки в базу даних подій безпеки.

Витяг даних з журналу аудиту полягає у виконанні операції читання даних з файлу журналу аудиту в деякий буфер. Конкретні дії, які необхідно виконати на цьому етапі залежать від способу організації зберігання подій безпеки в журналах аудиту. Сучасні засоби аудиту подій безпеки використовують два основних підходи для організації зберігання подій безпеки в файлах журналів аудиту - зберігання подій в структурованих файлах і зберігання подій в текстових файлах, де кожна окрема текстова рядок задає окрема подія. Якщо дані успішно отримані, то далі їх необхідно формалізувати, тобто перетворити дані до структур, що використовуються в системі для подання подій. Оскільки, лічені дані про події безпеки представлені в такому форматі, в якому вони зберігаються в журналі аудиту, то необхідно їх перетворити до

структури, зручною для подальшого подання в процесі обробки в системі. Для цього зазвичай необхідно виділити з масиву інформації окремі події і значення окремих полів даних структур, які задають події [4].

Рисунок 1.4 - Узагальнений алгоритм обробки даних аудиту подій безпеки

1.2.3 Аналіз діях, які шкідливого програмного забезпечення в системі

При проникненні на комп'ютери користувачів шкідливе програмне забезпечення залишає «сліди» діяльності в операційній системі у вигляді зміни файлів і параметрів, обумовлені деструктивними діями вірусів. У системах сімейства Windows існує можливість реєстрації даних подій в операційній системі за допомогою аудиту безпеки.

Деструктивну дію вірусу - стратегія його функціонування, що вживаються ним, часом непомітні для користувача, шкідливі дії спрямовані на порушення нормального функціонування операційної системи, а іноді її повного краху, а також умови, при яких вірус вступає в фазу свого прояву і його алгоритм роботи в ній.

Процес проникнення більшості вірусів може бути описаний таким чином:

- будучи запущеним необережним користувачем, створює в один з каталогів - найбільш часто в каталоги: Windows, System, System32, Temp, Application Data - файли під різними іменами з найбільш частим розширенням .exe, .dll, .dat, .ini, .bat ;

- для забезпечення свого запуску при кожному завантаженні Windows прописується в реєстрі в секції автозавантаження HKLM \ software \ microsoft \ windows \ currentversion \ run,

- або записує необхідні дані до реєстру, найчастіше в розділ HKLM \ SOFTWARE \

- створює свої копії у вигляді файлів з найбільш частими розширеннями .exe, .dll, .dat, .ini, .bat;

- функціонує відповідно до моделі деструктивної дії вірусу.

приклад:

Win32.HLLM.MyDoom.33808

Тип вірусу: Поштова черв'як масової розсилки

Уразливі ОС: Win95 / 98 / Me / NT / 2000 / XP

Розмір файлу: 22, 020 байт

Упакований: UPX

Технічна інформація

Хробак копіює себе в каталог% Windir% під ім'ям lsass.exe.

Для забезпечення свого запуску при кожному завантаженні Windows прописується в реєстрі в секції автозавантаження HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ Run "Traybar" = "% Windir% \ lsass.exe"

% Windir% - каталог з встановленою Windows.

Для свого поширення використовує власну реалізацію SMTP-протоколу.

Створює свої копії в папках, які містять підрядка

incoming ftproot download shar

у вигляді файлів з такими іменами:

index Kazaa Lite Harry Potter ICQ 4 Lite WinRAR.v.3.2.and.key Winamp 5.0 (en) Crack Winamp 5.0 (en) exe

Цим файлів присвоюються розширення:

.exe .com .ShareReactor.com .scr

Розсилає свої численні копії за адресами, які містять такі підрядки:

sales james spam abus master sample accoun privacycertific bug listserv submit ntivi suppor crosoft і т.д.

Найчастіше відсилається повідомлення про те, що відправлена кореспонденція була доставлена, і користувачеві пропонується ознайомитися з подробицями.

В поле Від може бути такий текст:

Postmaster Mail Administrator Automatic Email Delivery Software Post Office The Post Office Bounced mail Returned mail MAILER-DAEMON Mail Delivery Subsystem або підставлятися будь-якій іншій поштову адресу, знайдений в ураженій системі.

Для свого подальшого поширення шукає адреси, переглядаючи такі файли:

doc .txt .htm .html

Ім'я вкладення вибирається зі списку:

blank attachment document file letter mail message readme text transcript якому присвоюється одна з розширень:

.bat .cmd .com .exe .pif .scr .zip

Черв'як містить backdoor-процедуру: відкриває і слухає порт TCP 1042.

На підставі досліджень, проведених Лабораторією Касперського і ТОВ «Доктор Веб», і накопиченої статистки можна скласти список файлів і ключів реєстру, найбільш часто створюються або модифікуються шкідливими програмами. Така статистика може бути використана для виявлення найбільш часто вживаних вірусів.

1.2.4 Аналіз подій безпеки з метою виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин

Процес аналізу зареєстрованих подій безпеки характеризується необхідністю вирішення наступних основних завдань:

1. Об'єднання подій, отриманих з різних джерел, наприклад зареєстрованих на різних комп'ютерах мережевий інформаційного середовища.

2. Усунення надмірності журналу аудиту.

3. Пошук подій, які відповідають певним умовам.

4. Обробка подій «вручну».

5. Класифікація зареєстрованих подій безпеки.

6. Оповіщення персоналу, відповідального за безпеку, про факти виявлення особливо важливих подій.

При об'єднанні подій в єдиний журнал системні події утворюють журнал, який експортується в текстовий файл. Журнал представляє собою опису подій, розділені символом-роздільником. При експорті роздільником є символ «. Текстовий формат зберігання даних дозволяє розробникам засобів аудиту істотно спростити операції запису даних аудиту в журнали аудиту. Перегляд і обробка даних аудиту в текстовому форматі також є простими процедурами. Для цього необхідно провести розбір рядків текстового файлу журналу аудиту і виділити в них значення окремих полів запису про подію. Недоліком є те, що при текстовому способі зберігання даних аудиту стає неможливим довільне читання даних з журналу аудиту, дані можуть бути прочитані тільки послідовно [5].

Усунення надмірності журналу аудиту, тобто скорочення числа подій для подальшої обробки на підставі «чорного» і «білого» списків.

Як було сказано раніше, віруси при проникненні створюють файли і ключі реєстру, які на підставі досліджень, проведених Лабораторією Касперського і ТОВ «Доктор Веб», і накопиченої статистки дозволяють скласти список файлів і ключів реєстру, найбільш часто створюються або модифікуються

шкідливими програмами. Така статистика, регулярно оновлювана, може служити основою для «чорного» списку, який буде застосований для пошуку подій, що відносяться до цих файлів і ключів.

Так само, для значного зменшення числа подій доцільно використовувати «білий» список. «Білий список» слід формувати з довірених додатків і доповнювати при інсталяції нової програми.

Результатом застосування «чорного» і «білого» списків має бути формування списків несанкціонованих подій, санкціонованих подій і подій, призначених для подальшої обробки.

Пошук подій, які відповідають певним умовам. При необхідності провести сортування за такими критеріями як Дата / Час.

Обробка подій «вручну» полягає в перегляді та аналізі окремих подій адміністратором. На підставі знань адміністратора про систему, в якій здійснюється аудит, і його досвіду адміністратор виносить рішення про приналежність аналізованого події до одного з класів. Виділимо три класи: санкціоновані події, несанкціоновані події і «сумнівні» події. «Сумнівні» події - це ті події, щодо яких не можна зробити однозначного висновку є вони санкціонованими чи ні. Такі події вимагають перевірки із застосуванням додаткових коштів.

При віднесення події до одного з класів, визначається, до якого об'єкту відноситься подія (якщо категорія події - Аудит доступу до об'єктів), проводиться пошук всіх подій, що трапилися з цим об'єктом, і віднесення знайдених подій до того ж класу.

Класифікація зареєстрованих подій безпеки

На підставі попередніх пунктів складається три списки подій:

- список несанкціонованих подій, складений з подій, визначених «чорним» списком і відібраних адміністратором;

- список санкціонованих подій, складений з подій, визначених «білим» списком і відібраних адміністратором;

- список «сумнівних» подій.

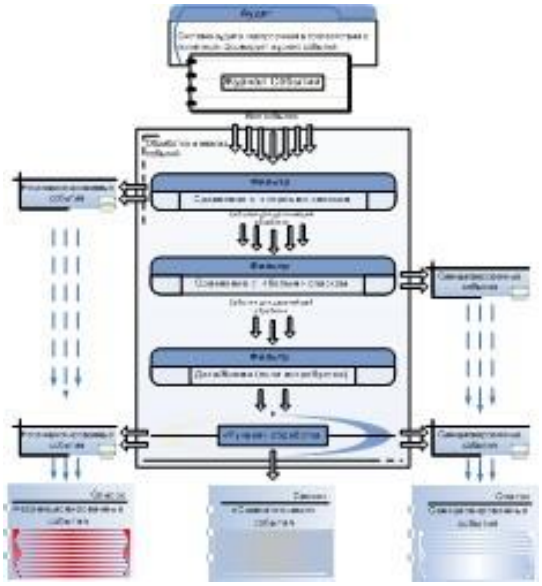


Рисунок 1.5 - Методика аналізу подій системи з метою виявлення несанкціонованого доступу ПО до ресурсів обчислювальних машин

1.3 Висновки

1. Процес аналізу зареєстрованих подій безпеки характеризується необхідністю вирішення наступних основних завдань: об'єднання подій, отриманих з різних джерел, наприклад зареєстрованих на різних комп'ютерах мережевий інформаційного середовища; усунення надмірності журналу аудиту; пошук подій, що відповідають певним умовам; обробка подій «вручну»; класифікація зареєстрованих подій безпеки; оповіщення про факти виявлення особливо важливих подій.

2. Системні події утворюють журнал, який імпортується в текстовий файл.

3. Журнал представляє собою опису подій, розділені символом-розділь-ником.

4. Усунення надмірності журналу аудиту відбувається на підставі «чорного» і «білого» списків.

5. Обробка подій «вручну» полягає в перегляді та аналізі окремих подій адміністратором.

6. Складається три списки подій: несанкціонованих подій, санкціонованих подій, «сумнівних» подій, що і є результатом.

2 РОЗРОБКА ПРОГРАМНОГО ЗАСОБУ АНАЛІЗУ ПОДІЙ СИСТЕМ РОДИНИ WINDOWS НА ОСНОВІ РОЗРОБЛЕНОЇ МЕТОДИКИ АНАЛІЗУ ПОДІЙ

2.1 Настройка системи аудиту windows на основі існуючої методики аналізу аудиту подій

Для реалізації програмного засобу моніторингу і аналізу подій безпеки необхідна правильна настройка системи аудиту подій Windows відповідно до обраної політикою безпеки.

До цієї політику повинні бути включені наступні критерії:

- об'єкти, що підлягають аудиту (файли, папки, ключі реєстру);

- результуюче властивість події доступу (успіх, відмова);

- тип події (події додатків, безпеки, установки, системні, що пересилаються);

- контрольовані користувачі (повний перелік користувачів, контроль за діями яких повинен бути врахований).

В якості базової політики безпеки обрана політика аудиту доступу до об'єктів, що мають важливе значення для функціонування системи Windows, а також найбільш часто піддаються атакам шкідливого програмного забезпечення.

