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»

Павловой Виктории Сергеевны

230711

студента гр. \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
Тема курсовой работы

«Анализ защищённости заданной конфигурации механизмов безопасности ОС Windows»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Параметры, определяемые проектируемым модулем, в соответствии с методическими указаниями.

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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

(ФИО)

Задание выдал \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

07 ноября 23

21.02.2023 г.

21.02.2023 г.

21.02.2023 г.

21.02.2023 г.

21.02.2023 г.

21.02.2023 г.

21.02.2023 г.

(ФИО)

(подпись)

Дата выдачи задания «\_\_» \_\_\_\_\_\_ 20\_\_г

в соответствии с методическими указаниями.

График выполнения КР \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рекомендации и особые отметки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_» \_\_\_\_\_\_\_\_20\_\_г

# **СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 4](#_Toc153530568)

[1 АСПЕКТЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ 5](#_Toc153530569)

[1.1 Параметры безопасности по умолчанию 7](#_Toc153530570)

[1.2 Анализ конфигурации параметров безопасности по умолчанию 9](#_Toc153530571)

[2 АНАЛИЗ ЗАЩИЩЁННОСТИ ЗАДАННОЙ КОНФИГУРАЦИИ МЕХАНИЗМОВ БЕЗОПАСНОСТИ ОС WINDOWS 12](#_Toc153530572)

[2.1 Описание программы-анализатора 13](#_Toc153530573)

[2.2 Рекомендуемые параметры конфигурации 18](#_Toc153530574)

[ЗАКЛЮЧЕНИЕ 22](#_Toc153530575)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 23](#_Toc153530576)

[ПРИЛОЖЕНИЕ А 24](#_Toc153530577)

[ПРИЛОЖЕНИЕ Б 29](#_Toc153530578)

# **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 предопределенными 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 антималварный 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 требоеваниям 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 предопределенными 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):

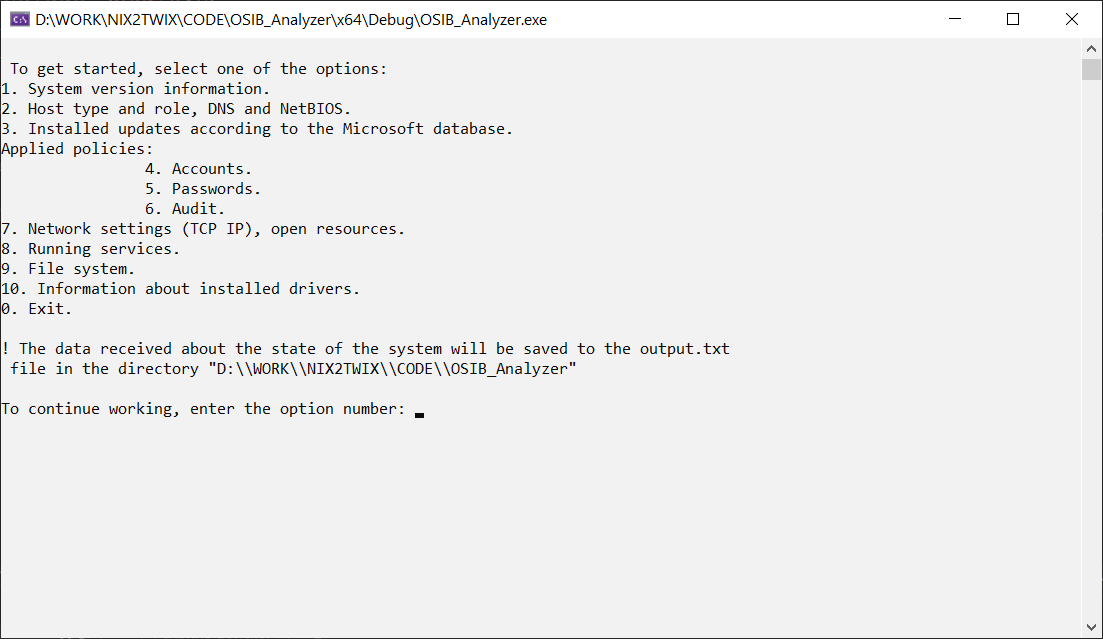


Рисунок 1 – Меню (опции) модуля

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.

