

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования «Тульский государственный университет»
Институт прикладной математики и компьютерных наук

Кафедра «Информационная безопасность»

КУРСОВАЯ РАБОТА

по дисциплине

«Операционные системы и их безопасность»

на тему

*«Анализ защищённости заданной конфигурации механизмов безопасности ОС
Windows»*

Вариант №2

Выполнила: ст. гр. 230711

(подпись)

Павлова В. С.

Проверил: доц. каф. ИБ

(подпись)

Антонов Д. М.

Тула, 2023 г.

ЗАДАНИЕ

на курсовую работу по дисциплине
«Операционные системы и их безопасность»

студента гр. 230711 Павловой Виктории Сергеевны

Тема курсовой работы

«Анализ защищённости заданной конфигурации механизмов безопасности
ОС Windows»

Исходные данные

Проектируемый модуль должен определить: вид операционной системы; тип и
роль узла, DNS и NetBIOS, установленные обновления (из базы Microsoft).
примененную политику учетных записей, примененную политику паролей,
примененную политику аудита, сетевые настройки (TCP IP и т.д.), открытые
ресурсы (совместно используемые ресурсы, разделяемые ресурсы NetBIOS
(NetBIOS Share); запущенные сервисы (какие необходимы в различных
случаях, особенно сетевые, анализ редко используемых сетевых сервисов);
файловую систему (тип файловой системы, определить права на доступ к особо
важным файлам, разрешения на основные файлы и папки); установленные
драйверы.

Задание получил _____
(ФИО) (подпись)

Задание выдал _____
(ФИО) (подпись)

Дата выдачи задания «07» ноября 2023г

График выполнения КР в соответствии с методическими указаниями.

Рекомендации и особые отметки _____

«__» _____ 20__ г

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
1 АСПЕКТЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ	5
1.1 Параметры безопасности по умолчанию	7
1.2 Анализ конфигурации параметров безопасности по умолчанию	9
2 АНАЛИЗ ЗАЩИЩЁННОСТИ ЗАДАННОЙ КОНФИГУРАЦИИ МЕХАНИЗМОВ БЕЗОПАСНОСТИ ОС WINDOWS.....	12
2.1 Описание программы-анализатора.....	13
2.2 Рекомендуемые параметры конфигурации	18
ЗАКЛЮЧЕНИЕ	22
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	23
ПРИЛОЖЕНИЕ А	24
ПРИЛОЖЕНИЕ Б.....	29

ВВЕДЕНИЕ

В современном информационном обществе, где компьютерные технологии проникают во все сферы деятельности, обеспечение безопасности операционных систем (ОС) становится ключевым аспектом в поддержании стабильности и надежности вычислительных систем. Одной из наиболее широко используемых операционных систем является Windows, разработанная корпорацией Microsoft. Сложившаяся экосистема этой ОС требует внимательного анализа и оценки уровня безопасности.

Цель настоящей курсовой работы заключается в проведении анализа защищённости заданной конфигурации механизмов безопасности операционной системы Windows. Для достижения этой цели предполагается разработка программы-анализатора, способной оценивать текущий уровень безопасности в соответствии с predetermined параметрами. Эта программа должна делать обзор текущего состояния безопасности и предлагать конструктивные пути для её улучшения, соответствуя современным требованиям и стандартам безопасности.

Исследование безопасности операционных систем, особенно Windows, имеет стратегическое значение, учитывая постоянно развивающиеся угрозы и высокий уровень взаимосвязи информационных технологий с повседневной жизнью. Актуальность данной работы подчёркивается не только необходимостью обеспечения защиты конфиденциальной информации, но и стремлением к постоянному совершенствованию механизмов безопасности для предотвращения потенциальных угроз и атак. На фоне быстрого технологического прогресса и увеличения уровня цифровой уязвимости, анализ защищённости операционных систем становится важной задачей, направленной на обеспечение стойкости и безопасности информационных систем.

1 АСПЕКТЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ

Корректная и целесообразная настройка безопасности операционной системы прежде всего является важной для отказоустойчивости и обеспечения информационной безопасности всех устройств, объединённых в рамках одной автоматизированной системы и самой системы в целом [1]. Компания Microsoft для поддерживаемых версий операционной системы Windows постоянно совершенствует меры безопасности, предоставляя пользователям различные инструменты и опции для защиты от различных угроз. Ниже приведены основные аспекты настроек безопасности в ОС Windows на основании документации Microsoft [2].

- **Windows Defender и антивирусная защита:**

Windows Defender — встроенный антивирусный и антималяварный продукт от Microsoft. С постоянными обновлениями баз данных, он способен эффективно выявлять и устранять угрозы. Пользователи также могут устанавливать сторонние антивирусные программы, но Windows Defender предоставляет базовую, но достаточно надежную защиту.

- **Обновления системы:**

Регулярные обновления операционной системы — ключевой компонент безопасности: Microsoft регулярно выпускает обновления для устранения уязвимостей и улучшения стабильности. Автоматическое обновление включено *по умолчанию*.

- **Брандмауэр и сетевая безопасность:**

Встроенный брандмауэр Windows контролирует сетевой трафик и защищает от несанкционированного доступа. Возможна настройка правил брандмауэра для улучшения безопасности своей сети.

- **Аутентификация и учетные записи:**

В Windows предусмотрены различные методы аутентификации, такие как пароли, PIN-коды, и в некоторых версиях — биометрические данные. Многие

функции, такие как BitLocker, предлагают защиту данных с использованием пароля.

- **Безопасность веб-браузера:**

Используемый веб-браузер также играет важную роль в безопасности. Microsoft Edge включает функции SmartScreen для блокировки фишинговых сайтов и опасных загрузок. Регулярные обновления браузера также улучшают его безопасность.

- **Управление правами доступа:**

Пользователи могут настраивать права доступа к файлам и папкам, что помогает предотвратить несанкционированный доступ к конфиденциальным данным. Разделение учетных записей на администраторские и обычные пользовательские также способствует повышению безопасности.

- **Защита от вредоносных программ и ресурсов:**

Система SmartScreen защищает от вредоносных программ и потенциально опасных файлов, предупреждая пользователя о возможных рисках. Встроенные инструменты анализа поведения программ также помогают выявлять подозрительную активность.

- **Шифрование данных:**

BitLocker — инструмент шифрования диска, предоставляющий дополнительный уровень защиты для хранящихся на компьютере данных. Пользователи могут зашифровать целый диск или отдельные разделы.

- **Центр безопасности Windows:**

Центр безопасности предоставляет обзор состояния безопасности системы и предупреждения о возможных проблемах. Это позволяет пользователям оперативно реагировать на потенциальные угрозы.

- **Облачные сервисы и учетные записи Microsoft:**

Использование облачных служб Microsoft, таких как OneDrive, в сочетании с учетной записью Microsoft, дает дополнительные инструменты для защиты и резервного копирования данных.

Несмотря на все усилия Microsoft по обеспечению безопасности Windows, важно, чтобы и сами пользователи принимали активное участие в защите своих систем. Это включает в себя обновление программ третьих сторон, использование сильных паролей и бдительность при взаимодействии с внешними ресурсами. В целом, система безопасности Windows предоставляет широкий спектр инструментов для обеспечения безопасности, и правильная настройка этих инструментов играет ключевую роль в предотвращении угроз.

1.1 Параметры безопасности по умолчанию

Настройки безопасности Windows имеют ряд параметров по умолчанию, которые предоставляют базовый уровень защиты. Далее рассмотрим некоторые из основных параметров и где их можно найти:

– **Windows Defender:**

- Расположение: Панель управления → Обновление и безопасность → Центр обеспечения безопасности Windows.
- Параметры по умолчанию: Обнаружение и удаление вредоносного ПО включено. Регулярные обновления базы данных.

– **Обновления операционной системы:**

- Расположение: Параметры → Обновление и безопасность → Windows Update.
- Параметры по умолчанию: Автоматические обновления включены. Обновления для безопасности и стабильности устанавливаются автоматически.

– **Брандмауэр Windows:**

- Расположение: Панель управления → Система и безопасность → Брандмауэр Windows.

- Параметры по умолчанию: Брандмауэр включен. Есть правила для разрешения или блокировки трафика приложений.
- **Центр безопасности Windows:**
 - Расположение: Панель управления → Обновление и безопасность → Центр обеспечения безопасности Windows.
 - Параметры по умолчанию: Предоставляет обзор обновлений, состояния антивируса (Windows Defender), брандмауэра и других аспектов безопасности.
- **Учетные записи и безопасность:**
 - Расположение: Параметры → Обновление и безопасность → Аккаунты.
 - Параметры по умолчанию: Возможность использования пароля, PIN-кода, биометрии. В Windows 10 есть также «Защита Windows Hello», использующаяся для биометрической аутентификации.
- **BitLocker:**
 - Расположение: Проводник → ПК → Управление BitLocker.
 - Параметры по умолчанию: BitLocker не включен по умолчанию. Если включен, предоставляет шифрование диска.
- **Сетевая безопасность:**
 - Расположение: Параметры → Сеть и интернет → Центр сетевого и общего доступа.
 - Параметры по умолчанию: Windows обнаруживает сети и автоматически применяет определенные параметры безопасности, например, для общественных или домашних сетей.
- **Защита от вредоносных программ и ресурсов:**

- Расположение: Параметры → Обновление и безопасность → Центр обеспечения безопасности Windows.
 - Параметры по умолчанию: Включает функции SmartScreen, предупреждения о потенциально опасных файлах и веб-страницах.
- **Облачные службы Microsoft:**
- Расположение: Параметры → Аккаунты → Дополнительные параметры аккаунта онлайн.
 - Параметры по умолчанию: Использование учетной записи Microsoft для доступа к облачным сервисам (например, OneDrive).

Важно отметить, что параметры безопасности могут различаться в зависимости от версии операционной системы Windows. Настройки по умолчанию обеспечивают базовый уровень защиты, но пользователи также должны регулярно обновлять систему, использовать сильные пароли, обращать внимание на предупреждения безопасности и следить за новыми угрозами, чтобы обеспечить максимальную безопасность своего компьютера.

1.2 Анализ конфигурации параметров безопасности по умолчанию

Рассмотрим, насколько предложенные Microsoft параметры по умолчанию обеспечивают безопасность, а также приведём возможные альтернативы:

1. Windows Defender:

- Оценка: Windows Defender предоставляет базовую защиту, но сторонние антивирусные программы обладают более широкими возможностями.
- Альтернативы: McAfee, Norton, Kaspersky – популярные антивирусные программы с расширенными функциями.