Контрольовані об'єкти:

- C: \ Windows \ System32 \;

- C: \ Program files \;

- C: \ Documents and Settings \;

- C: \ Windows \.

Перераховані каталоги є базовими для реалізованої політики аудиту.

Алгоритм налаштування системи аудиту для кожного з об'єктів ідентичний і розглянутий на прикладі налаштування системи аудиту для каталогу C: \ Windows \ System32 \.

Меню настройки аудиту знаходиться на вкладці Безпека меню властивості каталогу. При натисканні кнопки Додатково з'являється меню настройки розширеної безпеки, в якому необхідно вибрати вкладку Аудит.

Налаштування аудиту гнучкі, і дозволяють врахувати більшість потреб адміністратора з інформаційної безпеки при реалізації загальної політики аудиту для системи.

Для кожного користувача можна налаштувати індивідуальні параметри аудиту для більш детального опрацювання політики безпеки.

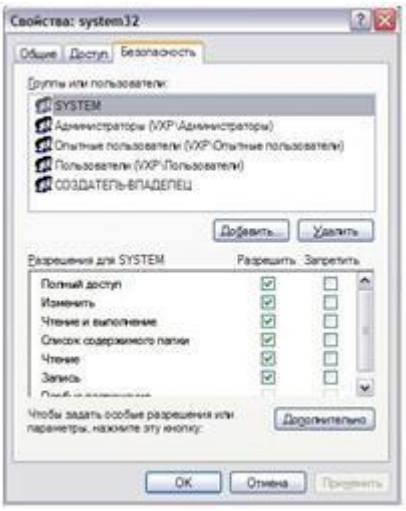


Рисунок 2.1 - Налаштування властивостей безпеки каталогу

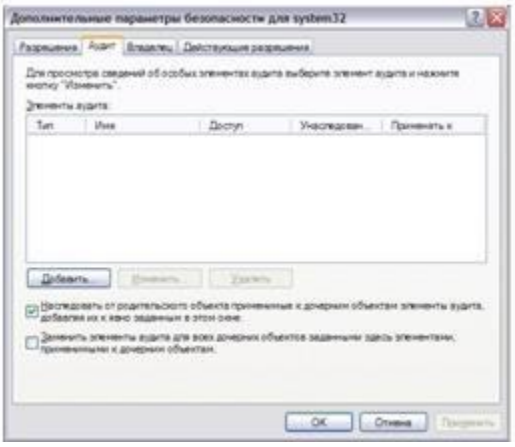


Рисунок 2.2 - Додавання аудиту для обраних користувачів

Для додавання аудиту дій певного користувача необхідно натиснути кнопку додати і вибрати необхідних користувачів, після чого відкриється вікно з вибором критеріїв для аудиту.

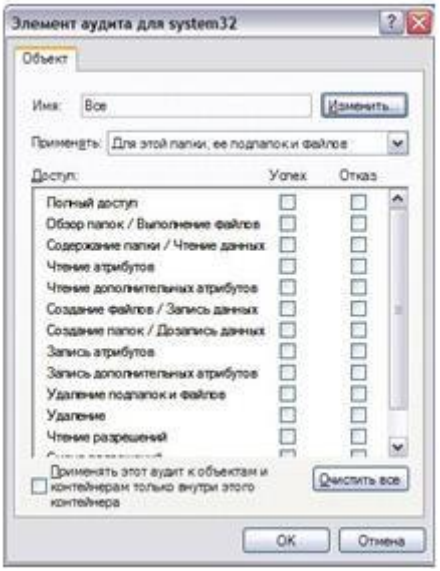


Рисунок 2.3 - Вибір критеріїв формування журналу аудиту

Для запобігання надмірності створюваного журналу необхідно вибрати в якості критеріїв тільки необхідні для подальшого аналізу - Огляд папок / Виконання файлів і Створення файлів / Запис даних. Для більш детального аналізу можна додати деякі інші критерії [6].

Після застосування параметрів аудиту в Журналі аудиту будуть фіксуватися всі події, що задовольняють заданим критеріям.

Схема формування журналу аудиту в залежності від обраних критеріїв представлена на (рис. 2.4).

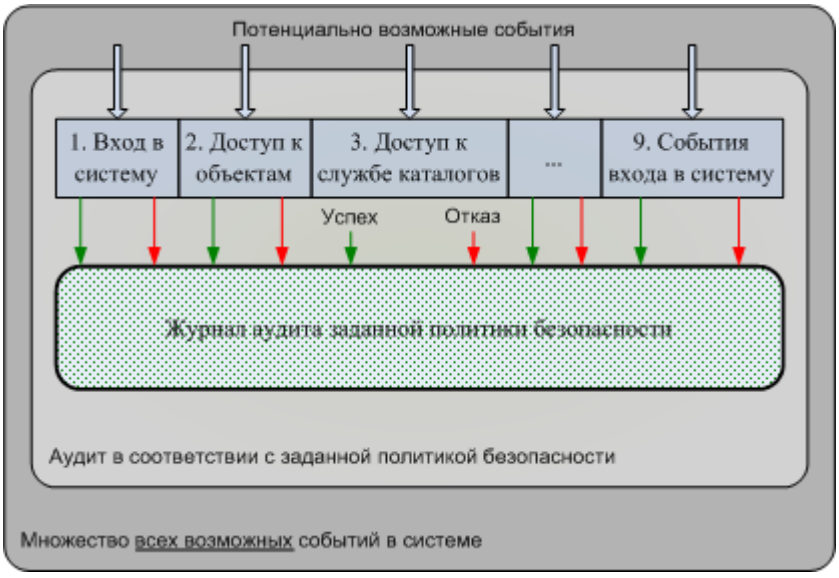


Рисунок 2.4 - Формування журналу аудиту відповідно до заданої політикою аудиту

2.2 Функціональне призначення реалізовану програмного засобу

Функціональне призначення розроблюваного програмного засобу являє собою сукупність наступних критеріїв:

1. Пошук несанкціонованих подій в сформованому системою аудиту журналі на основі деякої локальної або віддаленої бази шкідливого програмного забезпечення.

2. Усунення надмірності журналу.

3. Пошук подій за умовою і сортування.

4. «Ручна» обробка.

5. Висновок результатів.

Кожен етап передбачає видачу проміжних результатів аналізу журналу, що включають в себе імена файлів, що є підозрілими, кількість знайдених підозрілих подій, код події (створення, зміна).

На етапі пошуку по локальних або віддалених баз даних відбувається аналіз на відповідність, так званого, «чорного списку» відомих шкідливих програм.

На етапі усунення надмірності журналу відбувається видалення записів, свідомо є санкціонованими (певні системні події).

На етапі сортування за принципом етапу усунення надмірності відбувається видалення подій, які не потрапляють в ті чи інші, задані користувачем тимчасові рамки.

На етапі «ручний» обробки користувач має можливість самостійно впорядкувати залишилися після попередніх етапів необроблені підозрілі події.

На етапі аналізу отриманих даних користувач проводить експорт отриманих результатів з метою подальшої індивідуальної опрацювання кожного підозрілого події і запобігання несанкціонованого доступу програмного забезпечення до ресурсів обчислювальної машини.

Даний узагальнений алгоритм представлений на (рис. 2.5).

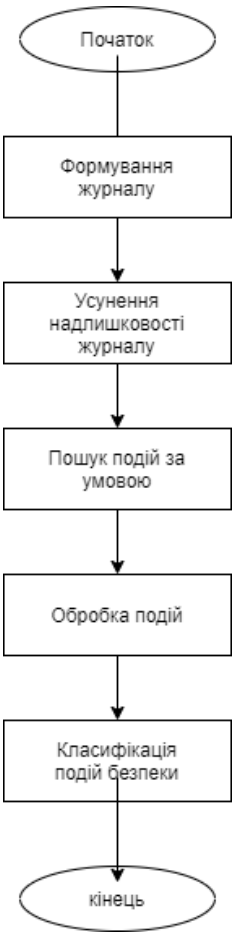


Рисунок 2.5 - Узагальнений алгоритм обробки журналу подій реалізованим програмним засобом

2.3 Розробка методу вилучення інформації про події безпеки з журналів аудиту

Як середовище розробки програмного засобу обрано середовище Delphi 7.

Вхідними даними для програмного засобу служить експортований журнал подій аудиту, сформований раніше при налаштуванні системи аудиту; «Чорний список» злісних програм, які отримують несанкціонований доступ до об'єктів системи; «Білий список» санкціонованих програм, службовець для усунення надмірності оброблюваного журналу [7].

Аналіз по базах санкціонованих і несанкціонованих програм відбувається шляхом пошуку в запису події відповідності імені файлу.

Кожна подія, що формується системою аудиту має такий вигляд:

1. Дата - дата появи події.

2. Час - час запису події.

3. Джерело - позначення ПО, який записав подію.

4. Тип - тип події за класифікацією Windows 2000: «Помилка», «Попередження», «Відомості», «Аудит успіхів» або «Аудит відмов».

5. Категорія - клас подію відповідно до визначення в джерелі, записав цю подію (Таблиця 1.1).

6. Код (ID) - номер визначає конкретну подію.

7. Користувач - ім'я користувача до якого відноситься подія.

8. Комп'ютер: точне ім'я комп'ютера, на якому було зареєстровано подія.

На основі аналізу даних в кожному з цих полів можна робити вибірку необхідної інформації.

2.4 Впровадження методів і алгоритмів формалізації і класифікації даних про події безпеки в реалізовану програмний засіб

На основі методики аналізу засобів аудиту подій систем сімейства Windows для виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин та методу отримання інформації про події безпеки з журналів аудиту, необхідно розробити деталізований алгоритм аналізу подій безпеки [8].

Деталізований алгоритм аналізу подій безпеки програмного засобу представлений на (рис. 2.6).

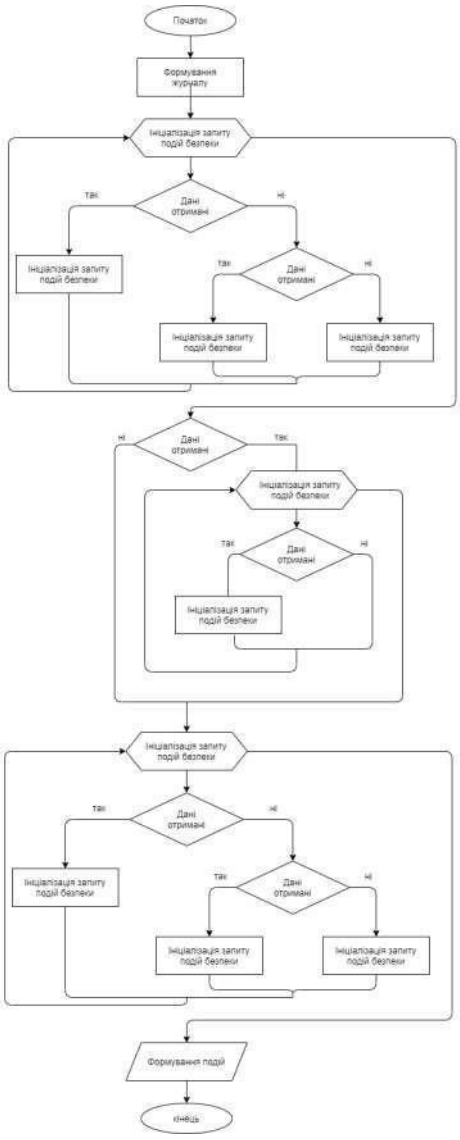


Рисунок 2.6 - Деталізований алгоритм аналізу подій безпеки

У разі, коли необхідно проаналізувати журнал тільки на створені файли, або тільки на змінені файли необхідно використовувати фільтри системи аудиту для створення відсортованих за кодами події журналів. Подальший експорт журналу з системи аудиту в програмний засіб дозволить враховувати тільки обрані коди подій [9].

В процесі роботи програмного засобу формуються три списки подій:

- список несанкціонованих подій, складений з подій, визначених «чорним» списком і відібраних адміністратором;

- список санкціонованих подій, складений з подій, визначених «білим» списком і відібраних адміністратором;

- список сумнівних подій.

Дані списки можна експортувати для подальшого опрацювання вад системи захисту і усунення шкідливих програм.

Зовнішній вигляд програмного засобу представлений на (рис. 2.7).

Інтерфейс включає в себе кілька полів для відображення проміжної інформації аналізу.

Виберіть Заборонені події, Дозволені події, Сортування, Ручна обробка - відповідають чотирьом етапам обробки вихідного журналу, що дозволяє більш детально опрацювати кожне зафіксоване системою аудиту подія.

Кнопки Завантажити журнал, Завантажити базу, Експортувати - служать відповідно для імпорту баз і експорту поточного обробленого журналу.

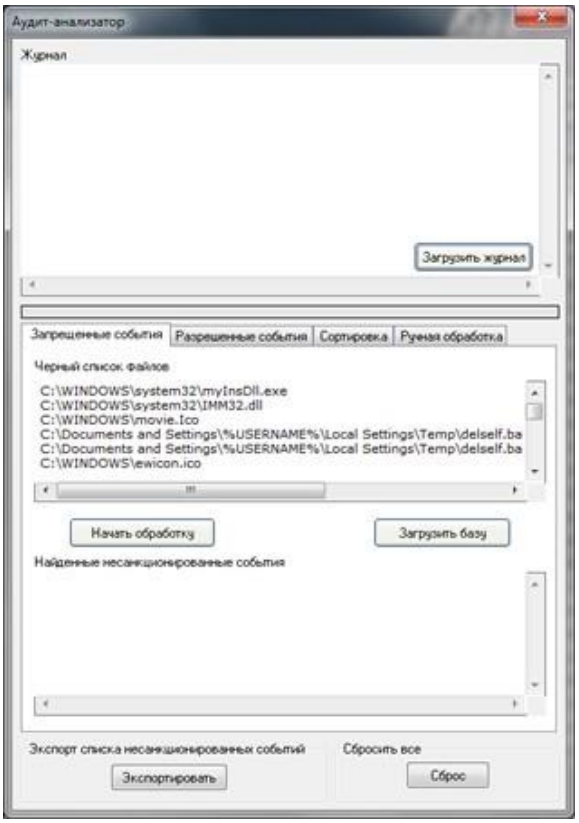


Рисунок 2.7 - Інтерфейс програмного засобу

2.5 Висновки

На основі проведений досліджень, була розглянута передбачувана структура системи моніторингу подій безпеки. Проведено аналіз основних етапів обробки подій безпеки в системі. Вивчено деструктивні дії шкідливого програмного забезпечення. Розроблено методику аналізу подій з метою запобігання несанкціонованого доступу ПО до ресурсів обчислювальних машин.

На підставі аналізу отриманих даних можна зробити наступні висновки:

1. Система повинна обробляти дані про події безпеки, які добувають із журналів аудиту.

2. Система моніторингу подій безпеки складається з агентів, які формують журнал, монітора подій безпеки, який забезпечує обробку даних про події безпеки, і модуля відображення, призначеного для відображення і дослідження результатів роботи монітора подій безпеки.

3. Обов'язковою складовою методики повинен бути аудит критично важливих об'єктів операційної системи.

4. Процес обробки даних аудиту подій безпеки може бути описаний алгоритмом.

5. У цьому алгоритмі можна виділити чотири основні етапи: вилучення даних з журналу аудиту, формалізація даних, аналіз і фільтрація подій безпеки, оповіщення про виявлені загрози.

6. При проникненні на комп'ютери користувачів шкідливе програмне забезпечення залишає «сліди» діяльності в операційній системі у вигляді зміни файлів і параметрів, обумовлені деструктивними діями вірусів.

7. Процес проникнення більшості вірусів може бути описаний таким чином: будучи запущеним, створює в один з каталогів файли, для забезпечення свого запуску при кожному завантаженні Windows прописується в реєстрі в секції автозавантаження, або записує необхідні дані до реєстру, створює свої копії у вигляді файлів , функціонує відповідно до моделі деструктивної дії вірусу.

3 АНАЛІЗ РЕЗУЛЬТАТІВ РОБОТИ РЕАЛІЗОВАНІ ПРОГРАМНО КОШТИ ТА РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ В ВИДІЛЕНИЙ СЕГМЕНТ ІНФОРМАЦІЙНОЇ СТРУКТУРИ ПІДПРИЄМСТВА

3.1 Аналіз інформаційної структури виділеного для реалізації сегменту мережі підприємства

Розроблена методика аналізу подій систем сімейства Windows може бути застосована практично до будь-якої інформаційної структурі підприємства і була впроваджена в інформаційну структуру Ставропольського філії підприємства [10].

Корпоративна мережа підприємства.

В якості базового мережевого протоколу в корпоративної мережі підприємства використовується протокол TCP / IP.

Як адресного простору використовується мережа класу A - 10.0.0.0/8, певна документом IETF RFC +1597 для приватних IP-мереж. У корпоративної мережі підприємства виділяються наступні типи адресних просторів:

- адресні простори, виділені філіальних фрагментами;
- адресні простори, виділені апарату управління підприємством;
- адресний простір для адресації магістрального сегменту корпоративної мережі;
- резервне адресний простір.

Використовувана схема розподілу адресного простору маркується наступним чином 10.xyz, де: x - номер філії; y - номер віртуальної мережі (VLAN) всередині філії; z - номер пристрою всередині віртуальної мережі.

Сервери.

Серверна структура підприємства грунтується на ОС Windows Server 2008. Функціонально вона поділяється на сервери підтримки спеціалізованих додатків, сервери підтримки загальнодоступних сервісів і сервери, що підтримують технологічні служби корпоративної мережі.

Робочі станції.

До інформаційної системи підприємства підключені автоматизовані робочі місця користувачів, що функціонують на базі ОС Microsoft Windows XP.

Лінії зв'язку і активне мережеве обладнання

Основу ІС становить стек комутаторів і маршрутизаторів Cisco Systems Inc. Виділені магістральні канали обміну даними використовуються для забезпечення зовнішнього інформаційного взаємодії ІС з філіями підприємства, районними експлуатаційними службами, а також для доступу до глобальної інформаційної мережі Інтернет [11].

Види інформаційних ресурсів, що зберігаються і обробляються в системі.

В ІС підприємства зберігаються і обробляються різні види відкритої та службової конфіденційної інформації.

До конфіденційної та службової інформації, що циркулює в КСПД, відносяться:

- персональні дані співробітників підприємства і партнерів, збережені в БД і передаються по мережі;

- повідомлення електронної пошти та інформація БД, що містять службові відомості, інформацію про діяльність підприємства і т.п .;

- конструкторська і технологічна документація, перспективні плани розвитку, модернізації виробництва, реалізації продукції та інші відомості, що становлять науково-технічну і технологічну інформацію, пов'язану з діяльністю підприємства;

- фінансова документація, бухгалтерська звітність, аналітичні матеріали досліджень про конкурентів і ефективності роботи на фінансових ринках;

- інші відомості, що становлять ділову інформацію про внутрішню діяльність підприємства.

Конфіденційна інформація, яка може поширюватися через IP, містить інформацію стратегічного характеру, і її розкриття порушує функціонування компанії, безпосередньо впливає на її життя і розвиток, а також відновлює

діяльність і престиж компанії. Завдає непоправної шкоди і веде до досягнення стратегічних цілей її політика і в кінцевому підсумку її падіння

Категорія "Публічна" містить всю іншу неконфіденційну інформацію.

Потік внутрішньої інформації. В ІС призначаються наступні інформаційні потоки.

Передача файлів між файловим сервером і призначеної для користувача робочою станцією по протоколу smb (відкритий протокол обміну інформацією між користувачем і сервером на основі стека tcp / ip).

- передача повідомлень електронної пошти, за допомогою використання хешувати з'єднання програмного забезпечення lotus notes;

- передача юридичної і довідкової інформації між серверами БД і призначеними для користувача робочими станціями;

- ділове листування;

- передача звітної інформації;

- передача бухгалтерської інформації між призначеними для користувача робочими станціями і сервером БД в рамках автоматизованих систем «1С бухгалтерія», «1С зарплата і кадри», «оперативний облік».

Зовнішні інформаційні потоки.

В якості зовнішніх інформаційних потоків використовуються:

- передача звітних документів (виробничі дані) від філій підприємства, по каналах корпоративної мережі, а також з використанням магнітних носіїв;

- передача платіжних документів в банки;

- передача фінансових і статистичних звітних документів від філій підприємства;

- внутрішньовідомчий і міжвідомчий обмін електронною поштою;

- передача інформації по комутованих каналах віддаленим користувачам;

- різні види інформаційних обмінів між ІС і мережею інтернет.

Для впровадження розроблюваного програмного засобу було виділено сегмент корпоративної мережі, що містить сервера БД Справа 11.0, БД Гарант-

MAX, БД Гарант-регіони. Розгортання серверів Windows Server 2008 було вироблено в середовищі віртуальних машин vmWare vSphere, функціонування яких обумовлено апаратної платформою IBM BladeCenter E до встановлених серверами-лезами HS 22. Як файлового сховища виступає SAS RAID сховище IBM System Storage DS3512.

Сегмент має два мережевих підключення до мереж MPLS і до відомчої мережі.

Інформаційна структура виділеного для впровадження ділянки інформаційної структури представлена на (рис. 3.1).

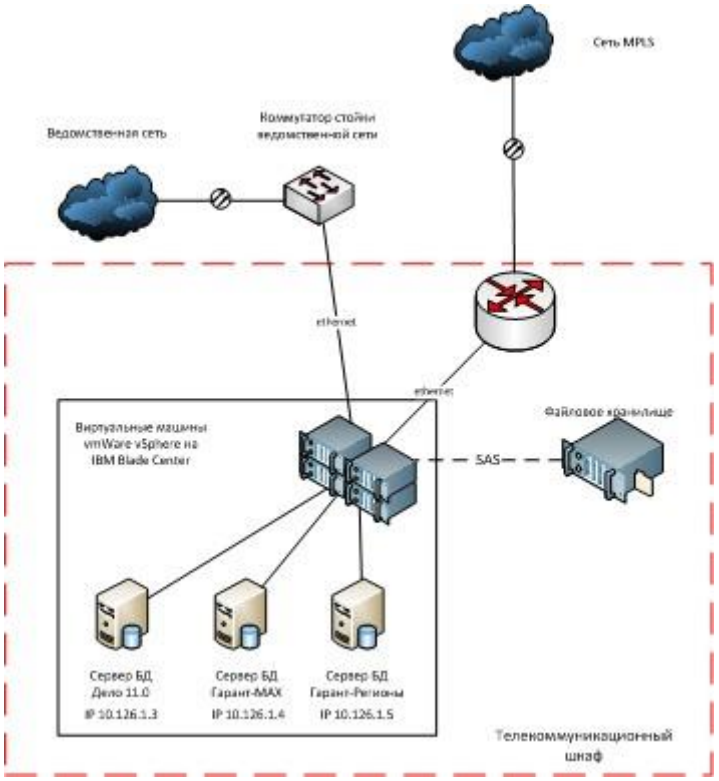


Рисунок 3.1- Виділений сегмент інформаційної структури підприємства

3.2 Аналіз загроз інформаційній безпеці, що привласнюються реалізацій сегментів інформаційної структури підприємства

Модель порушника корпоративної інформаційної безпеки

Порушник ІБ - це особа, яка може завдати шкоди інформаційних ресурсів компанії в результаті навмисного або ненавмисного поведінки.