2. Обновления операционной системы:

- Оценка: Автоматические обновления являются критическим аспектом безопасности. Однако, иногда они могут вызывать неудобства пользователям в момент работы.
- Альтернативы: Включение опции обновления в «удобное время» для автоматических обновлений, чтобы они не мешали важной работе.

3. Брандмауэр Windows:

- Оценка: Брандмауэр обеспечивает базовую защиту от несанкционированного доступа, но для продвинутой защиты требуются дополнительные средства.
- Альтернативы: Сторонние брандмауэры, такие как ZoneAlarm или Comodo, предоставляют более расширенные функции.

4. Центр безопасности Windows:

- Оценка: Предоставляет обзор общей конфигурации, но может быть ограничен в функциональности для продвинутых пользователей.
- Альтернативы: Использование сторонних программ и сканеров для мониторинга безопасности, таких как Security Center от Bitdefender.

5. Учетные записи и безопасность:

- Оценка: Разнообразные методы аутентификации, однако пароли, соответствующие требованиям по умолчанию, могут быть уязвимы.
- Альтернативы: Двухфакторная аутентификация (2FA) или использование аппаратных ключей безопасности для дополнительного слоя защиты.

6. BitLocker (если применяется):

- Оценка: Обеспечивает шифрование диска, но может быть недоступен в некоторых версиях Windows [3].

- Альтернативы: VeraCrypt – бесплатное и открытое программное обеспечение для шифрования дисков.

7. Сетевая безопасность:

- Оценка: Автоматически применяет определенные параметры для различных типов сетей.
- Альтернативы: Ручная настройка параметров сети, особенно в публичных сетях [4].

8. Защита от вредоносных программ и ресурсов:

- Оценка: Включает функции SmartScreen для блокировки потенциально опасных ресурсов.
- Альтернативы: Расширенные программы защиты от фишинга, такие как WOT (Web of Trust).

9. Облачные службы Microsoft:

- Оценка: Использование учетной записи Microsoft для доступа к облачным службам обеспечивает дополнительные уровни безопасности.
- Альтернативы: Использование других облачных служб с двухфакторной аутентификацией, таких как Google Drive.

Резюмируя, параметры безопасности Windows по умолчанию обеспечивают базовую защиту. Вопрос о повышении уровня безопасности и использовании сторонних решений и дополнительных настроек ставится в зависимости от конкретных потребностей и угроз, с которыми сталкивается конкретный пользователь или система.

2 АНАЛИЗ ЗАЩИЩЁННОСТИ ЗАДАННОЙ КОНФИГУРАЦИИ МЕХАНИЗМОВ БЕЗОПАСНОСТИ ОС WINDOWS

Регулярные проверки и обновления настроек соответствии с изменяющимся спектром угроз – ключевое условие обеспечения безопасности. Комплексный анализ защищённости должен охватывать различные аспекты безопасности системы, включая в себя проверку политик безопасности, состояния установленных обновлений, аудита системных событий, наличия и правильности настроек брандмауэра, антивирусной защиты и других средств безопасности [5].

Анализ защищённости должен быть комплексным и охватывать различные аспекты безопасности системы. В рамках данной курсовой работы предполагается разработка программы-анализатора, способной оценивать текущий уровень безопасности в соответствии с predetermined параметрами. Этот инструмент будет способен проводить систематическую проверку параметров безопасности, определенных заранее. Программа будет предлагать рекомендации по улучшению безопасности и включать в себя модули для сканирования системных файлов, проверки наличия и актуальности обновлений, анализа журналов аудита и другие функциональности. Более подробное описание разработанного консольного приложения приведено в пункте «Описание программы-анализатора».

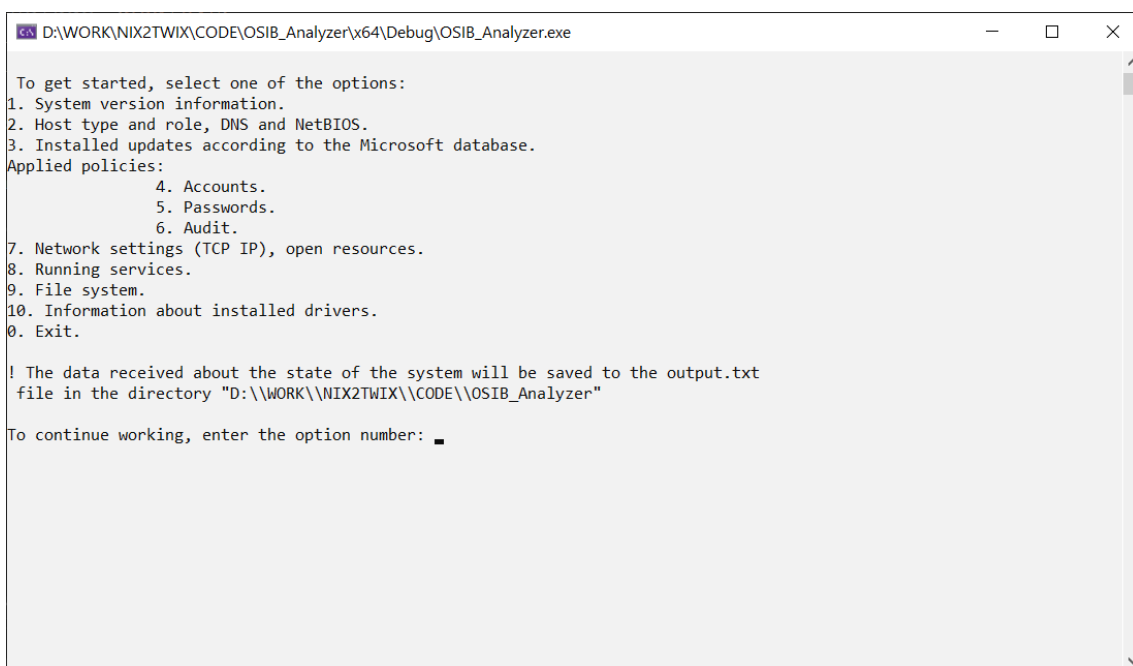
Эффективный анализ безопасности конфигурации ОС Windows помогает предотвращать атаки, обеспечивать стабильную работу системы и защищать конфиденциальные данные. Разработка программы-анализатора поддерживает подход к безопасности, акцентирующий внимание на проактивных мерах защиты и постоянном обновлении стратегий безопасности в соответствии с динамикой угроз информационной безопасности.

2.1 Описание программы-анализатора

В рамках данной курсовой работы необходимо написать программу-анализатора конфигурации настроек безопасности ОС. Код программы-анализатора приведён в листинге 1 приложения А. Ниже приведена инструкция пользователя по работе с каждой из опций программы.

Анализатор читает информацию об установленных настройках системы и сохраняет их файл для дальнейшего анализа. Программа написана на языке программирования C++ и использует функции обращения к командной строке `system()` [6-7]. Получая данные из консоли, анализатор сравнивает пользовательские настройки с рекомендованными параметрами безопасности, прописанными в ней по умолчанию, и выдает соответствующие рекомендации. Параметры, установленные как рекомендуемые программой, рассматриваются в пункте «Рекомендуемые параметры конфигурации» части 2 настоящей курсовой работы.

Управление программой осуществляется посредством записи в консоль номера выбранной опции. Написание сторонних символов не допускается. Проектируемый модуль имеет следующие опции (рисунок 1):



```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe

To get started, select one of the options:
1. System version information.
2. Host type and role, DNS and NetBIOS.
3. Installed updates according to the Microsoft database.
Applied policies:
    4. Accounts.
    5. Passwords.
    6. Audit.
7. Network settings (TCP IP), open resources.
8. Running services.
9. File system.
10. Information about installed drivers.
0. Exit.

! The data received about the state of the system will be saved to the output.txt
file in the directory "D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer"

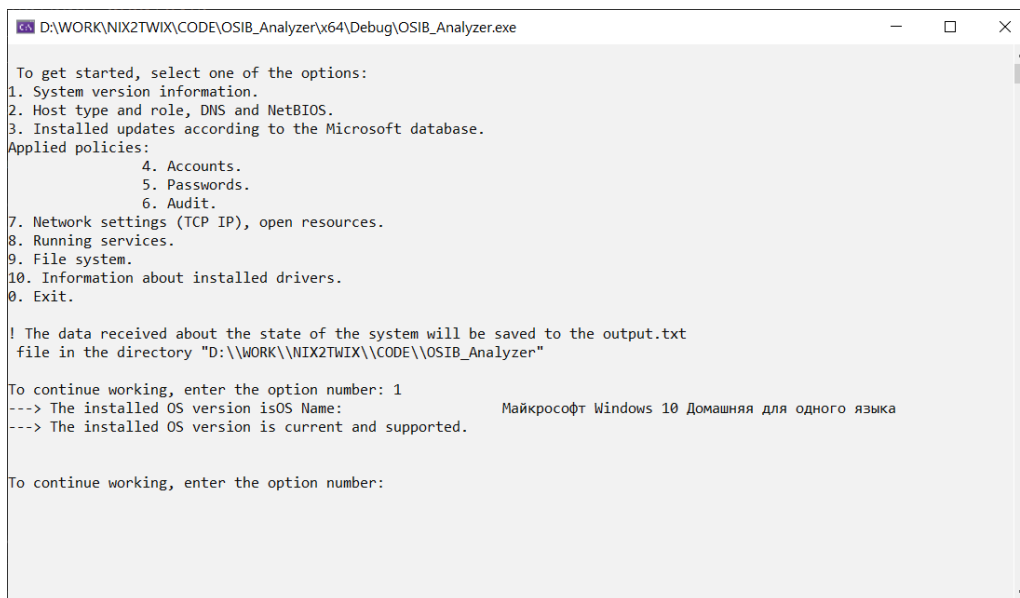
To continue working, enter the option number: █
```

Рисунок 1 – Меню (опции) модуля

Для корректной работы программы необходимо предоставить ей права внесения изменений на устройстве. Рассмотрим работу с каждой из опций.

1. Проверка актуальности версии ОС.