Атаки на ресурси корпоративної мережі - це спроби пошкодити інформаційні ресурси систем, підключених до мережі. Атаки можуть здійснюватися прямо або побічно зловмисником, за допомогою процесу, що виконується від імені зловмисника, або шляхом реалізації його в системному програмному забезпеченні або закладках обладнання, комп'ютерні віруси, троянських конях і т. д. [12]

Відповідно до моделі, всі злочинці діляться на зовнішніх і внутрішніх по підрозділах, що забезпечують функціонування IP компанії.

внутрішній злочинець

Інсайдерами можуть бути співробітники наступних категорій сервісних служб:

Розважальний персонал (системні адміністратори, адміністратори баз даних, адміністратори додатків і т. Д., Відповідальні за експлуатацію та технічне обслуговування обладнання і програмного забезпечення).

-Програміст, що відповідає за розробку і обслуговування системного та прикладного програмного забезпечення.

- технічний персонал (допоміжні робітники, прибиральниці і т. Д.);

-Співробітники бізнес-підрозділу компанії, яким надано доступ до об'єктів, на яких встановлено комп'ютер або комунікаційний пристрій.

Передбачається, що несанкціонований доступ сторонніх до об'єктів в системі буде усунутий за допомогою заходів фізичної безпеки (охорона території, організація доступу і т. Д).

Припущення щодо підсудності внутрішніх злочинців формулюються наступним чином:

Внутрішні злочинці.

Досвідчені професіонали в розробці і експлуатації програмного і апаратного забезпечення.

Знати деталі завдань, що вирішуються службою ІБ компанії.

Системний програміст, який може змінити поведінку операційної системи.

Корректно відображати функціональні характеристики системи і процесів, що беруть участь в зберіганні, обробці та відправці важливої інформації.

Ви можете використовувати як стандартне обладнання, так і програмне забезпечення, що входять до складу вашої системи, а також спеціальні інструменти для аналізу та злому вашої комп'ютерної системи.

Внутрішні порушники поділяються на п'ять категорій залежно від того, як вони отримують доступ до системних ресурсів і наданих їм привілеїв [13].

Категорія А: Ті, хто не зареєстрований в системі і яким дозволений доступ на об'єкт з обладнанням. Користувачі категорії А можуть: Ви можете отримати доступ до інформації, що доставляється через внутрішні канали зв'язку вашої корпоративної мережі. Отримайте інформацію про топології мережі, які використовуються протоколах зв'язку і мережевих службах. Він має ім'я зареєстрованого користувача системи і досліджує свій пароль користувача.

Категорія В: Зареєстровані користувачі системи, які отримують доступ до системи з віддаленої робочої станції. Категорія В Люди: ви можете використовувати всі функції категорії А. People. Я знаю принаймні одне припустиме ім'я доступу. У нього є всі атрибути, необхідні для надання доступу до системи (наприклад, зломи). Забезпечує доступ до баз даних, файлових серверів корпоративної мережі та інформації, що зберігається на робочих станціях користувачів. Права користувачів Категорії В на доступ до інформаційних ресурсів в корпоративній мережі компанії повинні відповідати політиці безпеки, прийнятої в компанії.

Категорія С: зареєстровані користувачі, які надають локальний або віддалений доступ до систем в корпоративній мережі. Люди категорії С: Мають всі здібності людей категорії В. Містить інформацію про топології

мережі, структурі бази даних і файлової системи сервера. Він має можливість реалізувати прямий фізичний доступ до інструментів IP-технологій.

Категорія D: Зареєстрований системний користувач з правами системного (мережевого) адміністратора. Люди категорії D: Має всі здібності людей категорії C. Отримайте повну інформацію про IP-адресу вашої системи і прикладного програмного забезпечення. Має повну інформацію про обладнання та конфігурації мережі. У вас є доступ до всього IP-обладнання та програмного забезпечення і ви маєте право налаштовувати апаратне і програмне забезпечення. Концепція безпеки вимагає підзвітності людей, що відносяться до категорії D, і здійснення незалежного контролю над їх діяльністю.

Категорія E: Програміст, відповідальний за розробку і обслуговування всієї системи і прикладного програмного забезпечення, використовуваного в IP. Категорія E: Можливість створення помилок, програмних закладок і установки троянів і вірусів на сервери корпоративної мережі. Ви можете використовувати фрагменти інформації про топології вашої мережі і IP-обладнанні.

Зовнішній зловмисник.

До зовнішніх порушників відносяться ті, хто не може залишатися в приміщенні з обладнанням без контролю співробітників компанії. Зовнішній зловмисник: перехоплює, аналізує і змінює інформацію, передану по лініях зв'язку за межами зони контролю. Виконує перехоплення і аналіз електромагнітного випромінювання від IP-обладнання [14].

Припущення про можливості зовнішніх злочинців формулюються наступним чином:

Кваліфікований фахівці в галузі технічних засобів перехоплення інформації.

-Дізнатися особливості вашої системи і прикладного програмного забезпечення, а також вашого IP-обладнання.

-Знати деталі рішення IP-завдань.

-Знати функціональні особливості системи і правила зберігання, обробки і передачі інформації всередині системи.

-Розуміти мережеве та канальне обладнання, а також протоколи передачі даних, що використовуються системами.

-Можна використовувати тільки послідовні пристрої, призначені для прийому інформації по кабельних лініях і бездротових каналах.

При аналізі потенційних загроз ІБ з використанням моделі порушника слід враховувати можливість змови між внутрішніми і зовнішніми порушниками.

Загрози використання мережі передачі даних слід розглядати індивідуально. Цей клас загроз характеризується доступом зловмисників до серверів баз даних, файлових серверів, маршрутизаторів і активного мережевого обладнання зсередини або ззовні. Для підприємства КСПД характерні наступні типи загроз:

ξперехоплення інформації про лінії зв'язку з використанням різних типів аналізаторів мережевого трафіку.

ξзамінювати, вставляти, видаляти або змінювати дані користувача в інформаційному потоці.

ξперехоплення інформації (наприклад, паролів користувачів), що відправляється по каналу зв'язку, для подальшого використання в обхід мережевий аутентифікації.

Статистичний аналіз мережевого трафіку (наприклад, наявність / відсутність конкретної інформації, частота передачі, напрямок, тип даних і т. Д).

джерело загрози

Виступає як зовнішній і внутрішній порушник, як джерело загроз безпеки технічних засобів системи.

Обрана політика безпеки містить такі обов'язкові елементи:

ξбрандмауер.

ξвіртуальне приватна мережа vpn.

ξvlan;

ξантивірусне захист;

ξорганізований заходи по боротьбі з несанкціонованим доступом.

Що стосується закріплених за реалізацією сегментів інформаційної структури, в розробленому проекті можливе виявлення несанкціонованого доступу до об'єктів на сервері. Зокрема, він може виявляти і класифікувати внутрішніх і зовнішніх порушників і своєчасно виявляти загрози, реалізовані з використанням програмного забезпечення.

Загрози, які реалізуються за допомогою програмного забезпечення в обраних сегментах інформаційної структури.

Використовуйте функції, що надаються Software IP, для забезпечення конфіденційності і цілісності інформаційних ресурсів, пов'язаних з несанкціонованим доступом до інформації, що зберігається і оброблюваної в системі, інформації, переданої по каналу зв'язку, і самому класу небезпеки. Більшість загроз, що розглядаються в цьому класі, реалізуються внутрішніми і зовнішніми зловмисниками, атакуючими локальні або видалені системні інформаційні ресурси. Успішна реалізація цих загроз може призвести до несанкціонованого доступу до інформації бази даних, файловим системам корпоративної мережі, даних, що зберігаються на робочих станціях оператора, конфігурацій маршрутизаторів і іншому активного мережевого обладнання [15].

В цьому класі розглядаються наступні основні типи загроз:

ξвикористання вірусів і інші деструктивні програмні ефекти.

ξпоказники порушення цілісності файлів.

ξпомилки коду і конфігурації для активного мережного обладнання.

ξаналіз та зміни програмного забезпечення.

ξпрограмне забезпечення має неоголошені функції, які залишені для налагодження або навмисно реалізовані.

ξмоніторинг активності системи за допомогою програмних засобів і утиліт wasp для аналізу мережевого трафіку. утиліта wasp надає інформацію про стан вашої системи і підключає вас до мережі.

ξвикористовує уразливості програмного забезпечення, щоб зламати захист програмного забезпечення, отримати несанкціонований доступ до інформаційних ресурсів і поставити під загрозу їх доступність.

ξодин користувач здійснює незаконну дію від імені іншого користувача («маскарад»).

ξрозкриття, перехоплення і крадіжка секретних кодів і паролів.

ξчитати оперативну пам'ять комп'ютера і іншу інформацію з зовнішніх носіїв.

ξпомилки введення керуючої інформації з арм оператора в базу даних.

ξзавантажити і встановіть в вашу систему неліцензовані, неперевірені системи і додатки.

ξпрограмне забезпечення блокує роботу користувачів системи.

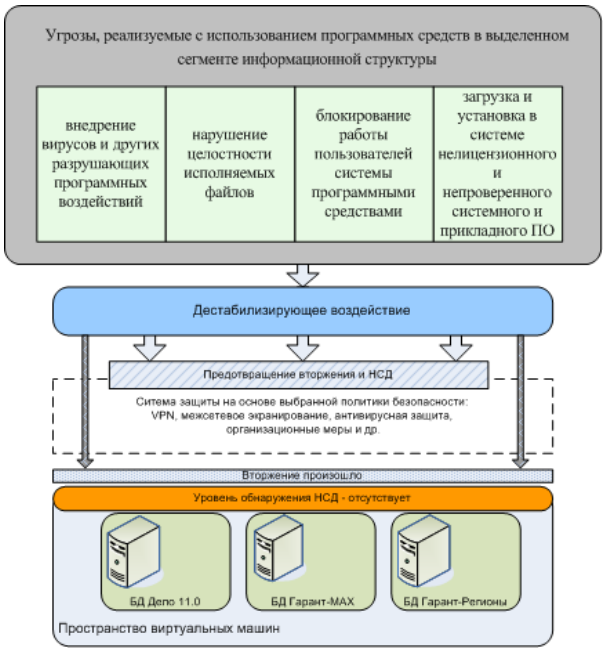


Рисунок 3.2 - Схеми загроз інформаційній безпеці з використанням програмного забезпечення в окремих сегментах інформаційної структури компанії

В разі, якщо політика безпеки виявляється неефективною, і зловмисник, подолавши всі бар'єри захисту, отримує доступ до сервера за допомогою програмних засобів, факт його діяльності повинен бути зафіксований з метою оповіщення адміністратора інформаційної безпеки і аналізу проведених дій. В існуючому сегменті інформаційної структури відсутні будь-які засоби для фіксування злочинних дій таких як:

ξдоступ до кореневого системному каталогу Windows і його підкаталогам;

ξдоступ до реєстру Windows;

ξдоступ до системних файлів;

ξдоступ до кореневого системному сховища System Volume Information;

ξдоступ до об'єктів автозапуску;

ξспроби входу в систему;

ξзміна облікових політик;

ξдоступ до інших критичним процесам і об'єктам.

Наведена на (рис. 3.2) схема загроз, що реалізуються з використанням програмних засобів відображає цей факт.

При дослідженні виділеного для реалізації сегмента інформаційної структури підприємства на предмет загроз інформаційній безпеці найбільш значущими і деструктивними визнані загрози інформаційної безпеки з використанням програмних засобів. При отриманні несанкціонованого доступу за допомогою програмних засобів до ресурсів обчислювальної машини, на якій функціонує база даних одного з відомчих програмних продуктів зловмисник може завдати значної шкоди. Для своєчасного виявлення і фіксації факту несанкціонованого доступу адміністратором інформаційної безпеки підприємства необхідно такий засіб, яке дозволяло б вирішувати поставлену задачу без утруднення доступності інформації для кінцевих користувачів. Найбільш підходящим засобом реалізації поставленого завдання обрана вбудована система аудиту в системах сімейства Windows. Оскільки система аудиту систем сімейства Windows являє собою потужний засіб, що дозволяє гнучко налаштувати аудит доступу до файлів і інших об'єктів, необхідно провести грамотну настройку даної системи. Метою проекту є розробка методики аналізів результатів роботи системи аудиту з подальшим зручним поданням отриманої інформації адміністратору з інформаційної безпеки [14].

3.3 Аналіз результатів впровадження реалізувати програмного засобу в виділений сегмент інформаційної структури підприємства

Впровадження розробленого програмного засобу в виділений сегмент інформаційної структури підприємства полягало в наступному:

1. Налаштування політик аудиту безпеки відповідно до вимог.

2. Встановлення та розгортання програмного засобу обробки журналів аудиту відповідно до розробленої методики.

3. Аналіз виявлених порушень та моделювання загрози несанкціонованого доступу шляхом навмисного внесення в список заборонених подій, свідомо дозволених.

В результаті впровадження програмного засобу були виявлені деякі незначні порушення доступу користувачів до загальних файлів і папок на виділених серверах.

В результаті моделювання загрози несанкціонованого доступу шляхом внесення завідомо дозволених подій в список заборонених була оцінена ефективність роботи програмного засобу. Всі дії несанкціонованого об'єкта були відслідковані. Аналіз журналу зайняв не більше 3 хвилин.

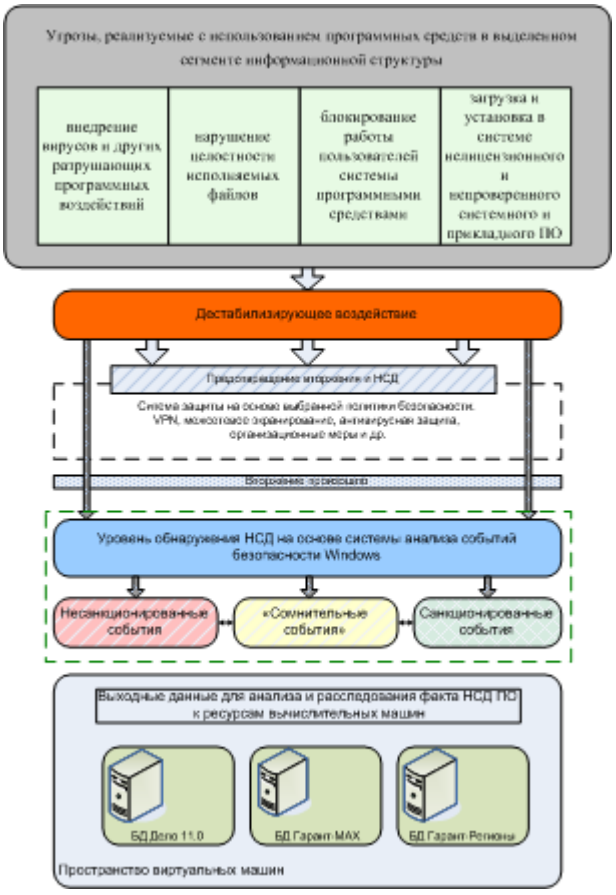


Рисунок 3.3 - Схема загроз інформаційній безпеці з використанням програмних засобів в виділеному сегменті інформаційної структури підприємства

Модель виявлення загроз, що реалізуються з використанням програмних засобів представлена на (рис. 3.3).

3.4 Аналіз результатів роботи реалізувати програмного засобу

Докладний алгоритм роботи з програмним засобом описаний далі:

На першому етапі необхідно імпортувати раніше сформований системою аудиту журнал в форматі * .txt - Завантажити журнал. Якщо журнал присутній в папці з програмою - завантаження відбудеться автоматично при запуску. База даних «чорного списку» також може бути завантажена автоматично або при натисканні кнопки - Завантажити базу. Формат бази «чорного списку» - ім'я та шлях до файлу з нового рядка в форматі * .txt. Після проведення попереднього завантаження вхідних даних необхідно натиснути кнопку - Почати обробку для пошуку несанкціонованих подій, які відповідають «чорному списку». Результат виконання цієї процедури (рис. 3.4).

В результаті виконання процедури було знайдено 15 відповідностей на шкідливий файл C: \ Windows \ system32 \ mmc.exe (доданий в базу «чорного списку» заздалегідь для прикладу). Отриманий список несанкціонованих подій можна експортувати для передачі особі, відповідальній за безпеку функціонування комп'ютера [15].

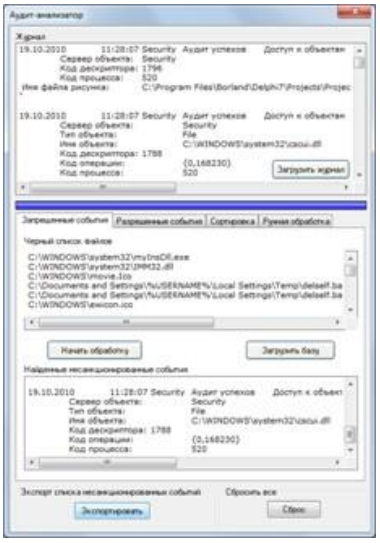


Рисунок 3.4 - Інтерфейс програмного засобу на першому етапі

На другому етапі роботи з програмою необхідно зменшити надмірність шляхом видалення з обробленого на минулому етапі журналу свідомо санкціонованих подій, що визначаються «білим списком». Як і у випадку з іншими вхідними даними «білий список» може бути завантажений і в автоматичному, і в ручному режимі. Після натискання кнопки - Продовжити обробку відбудеться відділення від вихідного журналу всіх санкціонованих подій. Отриманий журнал санкціонованих подій також можна експортувати для передачі. Результат роботи програми на другому етапі представлений на (рис. 3.5). З безлічі всіх подій були виділені події пов'язані з файлами msaudite.dll і Delphi7, так як вони присутні в списку довірених програм [17].

Зменшення надмірності дозволяє підвищити швидкодію роботи програми, а також провести чітку межу між «сумнівними» подіями і подіями, явно дозволеними. Завдяки подібному поділу на наступних етапах буде досягнутий оптимальний баланс між автоматично обробленим журналом, і журналом, яке обробляється вручну користувачем програмного засобу.

На даному етапі можна оперативно змінювати список дозволених програм, шляхом редагування відповідного поля або завантаження цілого списку дозволених програм. Завдяки цьому користувач має можливість випробувати різні списки дозволених програм для більш гнучкого аналізу.

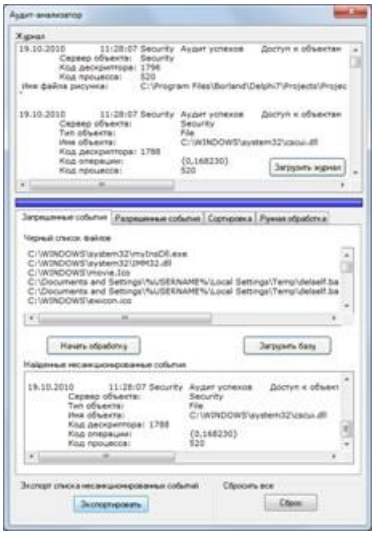


Рисунок 3.5 - Інтерфейс програмного засобу на другому етапі

На третьому етапі роботи програми є можливість відсортувати журнал, який залишився після попередніх етапів, за часом, датою, датою створення. Також є можливість експортувати відсортований список подій. На (рис. 3.6) показаний результат роботи програми після третього етапу роботи. Була проведена сортування журналу за датою 19.10.2010 в проміжку від 9:48:40 до 11:48:43.

Тимчасовий поділ подій грає важливу роль в процесі аналізу подій, сформованих системою аудиту Windows. Завдяки чіткому ведення графіка відвідуваності і використання комп'ютера, адміністратор або фахівець з інформаційної безпеки може виробляти вибірки за часом, відповідні знаходженню біля комп'ютера того чи іншого користувача. Це необхідно для подальшого формування загальної картини дій користувача, які спричинили за собою несанкціонований доступ програмного забезпечення до ресурсів обчислювальної машини. Залежно від отриманих на даному етапі даних фахівець з інформаційної безпеки може зробити висновки і внести відповідні поправки до повноважень користувачів на даному комп'ютері - заборонити будь-які дії, або навпаки дозволити. Найбільш точний аналіз досягається при одночасній сортування за датою і за часовим проміжком. На даному етапі також можливе вивантаження проміжного журналу для аналізу, незалежно скільки разів користувач проводив сортування вихідного журналу подій [18].

Рисунок 3.6 - Інтерфейс програмного засобу на третьому етапі

На останньому етапі роботи програми користувач має можливість вручну впорядкувати залишилися після попередніх етапів події. Кожна подія може бути марковано відповідними кнопками, після натискання яких події будуть заноситься відповідно в той чи інший список. На даному етапі є можливість експортувати кожен зі списків, а також переглянути повний звіт по чотирьом етапам роботи програми. У прикладі показано, як користувач відсортував події, пов'язані з файлом msimtf.dll в список несанкціонованих, а події, пов'язані з файлом csrss.exe – в список санкціонованих. На (рис. 3.7) показаний результат виконання четвертого етапу роботи програми.

Четвертий етап функціонування програми повинен бути виконаний в присутності безпосереднього фахівця в даній області – адміністратора, або фахівця з інформаційної безпеки, оскільки даний етап вимагає знання архітектури подій, що формуються системою аудиту. На підставі всіх застосованих раніше критеріїв користувач може, грунтуючись на різних параметрах події вибирати приналежність події до шкідливим або до санкціонованим. Отримані після ручного аналізу журнали підлягають вивантаженню і детальному дослідженню, оскільки як правило на цьому етапі можна виявити програмне забезпечення, що раніше не вказане в базі несанкціонованих програмних засобів.