Как показано на рисунке 2, программа определяет текущую версию операционной системы и анализирует её актуальность.



```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe

To get started, select one of the options:
1. System version information.
2. Host type and role, DNS and NetBIOS.
3. Installed updates according to the Microsoft database.
Applied policies:
    4. Accounts.
    5. Passwords.
    6. Audit.
7. Network settings (TCP IP), open resources.
8. Running services.
9. File system.
10. Information about installed drivers.
0. Exit.

! The data received about the state of the system will be saved to the output.txt
file in the directory "D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer"

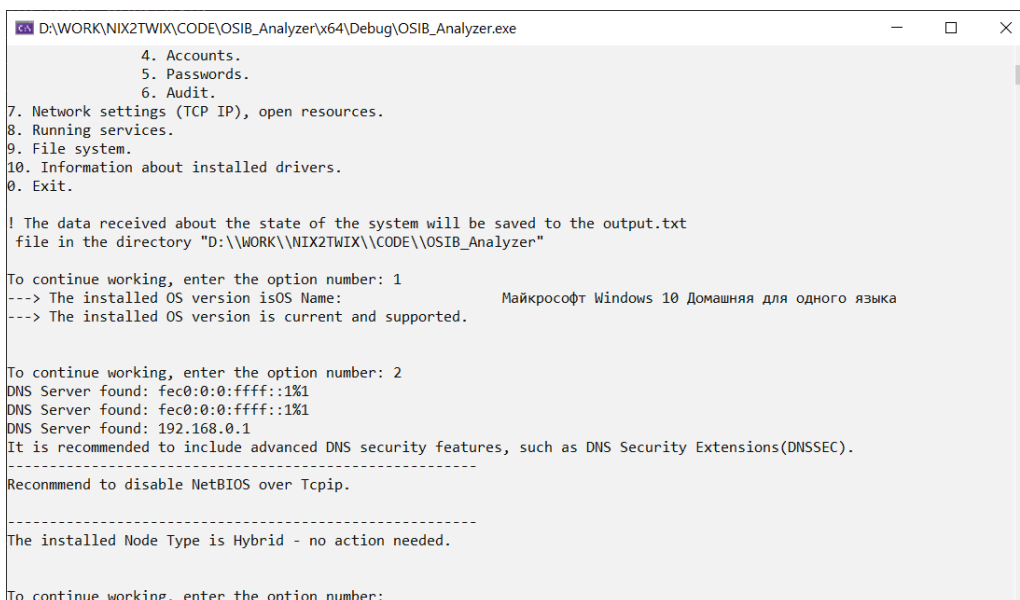
To continue working, enter the option number: 1
---> The installed OS version is OS Name: Майкрософт Windows 10 Домашняя для одного языка
---> The installed OS version is current and supported.

To continue working, enter the option number:
```

Рисунок 2 – Результат работы программы для проверки версии ОС

2. Анализ типа и роли узла, DNS и NetBIOS.

Как показано на рисунке 3, программа определяет имеющиеся DNS-сервера, параметры NetBIOS и тип узла и дает рекомендации по их настройке.



```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe

    4. Accounts.
    5. Passwords.
    6. Audit.
7. Network settings (TCP IP), open resources.
8. Running services.
9. File system.
10. Information about installed drivers.
0. Exit.

! The data received about the state of the system will be saved to the output.txt
file in the directory "D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer"

To continue working, enter the option number: 1
---> The installed OS version is OS Name: Майкрософт Windows 10 Домашняя для одного языка
---> The installed OS version is current and supported.

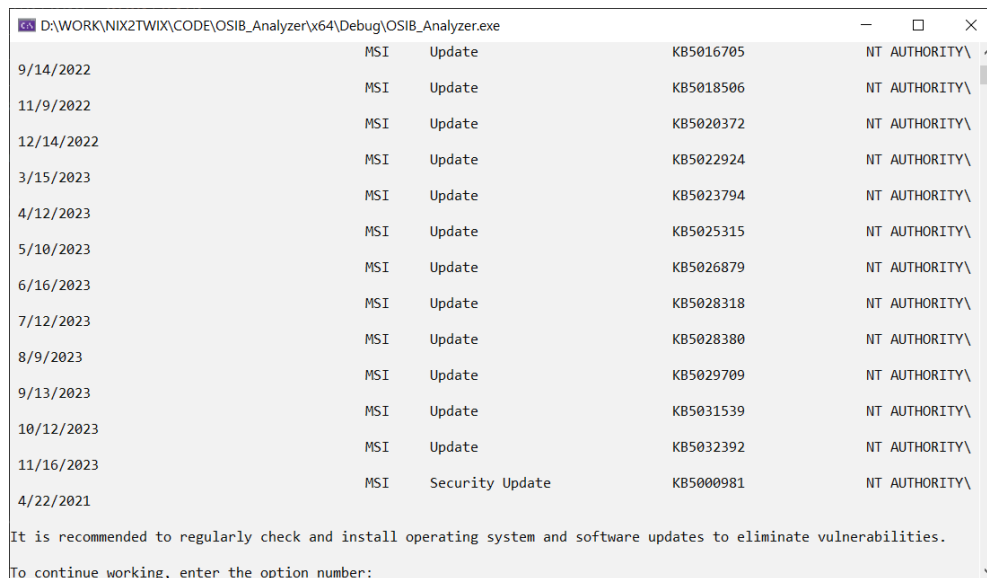
To continue working, enter the option number: 2
DNS Server found: fec0:0:0:ffff::1%1
DNS Server found: fec0:0:0:ffff::1%1
DNS Server found: 192.168.0.1
It is recommended to include advanced DNS security features, such as DNS Security Extensions(DNSSEC).
-----
Recommend to disable NetBIOS over Tcpip.
-----
The installed Node Type is Hybrid - no action needed.

To continue working, enter the option number: _
```

Рисунок 3 – Результат работы программы для проверки узла, DNS и NetBIOS

3. Установленные обновления

Как показано на рисунке 4, программа определяет имеющиеся обновления, а также дает рекомендации по их установке.



9/14/2022	MSI	Update	KB5016705	NT AUTHORITY\
11/9/2022	MSI	Update	KB5018506	NT AUTHORITY\
12/14/2022	MSI	Update	KB5020372	NT AUTHORITY\
3/15/2023	MSI	Update	KB5022924	NT AUTHORITY\
4/12/2023	MSI	Update	KB5023794	NT AUTHORITY\
5/10/2023	MSI	Update	KB5025315	NT AUTHORITY\
6/16/2023	MSI	Update	KB5026879	NT AUTHORITY\
7/12/2023	MSI	Update	KB5028318	NT AUTHORITY\
8/9/2023	MSI	Update	KB5028380	NT AUTHORITY\
9/13/2023	MSI	Update	KB5029709	NT AUTHORITY\
10/12/2023	MSI	Update	KB5031539	NT AUTHORITY\
11/16/2023	MSI	Update	KB5032392	NT AUTHORITY\
4/22/2021	MSI	Security Update	KB5000981	NT AUTHORITY\

It is recommended to regularly check and install operating system and software updates to eliminate vulnerabilities.

To continue working, enter the option number:

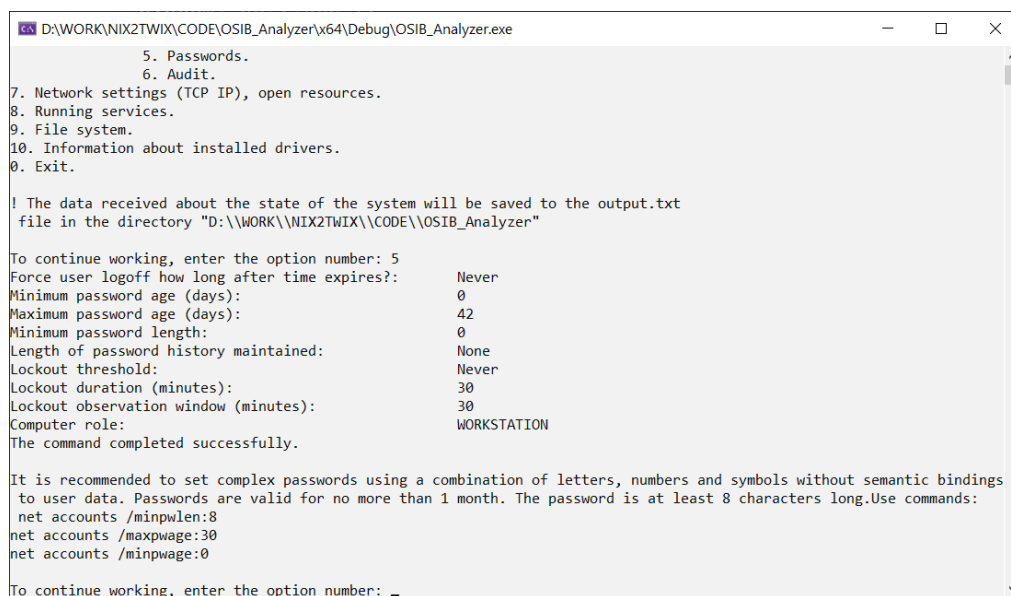
Рисунок 4 – Результат работы программы для проверки обновлений

4. Политика учетных записей

Как показано на рисунках 1.1-1.4 в приложении Б, программа определяет примененную политику учётных записей и даёт рекомендации по её настройке.

5. Парольная политика

Как показано на рисунке 5, программа определяет применённую политику паролей и рекомендует консольные команды для её изменения.



```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\Debug\OSIB_Analyzer.exe

5. Passwords.
6. Audit.
7. Network settings (TCP IP), open resources.
8. Running services.
9. File system.
10. Information about installed drivers.
0. Exit.

! The data received about the state of the system will be saved to the output.txt
file in the directory "D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer"

To continue working, enter the option number: 5
Force user logoff how long after time expires?: Never
Minimum password age (days): 0
Maximum password age (days): 42
Minimum password length: 0
Length of password history maintained: None
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: WORKSTATION
The command completed successfully.

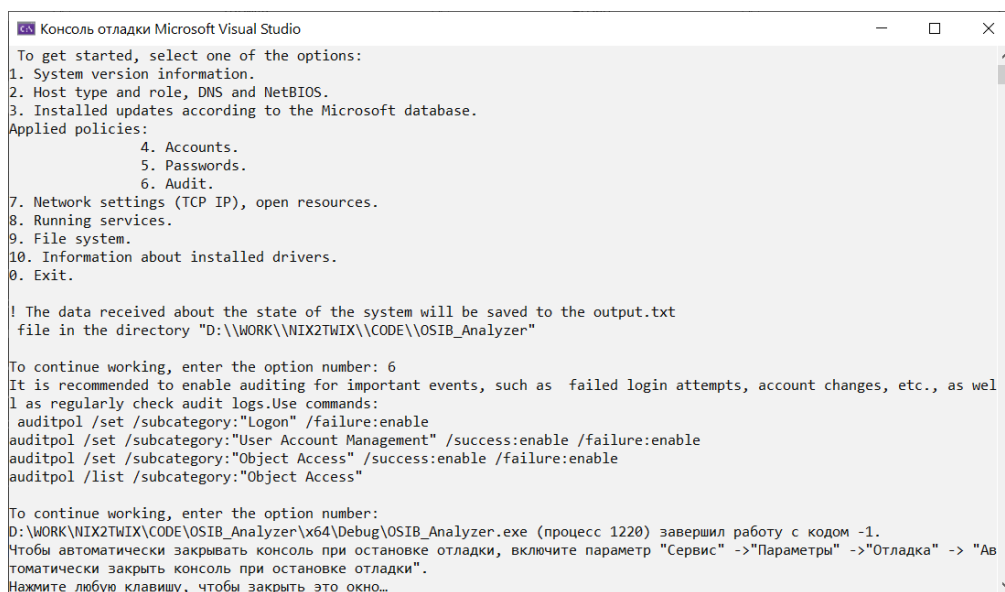
It is recommended to set complex passwords using a combination of letters, numbers and symbols without semantic bindings
to user data. Passwords are valid for no more than 1 month. The password is at least 8 characters long. Use commands:
net accounts /minpwlen:8
net accounts /maxpwage:30
net accounts /minpwage:0

To continue working, enter the option number: 
```