Заключний етап функціонування програмного засобу представлений на (рис. 3.8). На даному етапі відбувається висновок статистичних даних обробки, формування остаточного списку несанкціонованих подій і експорт результатів, отриманих після обробки вихідних даних. На основі отриманих статистичних даних фахівець з інформаційної безпеки може простежити факт несанкціонованого доступу і провести розслідування даного факту.

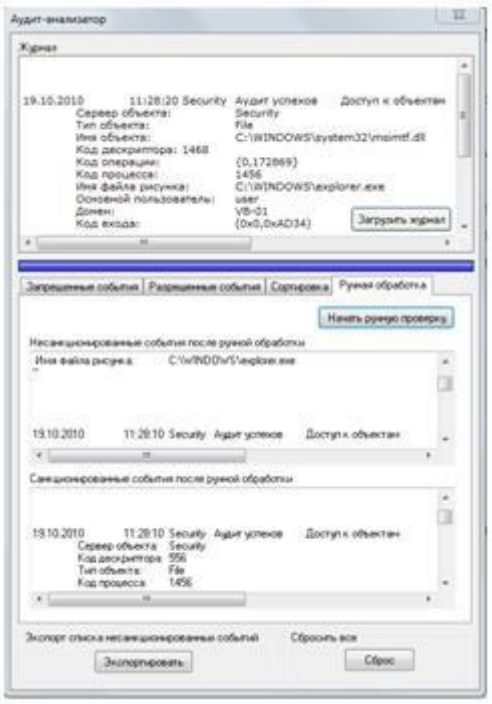


Рисунок 3.7 - Інтерфейс програмного засобу на четвертому етапі

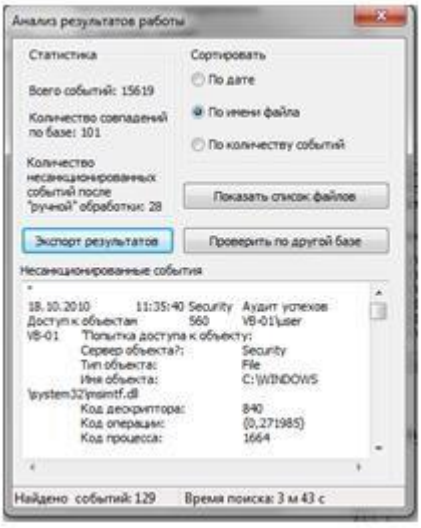


Рисунок 3.8 - Інтерфейс програмного засобу на заключному етапі

3.5 Організаційно - економічна сутність завдання

Розглянутий проект програмного засобу призначений для автоматизації обліку подій в системах сімейства Windows .

При проектуванні функцій даних підсистем враховувалася необхідність використання отриманих результатів при подальшому функціонуванні ІСС. В якості основних вимог до роботи підсистем висувалися:

- наявність гнучких зв'язків між функціональними блоками підсистеми;
- можливість подальшої модернізації;
- вхідні та вихідні дані, що відповідають стандартам;
- надання зручного інтерфейсу роботи зі звітами журналу аудиту систем Windows;
- надання інформації, придатної для функціонування інших підсистем АРМа, таких як ВО «Аудит-аналізатор» для ІКЦ в ХНУ і ін.

Вже згадана підсистема може бути використана клієнтами для відстеження шкідливих змін в операційному середовищі. Дані, отримані в результаті роботи з підсистемою використовуються як вихідні дані для адміністратора з інформаційної безпеки, метою якого є виявлення та запобігання несанкціонованого доступу до ресурсів обчислювальних машин [19].

3.6 Аналіз цілей запланованого впровадження

З впровадженням програмного засобу зміниться ситуація з використанням ручної праці при аналізі шкідливих подій. Після впровадження даного проекту з'являться такі позитивні ефекти:

1. Чи скоротиться час на пошук і отримання необхідної інформації про події.
2. Реалізується можливість централізованого збору інформації про дані аудиту.
3. Зменшення тимчасових і трудових витрат на обстеження інформаційної безпеки.

Аналіз даних позитивних властивостей показує наступні явно позитивні результати:

час на пошук і отримання необхідної інформації до впровадження виглядає наступним чином

а) пошук інформації адміністратором по необхідному події в середньому - 1,5 години. Після автоматизації:

а) пошук інформації скорочується до 10 хв.

Отже, можна обчислити різницю:

При пошуку за допомогою інформаційно-довідкової системи аудиту витрачається 33% в місяць від часу витраченої на пошук без неї.

Розрахуємо відношення тимчасових витрат:

До автоматизації пошук даних виробляли вручну. Розробка робочої інформації та аналіз для однієї групи подій без використання аналізатора-аудиту займає в середньому 1,5 -2 години.

Після автоматизації - 3-5 хвилин. Отже, можна підвести наступну статистику: При розробці робочої інформації в рамках АРМа за місяць використовується 4,16% від часу, використовуваного при ручній обробці.

3.7 Розрахунок комплексного коефіцієнта ефективності проекту

Проводиться оцінка техніко-економічної ефективності по комплексному коефіцієнту ефективності управління до і після автоматизації.

Кк. еф. = Ki * ai

, де

ai - вага кожного критерію, що показує відносну важливість і-го критерію (допускаємо, що ai = 1, тобто всі критерії равноважни); тобто

Кк. еф. = Ki (2.1);

Ki = Ppi / Pпi (2.2);

, деKi - коефіцієнт ефективності управління по і-му показнику (критерію);

Ppi - реальне значення і-го показника;

Pпi - планове значення і-го показника;

I - кількість показників.

Формула (2.2) застосовується при тенденції до зростання реального значення показника при поліпшенні якості управління. Формула (2.3) застосовується при зменшенні реального значення показника при поліпшенні якості управління. Дані заносяться в таблицю, а потім проводиться розрахунок за наведеними формулами. І на завершення обчислюємо комплексний коефіцієнт ефективності за формулою:

K =? Ki2 /? Ki1

K = 4,5 / 0.032 = 140,625.

3.8 Висновки

Описане функціональне призначення програмного засобу засноване на існуючому алгоритмі аналізу журналів системи аудиту, що дозволяє провести формалізацію і класифікацію подій [20].

На підставі дослідження алгоритмів формалізації і класифікації в реалізованому програмному засобі можна зробити наступні висновки:

1. Система повинна обробляти дані про події безпеки, які добувають із журналів подій системи аудиту Windows.

2. Вхідними даними для програмного засобу служить експортований журнал подій аудиту, сформований раніше при налаштуванні системи аудиту; «Чорний список» злісних програм, які отримують несанкціонований доступ до об'єктів системи; «Білий список» санкціонованих програм, службовець для усунення надмірності оброблюваного журналу.

3. деталізований алгоритм аналізу журналу подій включає чотири основні етапи: пошук несанкціонованих подій в сформованому системою аудиту журналі на основі деякої локальної або віддаленої бази шкідливого програмного забезпечення; усунення надмірності журналу; пошук подій за умовою і сортування; «Ручна» обробка.

4. На кожному етапі роботи програми проводиться проміжний аналіз і розрахунок статистики санкціонованих і несанкціонованих подій.

5. Після закінчення чотирьох етапів роботи програми користувач може переглянути повний звіт за всі чотири етапи для передачі його особі, відповідальній за інформаційну безпеку.

Провівши порівняльний аналіз ефективності можна сказати, даний проект економічно вигідний. А також, що є не менш важливим впровадження програмного підвищить соціальний аспект ефективності проекту набагато вище, ніж економічний.

У сучасних умовах основними критеріями діяльності підприємства є показники прибутку і рентабельності, які в першу чергу залежать від того, наскільки добре реалізовані бізнес-процеси.

Для аналізу подій безпеки зі швидкістю, необхідної для вирішення завдань в реальному масштабі часу потрібно:

1. Оперативний збір та аналіз подій;

2. Формування бази несанкціонованих програм;

3. Виведення результатів.

Все це надає автоматизована інформаційна система Аудит-аналізатор. На підставі наведених вище розрахунків і досвіду впровадження аналогічних систем на схожих підприємствах можна зробити висновок, що впровадження автоматизованої інформаційної системи Аудит-аналізатор спричинить за собою наступні позитивні ефекти:

1. Підвищення оперативності роботи.

2. Зменшення часу на виконання бізнес-процесів.

3. Поліпшення якості розрахунків.

4. Підвищення якості продукції, що випускається документації.

5. Зменшення кількості помилок.

6. Зменшення кількості паперових документів, що циркулюють в системі.

7. Чи дозволить приймати рішення в умовах визначеності.

8. Забезпечення всієї повноти необхідної інформації в будь-який зручний для користувача час.

На підставі цього можна зробити висновок про доцільність автоматизації діяльності ІКЦ в ХНУ.

ВИСНОВКИ

Поставлені цілі в рамках проведеного проекту аналізу і дослідження засобів аудиту подій систем сімейства Windows з метою виявлення несанкціонованого доступу програмного забезпечення до ресурсів обчислювальних машин були благополучно досягнуті.

Розроблене засіб моніторингу та аналізу подій безпеки на основі розробленої методики дозволяє спеціалісту з інформаційної безпеки на підприємстві проводити жорсткий контроль доступу до критичних об'єктів інформаційної системи, дозволяє своєчасно виявляти факти несанкціонованого доступу до ресурсів обчислювальної машини і проводити розслідування даних фактів.

Основою для реалізованого програмного засобу служить методика аналізу подій безпеки. Методика полягає в багатоступінчастої фільтрації і усунення надмірності журналу аудиту, сформованого системою аудиту Windows, з подальшою класифікацією кожної події за трьома групами: група санкціонованих подій, група несанкціонованих подій, група «сумнівних подій». Віднесення подій до тієї чи іншої групи засноване на попередньо сформованих «чорному» і «білому» списках, в які входять відповідно файли і ключі реєстру, однозначно класифікуються як шкідливі, і файли і ключі реєстру, однозначно класифікуються як нейтральні. Списки складаються на основі накопиченої статистики великих антивірусних компаній Лабораторія Касперського, і компанії Доктор Веб.

Впровадження методики в розробляється програмний засіб дозволило досягти високої швидкості обробки вхідних даних експортованого списку подій журналу Windows.

Впровадження розробленого програмного засобу в існуючий сегмент інформаційної структури підприємства ІКЦ в ХНУ дозволило досягти автоматизації рутинних процесів аналізу подій безпеки, тим самим значно скоротивши час пошуку та формалізації подій.

Відсутній раніше рівень виявлення несанкціонованого доступу безпосередньо після того, як доступ стався, з впровадженням програмного засобу за розробленою методикою став ще одним кордоном на шляху протидії спробам зловмисника вторгнутися в інформаційну систему.

Триваюче співробітництво з компанією Доктор Веб дозволить в подальшому вдосконалити методику аналізу, завдяки впровадженню додаткових функцій в програмний засіб і вдосконалення алгоритмів формалізації і класифікації даних.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Андон, Ф. А. Навчальний курс за мовними запитами SQL / Ф. А. Андон, В. М. Резніченко. СПб. Пітер, 2006. – 41 с.

2. Баймакова, І. А. Забезпечення захисту персональних даних: Методичний посібник, 2008. – 245 с.

3. А. І. Рогачов. - М.: 1С-Паблішинг, 2010. – 214 с.

4. Бернетт, С. Криптографія: Офіційне керівництво RSA Security / С. Бернетт, С. Пейн., 2002. – 384 с.

5. Б’ячуев, Т.А. Безпека корпоративних мереж: Підручник, 2004. – 161 с.