Рисунок 5 – Результат работы программы для проверки парольной политики

6. Политика аудита

Как показано на рисунке 6 и рисунках 2.1-2.3 в приложении Б, программа определяет примененную политику аудита и даёт рекомендации по её настройке, в частности, консольные команды для изменения параметров политики аудита.



```
Консоль отладки Microsoft Visual Studio

To get started, select one of the options:
1. System version information.
2. Host type and role, DNS and NetBIOS.
3. Installed updates according to the Microsoft database.
Applied policies:
4. Accounts.
5. Passwords.
6. Audit.
7. Network settings (TCP IP), open resources.
8. Running services.
9. File system.
10. Information about installed drivers.
10. Exit.

! The data received about the state of the system will be saved to the output.txt
file in the directory "D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer"

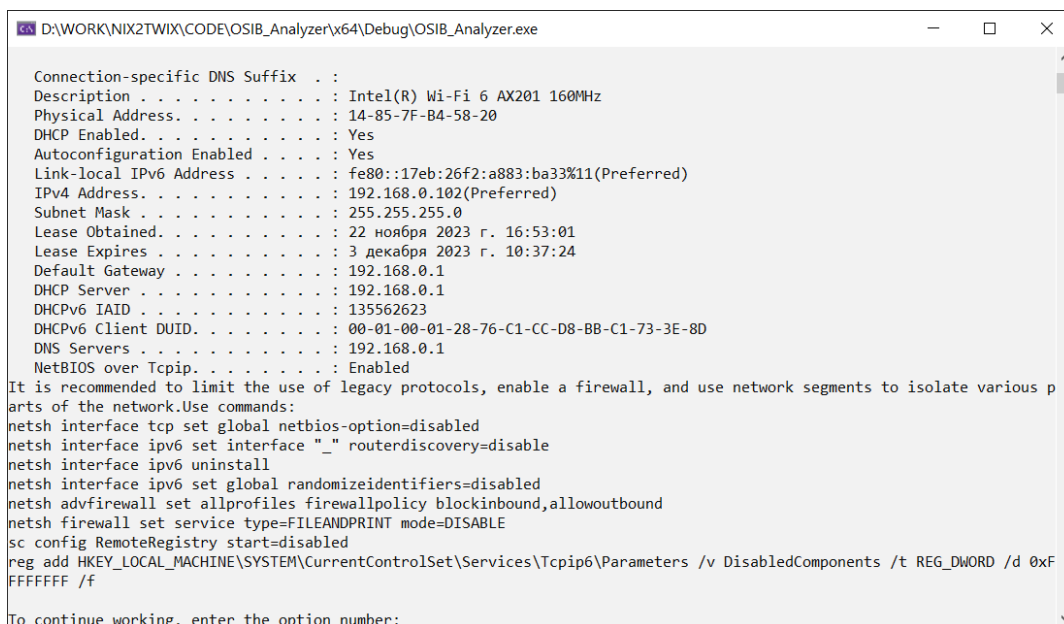
To continue working, enter the option number: 6
It is recommended to enable auditing for important events, such as failed login attempts, account changes, etc., as well as regularly check audit logs. Use commands:
auditpol /set /subcategory:"Logon" /failure:enable
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Object Access" /success:enable /failure:enable
auditpol /list /subcategory:"Object Access"

To continue working, enter the option number:
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe (процесс 1220) завершил работу с кодом -1.
Чтобы автоматически закрывать консоль при остановке отладки, включите параметр "Сервис" -> "Параметры" -> "Отладка" -> "Автоматически закрыть консоль при остановке отладки".
Нажмите любую клавишу, чтобы закрыть это окно...
```

Рисунок 6 – Результат работы программы для проверки политики аудита

7. Сетевые настройки (TCP IP):

Как показано на рисунке 7, программа выводит текущие сетевые настройки и даёт рекомендации по настройке – консольные команды для их изменения.



```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : 14-85-7F-B4-58-20
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::17eb:26f2:a883:ba33%11(Preferred)
IPv4 Address. . . . . : 192.168.0.102(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 22 ноября 2023 г. 16:53:01
Lease Expires . . . . . : 3 декабря 2023 г. 10:37:24
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 135562623
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-76-C1-CC-D8-BB-C1-73-3E-8D
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled

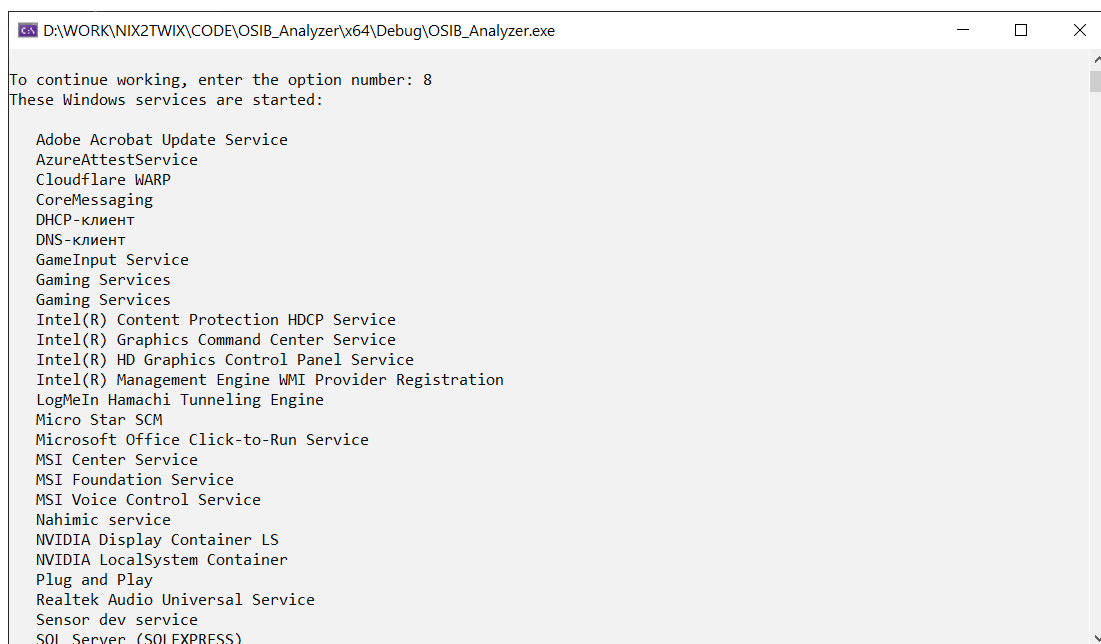
It is recommended to limit the use of legacy protocols, enable a firewall, and use network segments to isolate various parts of the network. Use commands:
netsh interface tcp set global netbios-option=disabled
netsh interface ipv6 set interface "_" routerdiscovery=disable
netsh interface ipv6 uninstall
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound
netsh firewall set service type=FILEANDPRINT mode=DISABLE
sc config RemoteRegistry start=disabled
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters /v DisabledComponents /t REG_DWORD /d 0xFFFFFFFF /f

To continue working, enter the option number: █
```

Рисунок 7 – Результат работы программы для проверки сетевых настроек

8. Запущенные сервисы

Как показано на рисунке 8.1 и 8.2, программа выводит список запущенных сервисов (служб) [1], а также даёт общие рекомендации по работе с ними.

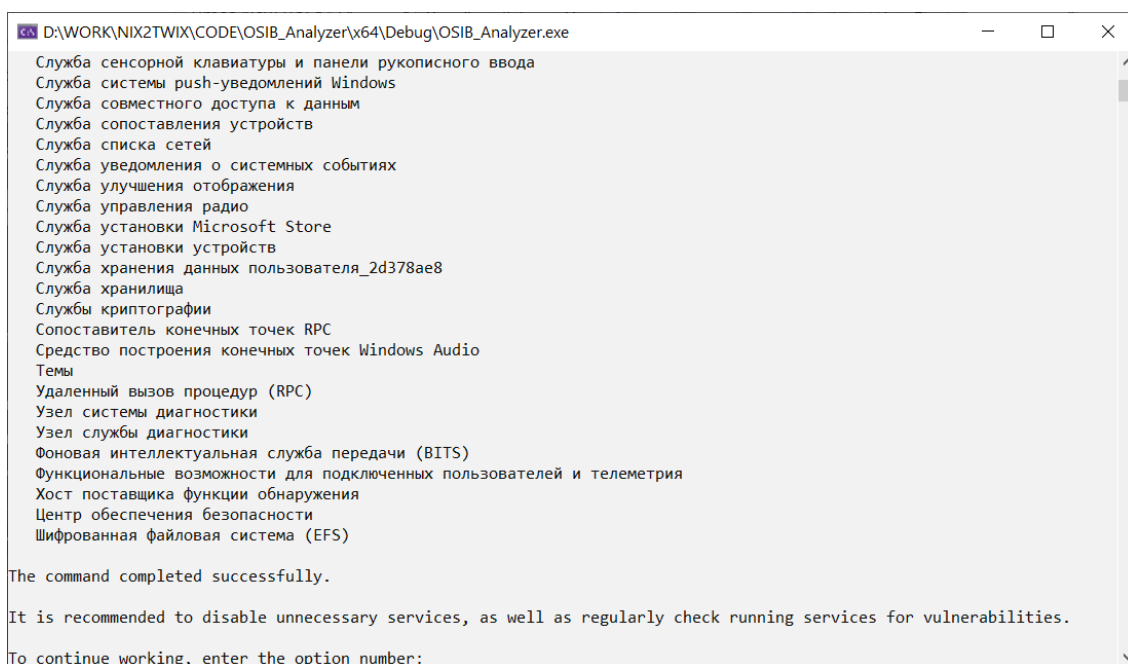


```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\64\Debug\OSIB_Analyzer.exe

To continue working, enter the option number: 8
These Windows services are started:

Adobe Acrobat Update Service
AzureAttestService
Cloudflare WARP
CoreMessaging
DHCP-клиент
DNS-клиент
GameInput Service
Gaming Services
Gaming Services
Intel(R) Content Protection HDCP Service
Intel(R) Graphics Command Center Service
Intel(R) HD Graphics Control Panel Service
Intel(R) Management Engine WMI Provider Registration
LogMeIn Hamachi Tunneling Engine
Micro Star SCM
Microsoft Office Click-to-Run Service
MSI Center Service
MSI Foundation Service
MSI Voice Control Service
Nahimic service
NVIDIA Display Container LS
NVIDIA LocalSystem Container
Plug and Play
Realtek Audio Universal Service
Sensor dev service
SQL Server (SQLEXPRESS)
```

Рисунок 8.1 – Результат работы программы для анализа запущенных сервисов



```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\64\Debug\OSIB_Analyzer.exe

Служба сенсорной клавиатуры и панели рукописного ввода
Служба системы push-уведомлений Windows
Служба совместного доступа к данным
Служба сопоставления устройств
Служба списка сетей
Служба уведомления о системных событиях
Служба улучшения отображения
Служба управления радио
Служба установки Microsoft Store
Служба установки устройств
Служба хранения данных пользователя_2d378ae8
Служба хранилища
Службы криптографии
Сопоставитель конечных точек RPC
Средство построения конечных точек Windows Audio
Темы
Удаленный вызов процедур (RPC)
Узел системы диагностики
Узел службы диагностики
Фоновая интеллектуальная служба передачи (BITS)
Функциональные возможности для подключенных пользователей и телеметрия
Хост поставщика функции обнаружения
Центр обеспечения безопасности
Шифрованная файловая система (EFS)

The command completed successfully.

It is recommended to disable unnecessary services, as well as regularly check running services for vulnerabilities.

To continue working, enter the option number:
```

Рисунок 8.2 – Результат работы программы для анализа запущенных сервисов

9. Файловая система

Как показано на рисунках 3.1-3.2 в приложении Б, программа открывает панель управления дисками для просмотра текущего вида файловой системы. В

консоль модуль анализа выводит рекомендации относительно типа файловой системы и методам работы с ней.

10. Установленные драйверы

Как показано на рисунках 4.1-4.5 в приложении Б, программа выводит список используемых драйверов и предлагает рекомендации по их своевременному обновлению.

2.2 Рекомендуемые параметры конфигурации

Поскольку проектируемый модуль должен определять и анализировать параметры конфигурации ОС, ниже приведены прописанные в нём параметры, рекомендуемые как общие параметры безопасности по умолчанию. Важно отметить, что любые параметры безопасности должны выбираться исходя из целей работы автоматизированной системы, её ресурсов и активов.

- *вид операционной системы;*

Рекомендуется использовать последнюю версию операционной системы с установленными обновлениями для обеспечения безопасности и поддержки новых функций безопасности, т.е. от Windows 10 и выше.

- *тип и роль узла, DNS и NetBIOS;*

По умолчанию рекомендуется тип узла Hybrid, который использует метод широковещательной передачи и обращение к определенному серверу. Рекомендуется, как правило, для больших сетей с различными сегментами. Для DNS рекомендуется включать расширенные средства защиты, такие как расширения безопасности DNS (DNSSEC). Также рекомендуется минимизировать использование NetBIOS из-за его уязвимостей, если это возможно.

- *установленные обновления (согласно базе Microsoft):*

По умолчанию рекомендуется регулярно проверять и устанавливать обновления операционной системы и программного обеспечения для устранения уязвимостей.

- *примененная политика учетных записей:*

По умолчанию рекомендуется минимизировать количество аккаунтов с высокими привилегиями, то есть использовать принцип наименьших привилегий и ограничивать доступ к административным аккаунтам.

- *примененная политика паролей:*

Рекомендуется задавать сложные пароли с использованием комбинации букв, цифр и символов, без семантических привязок к данным о пользователе. Срок действия паролей не больше 1 месяца. Длина пароля не менее 8 символов.

- *примененная политика аудита:*

Рекомендуется включить аудит для важных событий, таких как неудачные попытки входа, изменение учетных записей и прочее, а также регулярно проверять журналы аудита. Для повышения безопасности системы требуется:

- Включить «Аудит входа в систему» (успех/отказ). Все события входа и выхода в систему могут быть важными при расследовании инцидентов ИБ.
- «Аудит доступа к службе каталогов» не требуется.
- Включить «Аудит изменения политики» (успех). Все изменения политики аудита должны быть согласованы, иначе данное действие является потенциально опасным и подозрительным.
- Включить «Аудит отслеживания процессов» (успех/отказ). Отслеживание таких событий, как активация программы, выход из процесса, обработка дублирования и непрямого доступ к объекту может быть важно для критических объектов.
- Включить «Аудит системных событий» (отказ) – это минимальное требование безопасности на случай возникновения ошибок.
- Включить «Аудит использования привилегий (успех). Данная политика позволяет контролировать полномочия и привилегии на локальном компьютере и контроллере домена.

- Включить «Аудит событий входа» (успех). Регистрация событий, связанные с регистрацией пользователя в домене, также является важным событием безопасности.
- Включить «Аудит управления учетными записями» (успех). Все события управления учетными записями также должны регистрироваться, поскольку должны быть согласованными.

Конфигурация расширенной политики аудита (всё, что не упомянуто, не требует изменений):

- Аудит службы проверки подлинности Kerberos (успех и отказ)
- Аудит проверки учетных данных (успех и отказ)
- Аудит других событий управления учетными записями (успех)
- Аудит создания процессов (успех)
- Аудит завершения процессов (успех)
- Аудит сервера сетевых политик – без аудита
- Аудит общих папок (успех)
- Аудит файловой системы (успех)
- Целостность системы – без аудита
- *сетевые настройки (TCP/IP):*

Рекомендуется ограничить использование устаревших протоколов, включить брандмауэр и использовать сетевые сегменты для изоляции различных частей сети. В частности, отключение NetBIOS, ICMPv6, отключение IPv6 (если не используется), отключение автонастройки адреса IPv6, уастройка брандмауэра для блокировки входящих пакетов, Отключение File and Printer Sharing, отключение Remote Registry, отключение IPv6 на уровне реестра (если не используется) [2].

- *запущенные сервисы:*

Рекомендуется отключить ненужные сервисы, а также регулярно проверять запущенные сервисы на наличие уязвимостей.

– *файловая система:*

Принимается тип файловой системы – NTFS. Рекомендуется применять принцип наименьших привилегий при настройке прав доступа. Регулярно проводить аудит критически важных файлов и папок на предмет необычной активности.

– *установленные драйверы:*

Рекомендуется использовать только подписанные драйверы от доверенных источников и регулярно обновлять драйвера для устранения уязвимостей.

ЗАКЛЮЧЕНИЕ

В условиях быстрого технологического прогресса и увеличения цифровой уязвимости, анализ защищенности операционных систем становится ключевой задачей, направленной на обеспечение стойкости и безопасности информационных систем. В рамках данной курсовой работы была поставлена задача разработки программы-анализатора, которая предоставляет не только возможность оценки текущего уровня безопасности, но и конкретные рекомендации для улучшения безопасности системы, соответствуя современным требованиям и стандартам безопасности. Данная цель была достигнута.

Осознание стратегической значимости исследования безопасности операционных систем, особенно Windows, в контексте постоянно развивающихся угроз и тесной связи технологий с повседневной жизнью, подчеркивает актуальность данного анализа. Он ориентирован на постоянное совершенствование механизмов безопасности, нацеленное на предотвращение потенциальных угроз и атак, гарантируя тем самым стабильность и надежность информационных систем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Столлинс В., Берштейн И. В., Красиков И. В. Операционные системы: внутренняя структура и принципы проектирования. - 9-е издание изд. - Киев: Вильямс, 2020. - 1264 с.
2. Документация по системе безопасности // Microsoft Learn URL: <https://learn.microsoft.com/ru-ru/security/> (дата обращения: 01.12.2023).
3. Системные файлы Windows: где хранятся, как отобразить или восстановить // Hetman Software URL: https://hetmanrecovery.com/ru/recovery_news/what-does-windows-system-file-mean.htm (дата обращения: дата обращения: 26.11.23).
4. Сетевая безопасность – Обзор // CoderLessons URL: <https://coderlessons.com/tutorials/kachestvo-programmnogo-obespecheniia/izuchite-bezopasnost-seti/setevaia-bezopasnost-kratkoe-rukovodstvo> (дата обращения: 26.11.23).
5. Комплексная защита корпоративной информации: Уч. пособие. - М.: МИЭТ, 2009. - 404 с.
6. Страуструп Б. Язык программирования C++. Краткий курс. - 2-е издание изд. - Киев: Диалектика, 2019. - 320 с.
7. Шилдт Г. C++. Полное руководство. Классическое издание. - 2-е издание изд. - Киев: Диалектика-Вильямс, 2020. - 800 с.