6. Шнаєр Брюс. Прикладна криптографія: протокол, алгоритм, вихідний текст С / Bruce Schneier. : 2002. – 86 с.

7. Гатчина, Ю. А. Основи алгоритму шифрування: Навчальний посібник / Ю.О. А. Гатчина, А. Г. Коробейніков. СПб. : ГІТМО (ТУ), 2002. – 29 с.

8. Ігнатьєфф, Вірджинія Інформаційна безпека для сучасних комерційних підприємств, 2005. – 448 с.

9. А.Г. Коробейніков. Математичні основи криптографії, 2002. – 41 с.

10. Мельников, В.П. Інформаційна безпека та захист, В.П. Мельников, С.А.Клейменов. -М. : Видавничий центр «Академія», 2008. – 336 с.

11. Пономарьов В.С., База даних Delphi 7: Пітер, 2003. – 224 с.

12. Романець Ю. В. Захист інформації в комп'ютерних системах і мережах Ю. В. Романець, П. А. Тимофєєв, В. Ф. Шаніна. -М. : «Радио и связь», 2006. - 328 с.

13. Садердінов, А.А. Корпоративна інформаційна безпека / А.А. Садердінов. - М.: «Дашков і К», 2005. – 336 с.

14. Скрипкін, Економічна ефективність інформаційних систем К.Г. / К.Г. Скрипкін. -М. : ДМК Пресс, 2006. – 256 с.

15. Хомоненко, А.Д. База даних: Підручники вузів, 2009. – 106 с.

16. Хомоненко А.Д., Циганков В.М., Мальцев М.Г. Бази даних. Підручник для вищих навчальних закладів (6-е вид.), 2004. – 95 с.

17. Чіпига А.Ф. Автоматична система навчання інформаційної безпеки. АФ Чипига. -М. : Геліос АРМ, 2010. – 336 с.

18. Шангіна, В.Ф. Інформаційна безпека комп'ютерних систем і мереж: Навчальний посібник, 2008. – 416 с.

19. Ярочкин, В. І. Інформаційна безпека: Підручник для студентів вузів / В. І. Ярочкин. - М.: Академічний проект, 2008. – 544 с.

20. Вембо, Мао. Сучасна криптографія: теорія і практика, 2005. – 78 с.

ДОДАТОК А

(обов’язковий)

Вихідний код головного модуля програми

```
unit main;
interface
uses
Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
Dialogs, StdCtrls, ComCtrls, Buttons, ActnMan, ActnColorMaps,
SUIStatusBar, SUIProgressBar, {SUIMemo, SUIButton,} ExtCtrls, {SUIForm,}
        Menus, SUIMemo, SUIButton, {SUIMainMenu, SUISideChannel,
 SUISkinControl} DateUtils,
        XPMan;
        var
        Form1: TForm1;
        bad_events, curr_event, all_events, nobadandgood_events, whitelist,
 blacklist, good_events, nobad_events, sortedbydate, sortedbytime, sortedbyall:
 TStringList;
        handjob, exp: TStringList;
        F: TextFile;
firstk, lastk, eventsnum: integer;
implementation
procedure proverka_blacklist;
var
flag: boolean;
begin
flag: = false;
for i: = 0 to curr_event.Count-1 do
begin
for j: = 0 to blacklist.Count-1 do
begin
if pos (form1.Memo4.Lines.Strings [j], curr_event.Strings [i]) <> 0 then
begin
flag: = true;
bad_events.Insert (0, curr_event.Text);
if flag = false then nobad_events.Insert (0, curr_event.Text);
end;
procedure proverka_whitelist;
```

```
var
i, j: integer;
flag: boolean;
begin
flag: = false;
for i: = 0 to curr_event.Count-1 do
procedure proverka_vrem;
var
procedure proverka_man;
var
buttonSelected: Integer;
procedure TForm1.suitempButton2Click (Sender: TObject);
var
count, i, k, j: integer;
begin
count: = 0;
firstk: = - 1;
for i: = 0 to all_events.Count-1 do
begin
if all_events.Strings [i] = ' '" then
begin
j: = 0;
curr_event.Clear;
lastk: = i;
for k: = firstk + 1 to lastk do
begin
curr_event.Insert (j, all_events.Strings [k]);
j: = j + 1;
if k = lastk then proverka_blacklist;
end;
firstk: = lastk;
end;
ProgressBar1.StepBy (1);
end;
memo3.Lines.Text: = bad_events.Text;
memo1.Lines.Text: = nobad_events.Text;
form1.Memo1.Lines.Insert (0, ");
end;
procedure TForm1.FormCreate (Sender: TObject);
begin
eventsnum: = 0;
nobadandgood_events: = TStringList.Create;
```

```
bad_events: = TStringList.Create;
good_events: = TStringList.Create;
nobadandgood_events: = TStringList.Create;
whitelist: = tstringlist.create;
sortedbydate: = TStringList.Create;
sortedbytime: = TStringList.Create;
sortedbyall: = TStringList.create;
curr_event: = TStringList.Create;
all_events: = TStringList.Create;
blacklist: = TStringList.Create;
nobad_events: = TStringList.Create;
handjob: = TStringList.Create;
exp: = TStringList.Create;
blacklist.LoadFromFile ( 'blacklist.txt');
whitelist.LoadFromFile ( 'whitelist.txt');
memo4.Lines.Text: = blacklist.Text;
memo5.Lines.Text: = whitelist.Text;
PageControl1.ActivePageIndex: = 0;
end;
procedure TForm1.suitempBitBtn1Click (Sender: TObject);
begin
if OpenDialog1.Execute then
memo4.Lines.LoadFromFile (OpenDialog1.FileName);
end;
procedure TForm1.suiSideChannel1Pop (Sender: TObject);
begin
Form1.width: = Form1.width + 185
end;
procedure TForm1.suiSideChannel1Push (Sender: TObject);
begin
Form1.width: = Form1.width-185
end;
procedure TForm1.BitBtn2Click (Sender: TObject);
var
count, i, k, j: integer;
begin
count: = 0;
firstk: = - 1;
memo2.Clear;
sortedbydate.Clear;
for i: = 0 to Memo1.Lines.Count-1 do
begin
```

```
if Memo1.Lines.Strings [i] = ' '" then
begin
j: = 0;
curr_event.Clear;
lastk: = i;
for k: = firstk + 1 to lastk do
begin
curr_event.Insert (j, Memo1.Lines.Strings [k]);
j: = j + 1;
if k = lastk then proverka_dat;
end;
firstk: = lastk;
end;
end;
memo2.Lines.Insert (0, sortedbydate.Text);
end;
procedure TForm1.BitBtn3Click (Sender: TObject);
var
count, i, k, j: integer;
begin
count: = 0;
firstk: = - 1;
memo2.Clear;
sortedbytime.Clear;
for i: = 0 to Memo1.Lines.Count-1 do
begin
if Memo1.Lines.Strings [i] = ' '" then
begin
j: = 0;
curr_event.Clear;
lastk: = i;
for k: = firstk + 1 to lastk do
begin
curr_event.Insert (j, Memo1.Lines.Strings [k]);
j: = j + 1;
if k = lastk then proverka_vrem;
end;
firstk: = lastk;
end;
end;
memo2.Lines.Insert (0, sortedbytime.Text);
end;
```

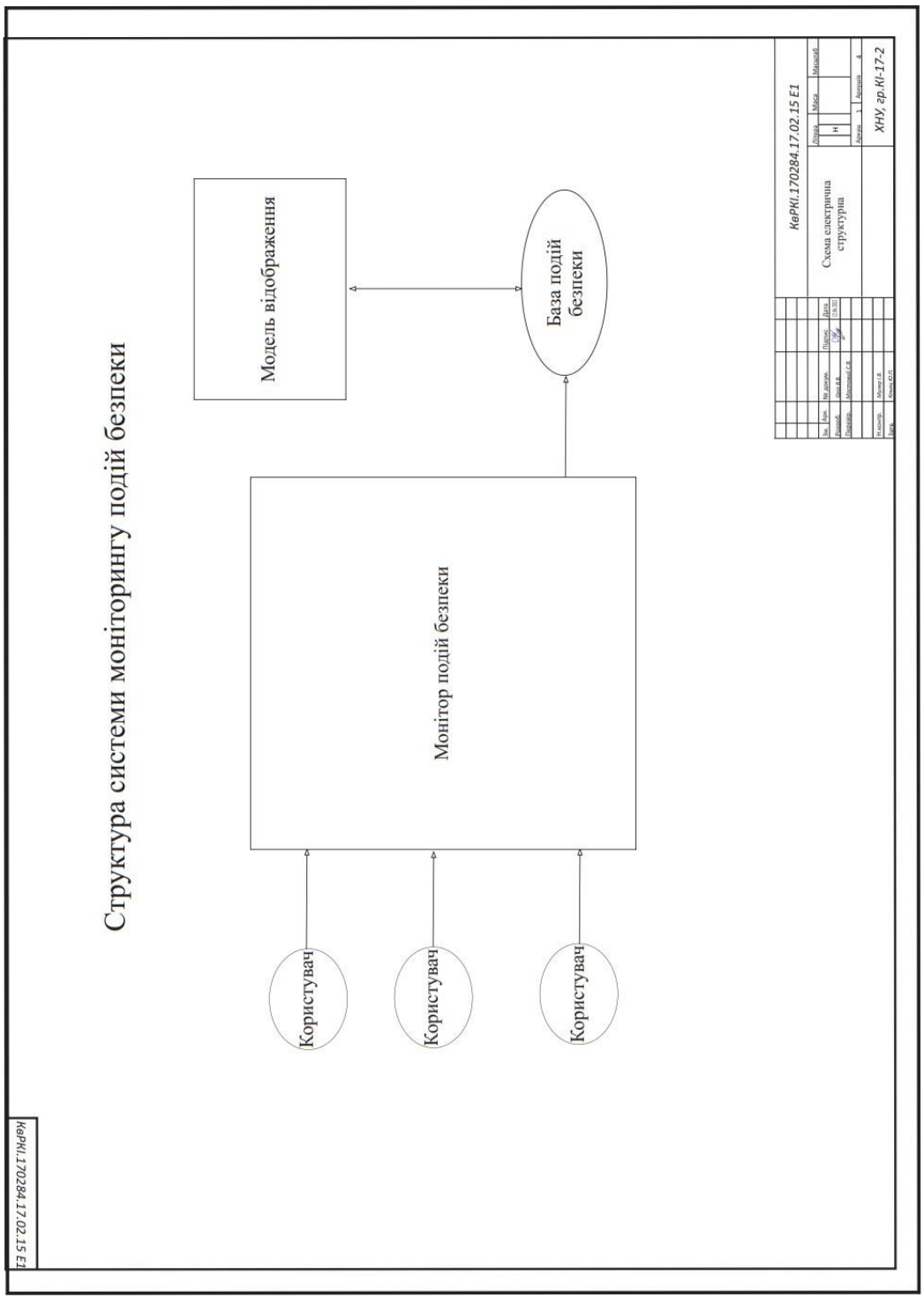
```
procedure TForm1.BitBtn4Click (Sender: TObject);
var
count, i, k, j: integer;
begin
if OpenDialog1.Execute then
memo5.Lines.LoadFromFile (OpenDialog1.FileName);
end;
procedure TForm1.BitBtn5Click (Sender: TObject);
var
count, i, k, j: integer;
begin
count: = 0;
firstk: = - 1;
ProgressBar1.Position: = 0;
ProgressBar1.Max: = memo1.Lines.Count-1;
for i: = 0 to memo1.Lines.Count-1 do
begin
if memo1.Lines.Strings [i] = ' '" then
begin
j: = 0;
curr_event.Clear;
lastk: = i;
for k: = firstk + 1 to lastk do
begin
curr_event.Insert (j, memo1.Lines.Strings [k]);
j: = j + 1;
if k = lastk then proverka_whitelist;
end;
firstk: = lastk;
end;
ProgressBar1.StepBy (1);
end;
memo6.Lines.Text: = good_events.Text;
memo1.Lines.Text: = nobadandgood_events.Text;
form1.Memo1.Lines.Insert (0, ");
end;
procedure TForm1.BitBtn7Click (Sender: TObject);
begin
nobadandgood_events.clear;
bad_events.clear;
good_events.clear;
nobadandgood_events.clear;
```

```
        whitelist.clear;
        sortedbydate.clear;
        sortedbytime.clear;
        sortedbyall.clear;
        curr_event.clear;
        all_events.clear;
        blacklist.clear;
        nobad_events.clear;
        handjob.clear;
        exp.clear;
        end;
        procedure TForm1.Button3Click (Sender: TObject);
        begin
        exp.clear;
        exp.Insert (0, memo3.Text);
        exp.Insert (0, memo7.Text);
        if SaveDialog1.Execute then
        exp.SaveToFile (SaveDialog1.FileName);
        end;
        procedure TForm1.Button4Click (Sender: TObject);
        begin
        memo2.Text: = memo1.Text;
        end;
end
```