Листинг 1 – Код программы-анализатора

```
#include <iostream>
#include <Windows.h>
#include <fstream>
#include <filesystem>
#include <stdio.h>
#include <locale>
#include <string>
#include <regex>
using namespace std;

int main()
{
    system("color F0");
    std::string command;
    char bufferIpconfig[256];
    FILE* pipeIpconfig;
    FILE* pipeFindstr;
    FILE* pipeSysteminfo;
    FILE* pipe;
    LPCWSTR LPcommand = L"cmd.exe /C auditpol /get /category:*";
    HINSTANCE hInstance = ShellExecute(NULL, L"runas", L"cmd.exe", LPcommand,
    NULL, SW_SHOWNORMAL);

    SetConsoleCP(1251);
    SetConsoleOutputCP(65001);

    ifstream sysInfoFile;
    ofstream infoFile;
    string line;

    int t = 1;

    cout << "\n To get started, select one of the options: ";
    cout << "\n1. System version information.";
    cout << "\n2. Host type and role, DNS and NetBIOS.";
    cout << "\n3. Installed updates according to the Microsoft database.";
    cout << "\nApplied policies:";
    cout << "\n\t\t4. Accounts.";
    cout << "\n\t\t5. Passwords.";
    cout << "\n\t\t6. Audit.";
    cout << "\n7. Network settings (TCP IP), open resources.";
    cout << "\n8. Running services.";
    cout << "\n9. File system.";
    cout << "\n10. Information about installed drivers.";
    cout << "\n0. Exit.";

    cout << "\n\n! The data received about the state of the system will be saved
to the output.txt\n"
    << " file in the directory " << filesystem::current_path();

    while (t != 0)
    {
        cout << "\n\nTo continue working, enter the option number: ";
        cin >> t;
        switch (t)
        {
            case 1:
                // Анализ версии ОС
                system("systeminfo >> output.txt");
```


Листинг 1 – Код программы-анализатора (продолжение)

```

sysInfoFile.open("output.txt");
while (std::getline(sysInfoFile, line))
{
    if (line.find("OS Name:") != std::string::npos)
    {
        std::smatch match;
        std::regex pattern(R"((\d+))");
        if (std::regex_search(line, match, pattern))
        {
            int version = std::stoi(match[0]);
            if (version >= 10)
            {
                std::cout << "---> The installed OS
version is" + line << "\n";
                std::cout << "---> The installed OS
version is current and supported.\n";
            }
            else {
                std::cout << "---> It is recommended to
upgrade the OS version to 10 and above.\n";
            }
        }
        break;
    }
}
sysInfoFile.close();

break;

case 2:

    // Анализ конфигурации DNS
    system("ipconfig /all >> output.txt");

    sysInfoFile.open("output.txt");
    while (std::getline(sysInfoFile, line)) {
        if (line.find("DNS Servers") != std::string::npos) {
            std::regex
pattern("\\b(?:\\d{1,3}\\.){3}\\d{1,3}\\b|\\b(?:[0-9a-fA-F]{0,4}){2,7}[0-9a-fA-
F]{0,4}%\\d+\\b");
            std::sregex_iterator it(line.begin(), line.end(),
pattern);
            std::sregex_iterator end;

            for (; it != end; ++it) {
                std::cout << "DNS Server found: " << it->str()
<< std::endl;
            }
        }
    }
    std::cout << "It is recommended to include advanced DNS security
features, "
        << "such as DNS Security Extensions(DNSSEC).";
    sysInfoFile.close();
    cout << "\n-----
--\n";

    // Анализ конфигурации NetBIOS
    system("nbtstat -n >> output.txt");

    sysInfoFile.open("output.txt");
    while (std::getline(sysInfoFile, line))
    {

```

Листинг 1 – Код программы-анализатора (продолжение)

```

        if (line.find("NetBIOS over Tcpip") != std::string::npos)
        {
            std::smatch match;
            std::regex pattern(":\\s*(\\w+)");
            if (std::regex_search(line, match, pattern)) {
                std::cout << "Recommmend to disable NetBIOS
over Tcpip.\n";
            }
            else {
                std::cout << "No action needed.\n";
            }
            break;
        }
    }
    sysInfoFile.close();

    cout << "\n-----\n";

    // Анализ типа и роли узла
    system("nltest /dsgetdc >> output.txt 2> nul");

    sysInfoFile.open("output.txt");
    while (std::getline(sysInfoFile, line))
    {
        if (line.find("Node Type") != std::string::npos) {
            if (line == "    Node Type . . . . . :
Broadcast") {
                std::cout << "The installed Node Type is
Broadcast - no action needed.\n";
            }
            else if (line == "    Node Type . . . . . :
. : Peer to Peer") {
                std::cout << "The installed Node Type is Peer
to Peer - consider changing to Hybrid.\n";
            }
            else if (line == "    Node Type . . . . . :
. : Mixed") {
                std::cout << "The installed Node Type is Mixed
- consider changing to Hybrid.\n";
            }
            else if (line == "    Node Type . . . . . :
. : Hybrid") {
                std::cout << "The installed Node Type is Hybrid
- no action needed.\n";
            }
            else {
                std::cout << "Unknown Node Type found.\n";
            }
            break;
        }
    }
    sysInfoFile.close();

    break;

case 3:
    system("wmic qfe list >> output.txt");
    system("wmic qfe list");
    std::cout << "It is recommended to regularly check and install
operating system "
        << "and software updates to eliminate vulnerabilities.";

```

Листинг 1 – Код программы-анализатора (продолжение)

```
        break;
    case 4:
        system("net localgroup Администраторы");
        cout << "\n-----\n";

        system("gpresult /Scope User /v");
        std::cout << "\nBy default, it is recommended to minimize the
number of accounts "
        << "with high privileges, that is, use the principle of
least privileges and "
        << "restrict access to administrative accounts.";

        break;

    case 5:
        system("net accounts");
        std::cout << "It is recommended to set complex passwords using a
combination of letters,"
        << " numbers and symbols without semantic bindings to user
data. Passwords are valid"
        << " for no more than 1 month. The password is at least 8
characters long.";
        std::cout << "Use commands:\n net accounts /minpwlen:8\nnet
accounts /maxpwage:30\nnet accounts /minpwage:0";
        break;

    case 6:
        ShellExecute(nullptr, L"runas", L"cmd.exe", L"/K auditpol /get
/category:*", nullptr, SW_SHOWNORMAL);

        std::cout << "It is recommended to enable auditing for important
events, such as "
        << " failed login attempts, account changes, etc., as well
as regularly check audit logs.";
        std::cout << "Use commands:\n auditpol /set
/subcategory:\"Logon\" /failure:enable\n"
        << "auditpol /set /subcategory:\"User Account Management\"
/success:enable /failure:enable\n"
        << "auditpol /set /subcategory:\"Object Access\"
/success:enable /failure:enable\n"
        << "auditpol /list /subcategory:\"Object Access\"";
        break;

    case 7:
        system("ipconfig /all");
        std::cout << "It is recommended to limit the use of legacy
protocols, enable a firewall, "
        << "and use network segments to isolate various parts of
the network.";
        std::cout << "Use commands:\nnetsh interface tcp set global
netbios-option=disabled\n"
        << "netsh interface ipv6 set interface \"Имя_интерфейса\"
routerdiscovery=disable\n"
        << "netsh interface ipv6 uninstall\n"
        << "netsh interface ipv6 set global
randomizeidentifiers=disabled\n"
        << "netsh advfirewall set allprofiles firewallpolicy
blockinbound,allowoutbound\n"
        << "netsh firewall set service type=FILEANDPRINT
mode=DISABLE\n"
        << "sc config RemoteRegistry start=disabled\n"
```

Листинг 1 – Код программы-анализатора (продолжение)

```
        << "reg add
HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Tcpip6\\Parameters /v
DisabledComponents /t REG_DWORD /d 0xFFFFFFFF /f";
        break;

    case 8:
        system("net start");
        std::cout << "It is recommended to disable unnecessary services,
as well as "
        << "regularly check running services for vulnerabilities.";
        break;

    case 9:
        system("diskmgmt");
        std::cout << "It is recommended to use NTFS and apply the
principle of least privilege when configuring access rights. "
        << "Regularly audit critical files and folders for unusual
activity.";
        break;
    case 10: system("driverquery >> output.txt");
        system("driverquery");
        std::cout << "It is recommended to use only signed drivers from
trusted sources and regularly update "
        << "drivers to eliminate vulnerabilities.";
        break;

    case 0: break;
    default: cout << "Error! No option found\n"; break;
}
}
return 0;
}
```

```

D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe
Alias name      Администраторы
Comment        Администраторы имеют полные, ничем не ограниченные права доступа к компьютеру или домену

Members

-----
victory
Администратор
The command completed successfully.

-----

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on [ 26.11.2023 at 14:54:25

RSOP data for MSI\victory on MSI : Logging Mode
-----

OS Configuration:      Standalone Workstation
OS Version:            10.0.19045
Site Name:             N/A
Roaming Profile:       N/A
Local Profile:         C:\Users\Вика
Connected over a slow link?: No
  
```

Рисунок 1.1 – Результат работы программы для проверки учетных записей

```

D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe
USER SETTINGS
-----

Last time Group Policy was applied: 26.11.2023 at 10:37:33
Group Policy was applied from:      N/A
Group Policy slow link threshold:   500 kbps
Domain Name:                       MSI
Domain Type:                       <Local Computer>

Applied Group Policy Objects
-----
N/A

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups
-----
Отсутствует
Все
Локальная учетная запись и член группы "Администраторы"
Администраторы
Пользователи
Пользователи журналов производительности
ИНТЕРАКТИВНЫЕ
КОНСОЛЬНЫЙ ВХОД
Прошедшие проверку
Данная организация
  
```

Рисунок 1.2 – Результат работы программы для проверки учетных записей (продолжение)

```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe

Высокий обязательный уровень

The user has the following security privileges
-----

Resultant Set Of Policies for User
-----

Software Installations
-----
N/A

Logon Scripts
-----
N/A

Logoff Scripts
-----
N/A

Public Key Policies
-----
N/A

Administrative Templates
-----
N/A

Folder Redirection
```

Рисунок 1.3 – Результат работы программы для проверки учетных записей (продолжение)

```
D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe

N/A

Folder Redirection
-----
N/A

Internet Explorer Browser User Interface
-----
N/A

Internet Explorer Connection
-----
N/A

Internet Explorer URLs
-----
N/A

Internet Explorer Security
-----
N/A

Internet Explorer Programs
-----
N/A

By default, it is recommended to minimize the number of accounts with high privileges, that is, use the principle of least privileges and restrict access to administrative accounts.

To continue working, enter the option number: _
```

Рисунок 1.4 – Результат работы программы для проверки учетных записей (продолжение)

Выбрать Администратор: C:\Windows\System32\cmd.exe

Категория или подкатегория	Параметр
Политика аудита системы	
Система	
Расширение системы безопасности	Без аудита
Целостность системы	Успех и сбой
Драйвер IPSEC	Без аудита
Другие системные события	Успех и сбой
Изменение состояния безопасности	Успех
Вход/выход	
Вход в систему	Успех и сбой
Выход из системы	Успех
Блокировка учетной записи	Успех
Основной режим IPsec	Без аудита
Быстрый режим IPsec	Без аудита
Расширенный режим IPsec	Без аудита
Специальный вход	Успех
Другие события входа и выхода	Без аудита
Сервер сетевых политик	Успех и сбой
Заявки пользователей или устройств на доступ	Без аудита
Членство в группа	Без аудита
Доступ к объектам	
Файловая система	Без аудита
Реестр	Без аудита
Объект-задание	Без аудита
SAM	Без аудита
Службы сертификации	Без аудита
Создано приложением	Без аудита
Работа с дескриптором	Без аудита
Общий файловый ресурс	Без аудита
Отбрасывание пакета платформой фильтрации	Без аудита

Рисунок 2.1 – Результат работы программы для проверки политики аудита

Выбрать Администратор: C:\Windows\System32\cmd.exe

Заявки пользователей или устройств на доступ	Без аудита
Членство в группа	Без аудита
Доступ к объектам	
Файловая система	Без аудита
Реестр	Без аудита
Объект-задание	Без аудита
SAM	Без аудита
Службы сертификации	Без аудита
Создано приложением	Без аудита
Работа с дескриптором	Без аудита
Общий файловый ресурс	Без аудита
Отбрасывание пакета платформой фильтрации	Без аудита
Подключение платформы фильтрации	Без аудита
Другие события доступа к объекту	Без аудита
Сведения об общем файловом ресурсе	Без аудита
Съемные носители	Без аудита
Сверка с централизованной политикой	Без аудита
Использование прав	
Использование прав, не затрагивающее конфиденциальные данные	Без аудита
Другие события использования прав	Без аудита
Использование прав, затрагивающее конфиденциальные данные	Без аудита
Подробное отслеживание	
Создание процесса	Без аудита
Завершение процесса	Без аудита
Активность DPMI	Без аудита
События RPC	Без аудита
Самонастраиваемые события	Без аудита
События изменений прав маркера	Без аудита
Изменение политики	
Аудит изменения политики	Успех

Рисунок 2.2 – Результат работы программы для проверки политики аудита (продолжение)

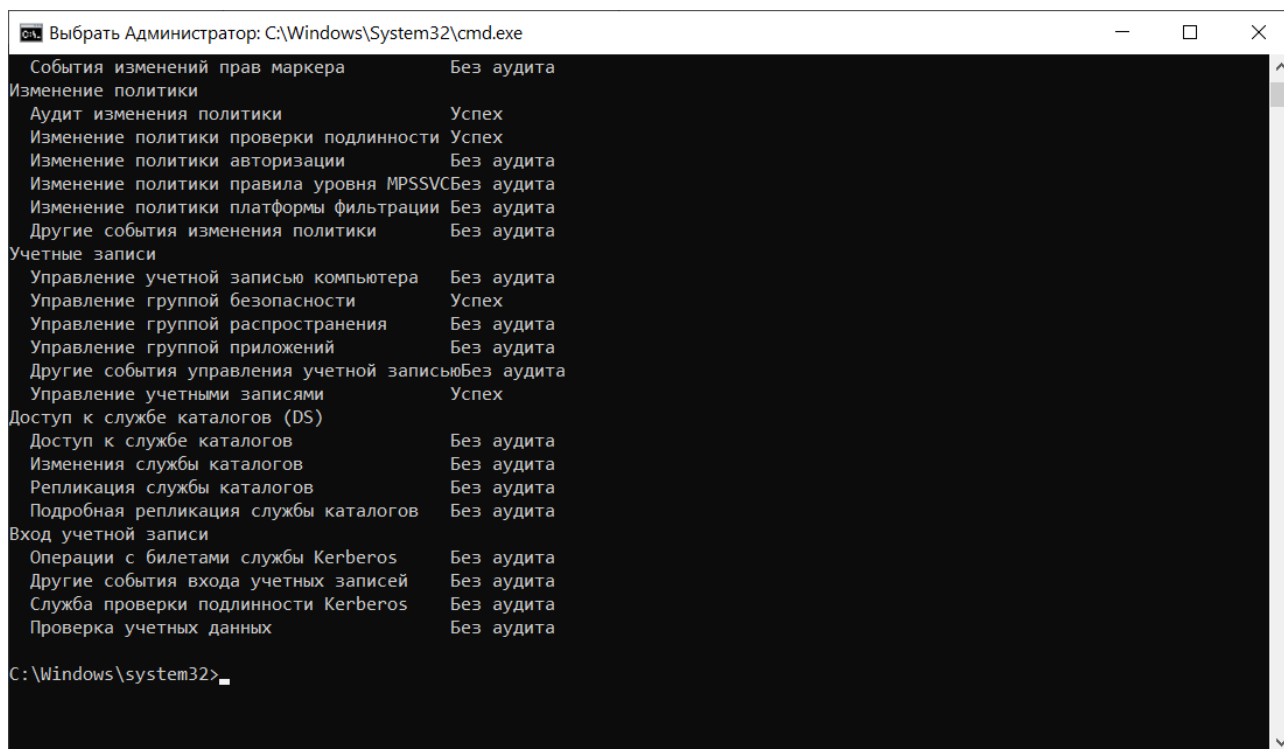


Рисунок 2.3 – Результат работы программы для проверки политики аудита (продолжение)

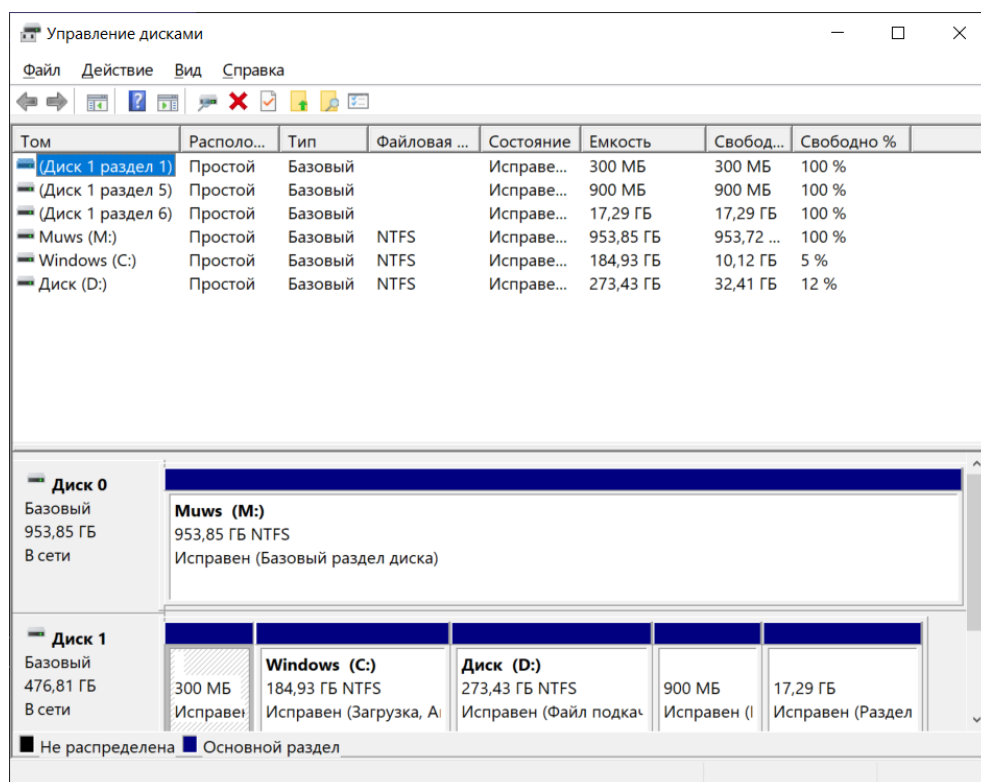


Рисунок 3.1 – Результат вызова метода анализа файловой системы

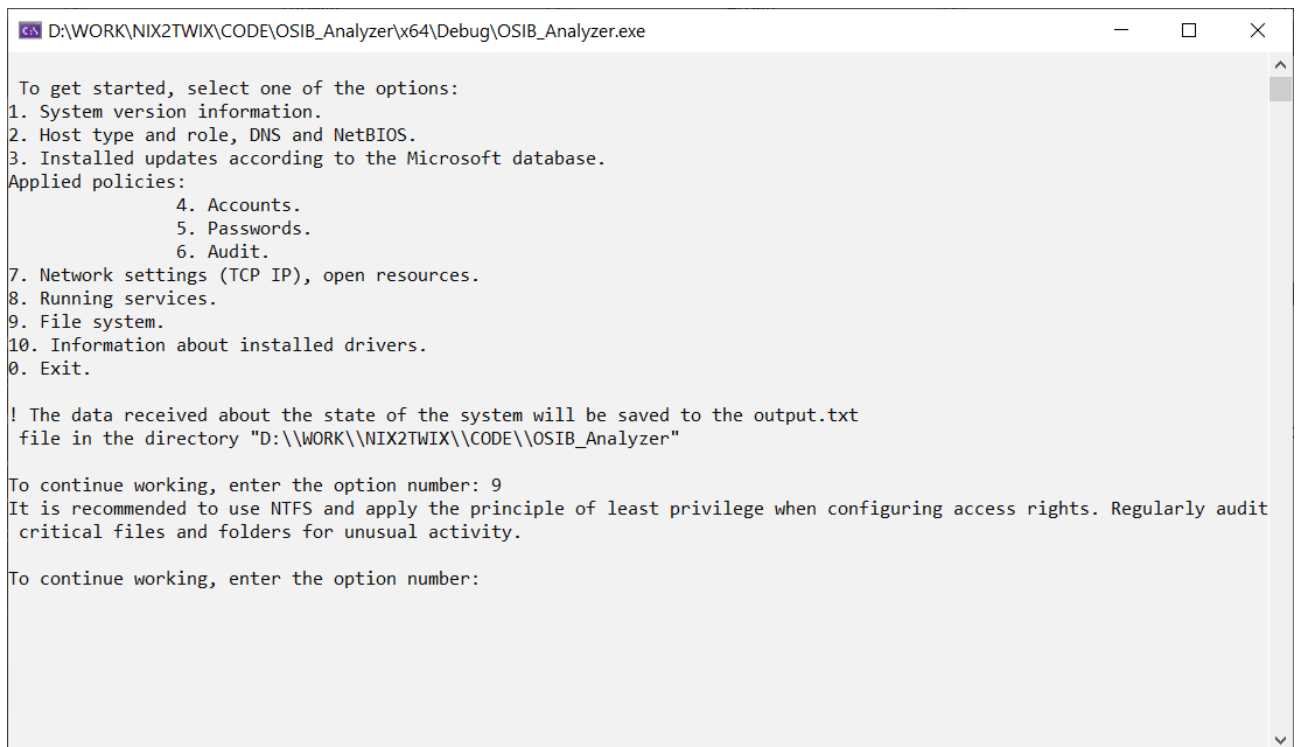


Рисунок 3.2 – Результат вызова метода анализа файловой системы (продолжение)