ДОДАТОК Б

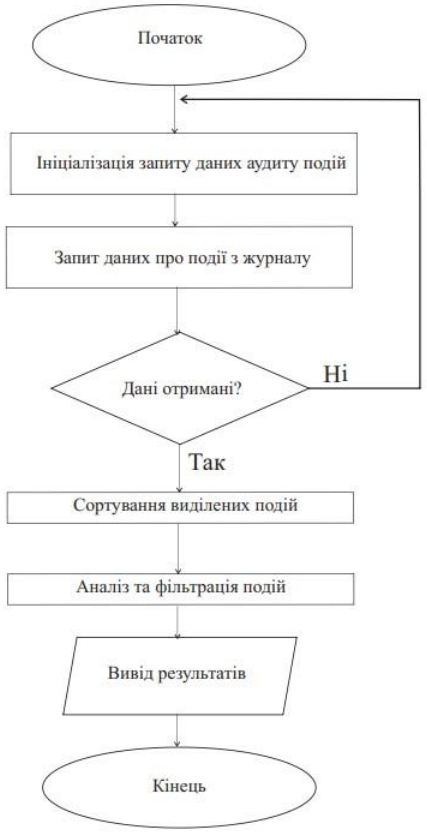
(обов’язковий)

Алгоритми роботи та зовнішній вигляд головного модуля



КвРКІ.170284.17.02.15 Е2

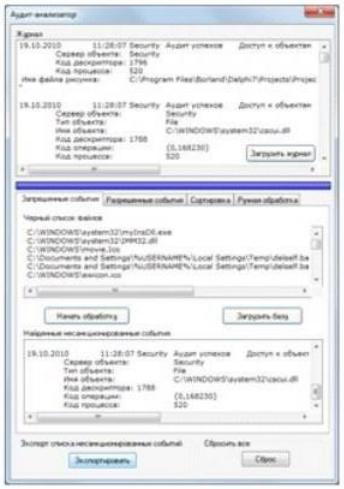
Узагальнений алгоритм обробки даних аудиту подій безпеки



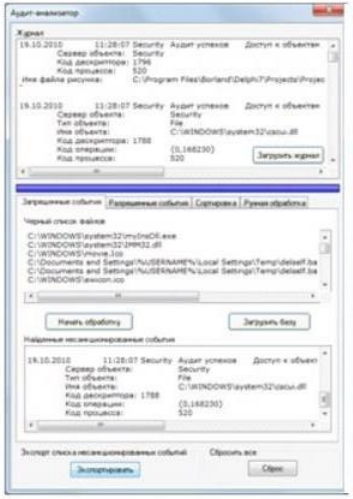
Узагальнений алгоритм обробки журналу подій реалізованим програмним засобом

					КвРКІ.170284.17.02.15 Е2		
Зм.	Арк.	№ докум.	Підпис	Дата	Схема електрична функціональна	Літера	Маса	Масштаб
Розроб.		Оник В.В.				Н		
Перевір.		Мостовий С.В.				Аркуш 2	Аркушів 4	
Н.контр.		Мулер І.В.			ХНУ, гр.КІ-17-2			
Затв.		Кільох Ю.Л.						

Інтерфейс програмного засобу на першому етапі

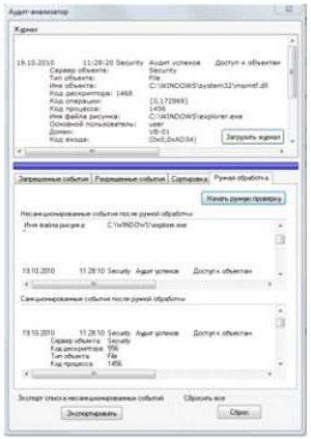


Інтерфейс програмного засобу на другому етапі

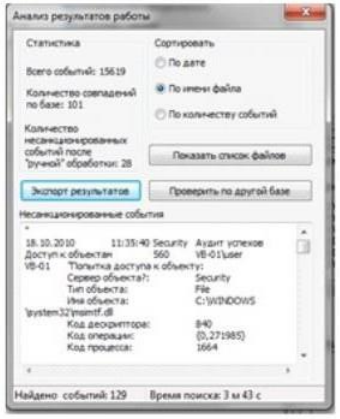


Інтерфейс програмного засобу на третьому етапі

Інтерфейс програмного засобу на четвертому етапі

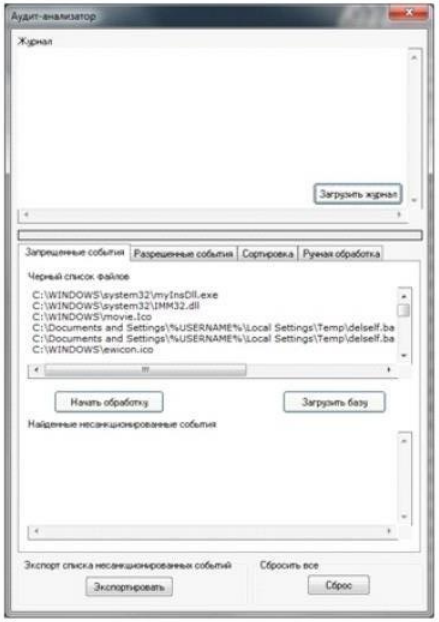


Інтерфейс програмного засобу на заключному етапі

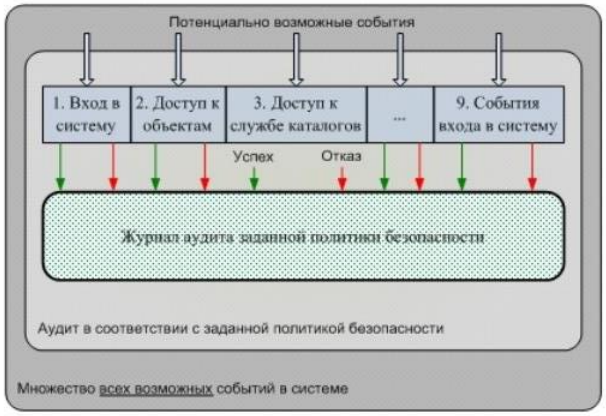


					КвРКІ.170284.17.02.15 Е3	
Зм.	Арк.	№ докум.	Підпис	Дата	Схема електрична принципова	Літера: Н; Маса; Масштаб
Розроб.		Оньї В.В.		01.06.20		
Перевір.		Мостовий С.Я				Аркуш 3 / Аркушів 4
Н.контр.		Мулик І.В.				ХНУ, гр.КІ-17-2
Затв.		Кінець Ю.Л.				

Інтерфейс програмного засобу



Формування журналу аудиту відповідно до заданої політикою аудиту



						КвРКІ.170284.17.02.15 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Алгоритм роботи	Літера	Маса	Масштаб
Розроб.		Оліх В.В.				Н		
Перевір.		Мостовий С.В.				Аркуш 4	Аркушів 4	
Н.контр.		Мулер І.В.						
Затв.		Кільчу Ю.Л.				ХНУ, гр.КІ-17-2		

UNICHECK

User name:
Кафедра кибербезпеки

Check ID:
1008322053

Check date:
17.06.2021 16:26:30 EEST

Check type:
Doc vs Internet

Report date:
17.06.2021 16:26:58 EEST

User ID:
100005590

File name: **Дипломна Оліх рамки 1**

Page count: **57** Word count: **9798** Character count: **77828** File size: **1.46 MB** File ID: **1008393852**

0.88% Matches

Highest match: **0.7%** with Internet source (**https://vms.drweb.ru/virus/?i=66356&lng=ru**)

0.88% Internet sources	34

Page 59

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters	6

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

ID: 94586 Название: мання інформації про про- цеси для ОС Windows Добавлено в БД: 2021-06-17 Авторы: Оліх В.В. Руководители: Мостовий С.В. Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	61092	916	0 (0%)	0 (0%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Оліх Василь Володимирович

Тема Розробка модуля отримання інформації про процеси для ОС Windows

Спеціальність 123 – Комп'ютерна інженерія

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 4; кількість сторінок записки 60.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розроблено модуль отримання інформації про процеси для ОС Windows.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота не в повній мірі відповідає поставленому завданню

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, У першому розділі проведено огляд засобів аудиту подій операційних систем, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі розроблено модуль аудиту подій на основі існуючої політики безпеки. В третьому розділі проведено аналіз роботи розробленого модуля.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну практичну цінність. Практична цінність результатів кваліфікаційної роботи полягає у створені модуля аудиту подій

5. Негативні сторони роботи Розроблений в роботі модуль має вузький функціонал

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки.

8. Інші зауваження Окремі описи в пояснювальній записці подано занадто деталізовано, що ускладнює сприйняття матеріалу фахівцями в обраній предметній галузі.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «задовільно» D.

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Бармак О.В. зав. кафедри КМП

«14» червня 2021. (підпис)

Завідувачу кафедри КІСП
к-т.техн.наук, доцент. Кльоц Ю.П.

Оліх Василь Володимирович
ПІБ здобувача вищої освіти

ФПКТС, 4 курсу, групи КІ-17-2

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 29.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

18.06.21
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Розробка модуля отримання інформації про процеси для ОС Windows

Автор: Оліх Василь Володимирович

Спеціальність: 123 – Комп'ютерна інженерія та програмування

Освітня програма: освітньо-професійна

Науковий керівник: Мостовий Сергій Володимирович, старший викладач

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) в якості запозичень в окремих місцях системою зафіксовано послідовності чотирьохрозрядних двійкових кодів, які є вхідними даними до великої кількості задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
5) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.(Тут текст можна і треба модифікувати)

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 0.88% і адресується до 34 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ С. В. Мостовий

Гарант ОП _____ С. М. Лисенко

Завідувач кафедри КІСП _____ Ю. П. Кльоц