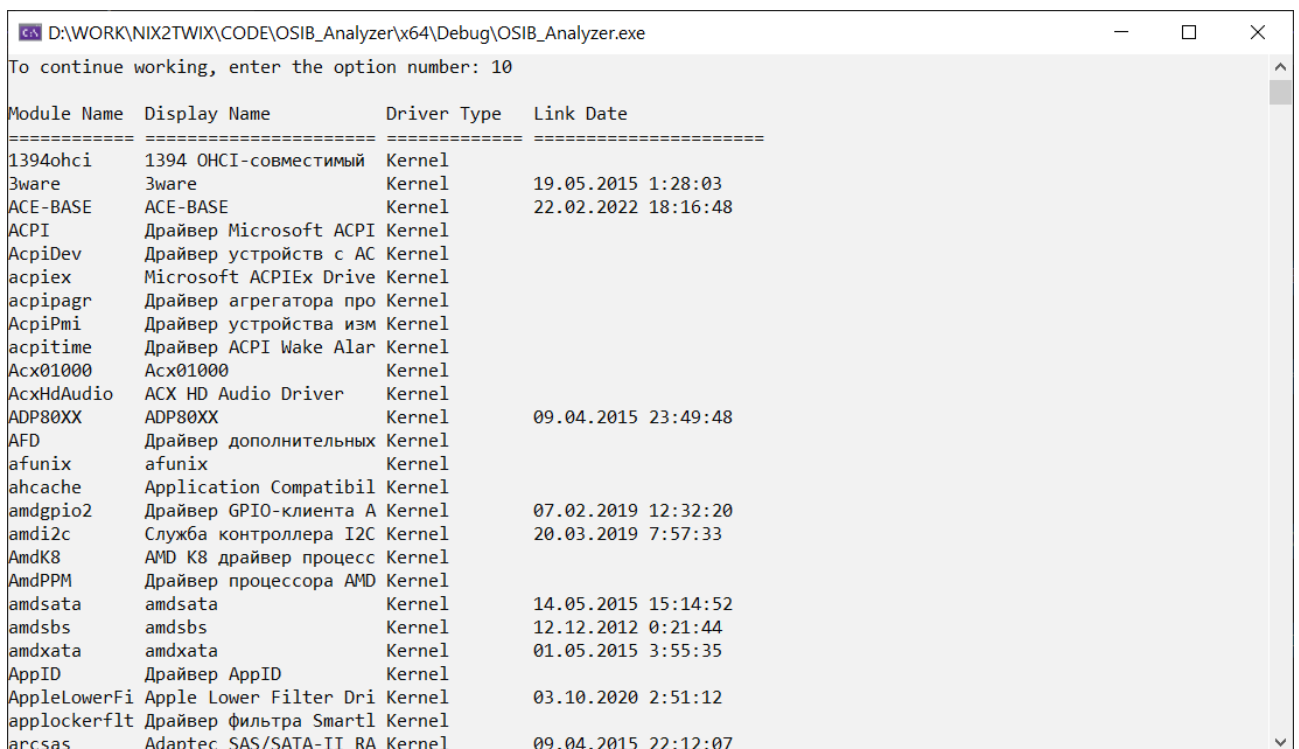


Рисунок 4.1 – Результат вызова метода анализа драйверов

D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe			
AsyncMac	Драйвер асинхронного н	Kernel	
atapi	Канал IDE	Kernel	
b06bdrv	Сетевой адаптер VBD QL	Kernel	25.05.2016 10:03:08
bam	Background Activity Mo	Kernel	
BasicDisplay	BasicDisplay	Kernel	
BasicRender	BasicRender	Kernel	
bcmfn2	bcmfn2 Service	Kernel	01.11.2016 5:09:15
Beep	Beep	Kernel	
bindflt	Windows Bind Filter Dr	File System	
browser	Браузер	File System	
BthA2dp	Microsoft Bluetooth A2	Kernel	
BthEnum	Служба перечислителя B	Kernel	
BthHFEnum	Драйвер профиля гарнит	Kernel	
BthLEEnum	Драйвер Bluetooth с ни	Kernel	
BthMini	Драйвер радио Blueoot	Kernel	
BTHMODEM	Драйвер связи Bluetooth	Kernel	
BthPan	Устройства Bluetooth (Kernel	
BTHPORT	Драйвер порта Bluetooth	Kernel	
BTHUSB	Драйвер порта USB ради	Kernel	
bttflt	Фильтр Microsoft Hyper	Kernel	
buttonconver	Служба для устройств к	Kernel	
CAD	Драйвер вынесения реше	Kernel	
cdfs	CD/DVD File System Rea	File System	
cdrom	Драйвер CD-ROM дисково	Kernel	
cht4iscsi	cht4iscsi	Kernel	05.02.2019 16:51:31
cht4vbd	Драйвер виртуальной ши	Kernel	05.02.2019 16:47:51
CimFS	CimFS	File System	
circlass	Потребительские ИК-уст	Kernel	
CldFlt	Windows Cloud Files Fi	File System	
CLFS	Common Log (CLFS)	Kernel	

Рисунок 4.2 – Результат вызова метода анализа драйверов (продолжение)

D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe			
CmBatt	Драйвер батареи с ACPI	Kernel	
CNG	CNG	Kernel	
cnghwassist	CNG Hardware Assist al	Kernel	
CompositeBus	Драйвер перечислителя	Kernel	
condrv	Console Driver	Kernel	
dam	Desktop Activity Moder	Kernel	
Dfsc	Драйвер клиента простр	File System	
disk	Драйвер диска	Kernel	
dmvsc	dmvsc	Kernel	
dptf_acpi	dptf_acpi	Kernel	04.11.2020 3:24:14
dptf_cpu	dptf_cpu	Kernel	04.11.2020 3:24:16
drmkaud	Доверенные аудиодрайве	Kernel	
DXGKrn1	LDDM Graphics Subsys	Kernel	
ebdrv	Адаптер QLogic 10 Giga	Kernel	25.05.2016 10:01:05
EhStorClass	Enhanced Storage Filte	Kernel	
EhStorTcgDrv	Драйвер Майкрософт для	Kernel	
EneTechIo	EneTechIo	Kernel	08.05.2020 9:07:19
ErrDev	Microsoft Hardware Err	Kernel	
esif_lf	esif_lf	Kernel	04.11.2020 3:24:41
exfat	exFAT File System Driv	File System	
fastfat	FAT12/16/32 File Syste	File System	
fdc	Драйвер контроллера ги	Kernel	
FileCrypt	FileCrypt	File System	
FileInfo	File Information FS Mi	File System	
Filetrace	Filetrace	File System	
flpydisk	Драйвер дисководов гибк	Kernel	
FltMgr	Диспетчер фильтров	File System	
FsDepends	File System Dependency	File System	
fvevol	Драйвер фильтра шифров	Kernel	
gameflt	gameflt	File System	

Рисунок 4.3 – Результат вызова метода анализа драйверов (продолжение)

D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe			
gencounter	Счетчик создания Micro	Kernel	
GENERICDRV	GENERICDRV	Kernel	18.09.2020 9:26:30
genericusbfn	Общий класс функции US	Kernel	
GPIOClx0101	Microsoft GPIO Class E	Kernel	
GpuEnergyDrv	GPU Energy Driver	Kernel	
Hamachi	LogMeIn Hamachi Virtua	Kernel	30.03.2015 16:28:42
hanvonugeemf	HID-Compliant Mouse	Kernel	25.05.2021 9:27:41
HdAudAddServ	Драйвер функции UAA дл	Kernel	
HDAudBus	Драйвер для шины UAA д	Kernel	
HidBatt	Драйвер батареи ИБП HI	Kernel	
HidBth	Microsoft Bluetooth HI	Kernel	
hidi2c	Драйвер минипорта для	Kernel	
hidinterrupt	Общий драйвер для кноп	Kernel	
HidIr	Драйвер Microsoft Infr	Kernel	
hidspi	Драйвер минипорта для	Kernel	
HidSpiCx	HidSpi KMDF Class Exte	Kernel	
HidUsb	Драйвер класса HID Mic	Kernel	
HoYoProtect	HoYoProtect	Kernel	02.08.2023 11:26:00
HpSAMD	HpSAMD	Kernel	27.03.2013 0:36:54
HTTP	HTTP-служба	Kernel	
hvcrash	hvcrash	Kernel	
hvservice	Hypervisor/Virtual Mac	Kernel	
HwNClx0101	Microsoft Hardware Not	Kernel	
hwpolicy	Hardware Policy Driver	Kernel	
hyperkbd	hyperkbd	Kernel	
HyperVideo	HyperVideo	Kernel	
i8042prt	Драйвер i8042-клавиату	Kernel	
iagpio	Драйвер контроллера GP	Kernel	23.07.2018 12:04:46
iai2c	Intel(R) Serial IO I2C	Kernel	23.07.2018 12:04:39
iaLPSS2i_GPI	Драйвер версии 2 Intel	Kernel	19.04.2018 10:53:24

Рисунок 4.4 – Результат вызова метода анализа драйверов (продолжение)

D:\WORK\NIX2TWIX\CODE\OSIB_Analyzer\x64\Debug\OSIB_Analyzer.exe			
wdiwifi	WDI Driver Framework	Kernel	
WdmCompanion	WdmCompanionFilter	Kernel	
WdNisDrv	Системный драйвер пров	Kernel	
WFPLWFS	Платформа фильтрации M	Kernel	
WIMMount	WIMMount	File System	
WindowsTrust	Windows Trusted Execut	Kernel	
WindowsTrust	Служба безопасности до	Kernel	
WINIO	WINIO	Kernel	10.08.2018 9:24:22
WinMad	Служба WinMad	Kernel	19.06.2019 16:18:11
WinNat	Драйвер NAT Windows	Kernel	
WINUSB	Драйвер WinUsb	Kernel	
WinVerbs	Служба WinVerbs	Kernel	19.06.2019 16:18:12
WmiAcpi	Microsoft Windows Mana	Kernel	
Wof	Windows Overlay File S	File System	
WpdUpFltr	WPD Upper Class Filter	Kernel	
ws2ifsl	Драйвер WinSock IFS	Kernel	
WudFPf	User Mode Driver Frame	Kernel	
WUDFRd	Windows Driver Foundat	Kernel	
WUDFWpdFs	Драйвер файловой систе	Kernel	
WUDFWpdMtp	WUDFWpdMtp	Kernel	
xboxgip	Драйвер протокола игро	Kernel	
xinputhid	Драйвер-фильтр HID XIN	Kernel	
XPpenTablet	XP-Pen Tablet	Kernel	28.05.2021 6:19:47
Xvdd	XVDD Port Driver	Kernel	
MpKsl8ff0e44	MpKsl8ff0e447	Kernel	
It is recommended to use only signed drivers from trusted sources and regularly update drivers to eliminate vulnerabilities.			
To continue working, enter the option number: █			

Рисунок 4.5 – Результат вызова метода анализа драйверов (продолжение)