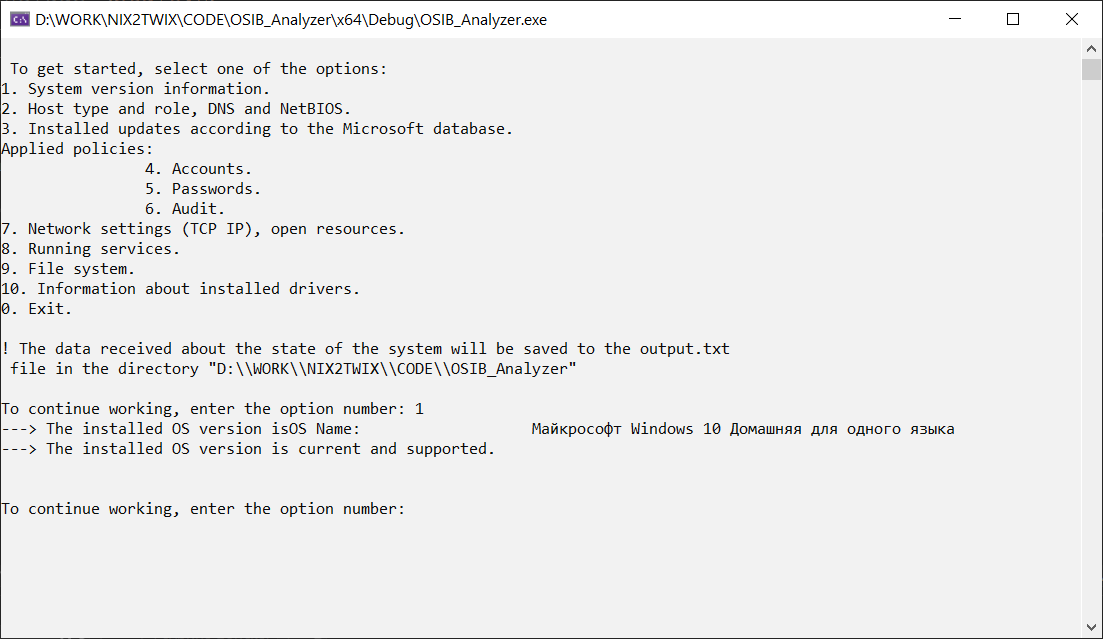


Рисунок 2 – Результат работы программы для проверки версии ОС

1. **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.

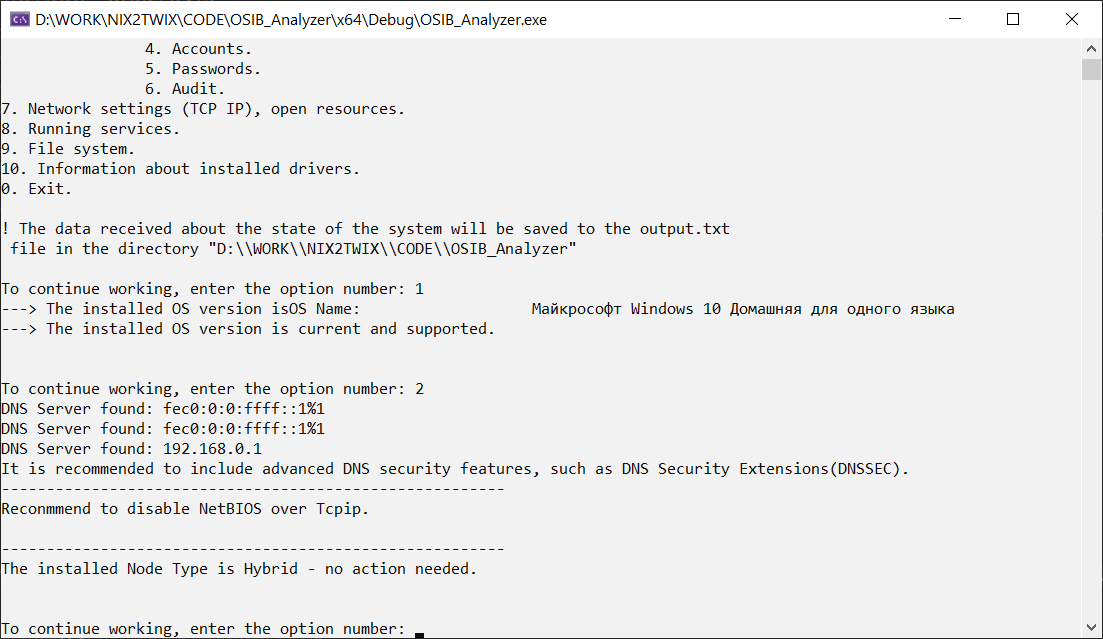


Рисунок 3 – Результат работы программы для проверки узла, DNS и NetBIOS

1. **Установленные обновления**

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

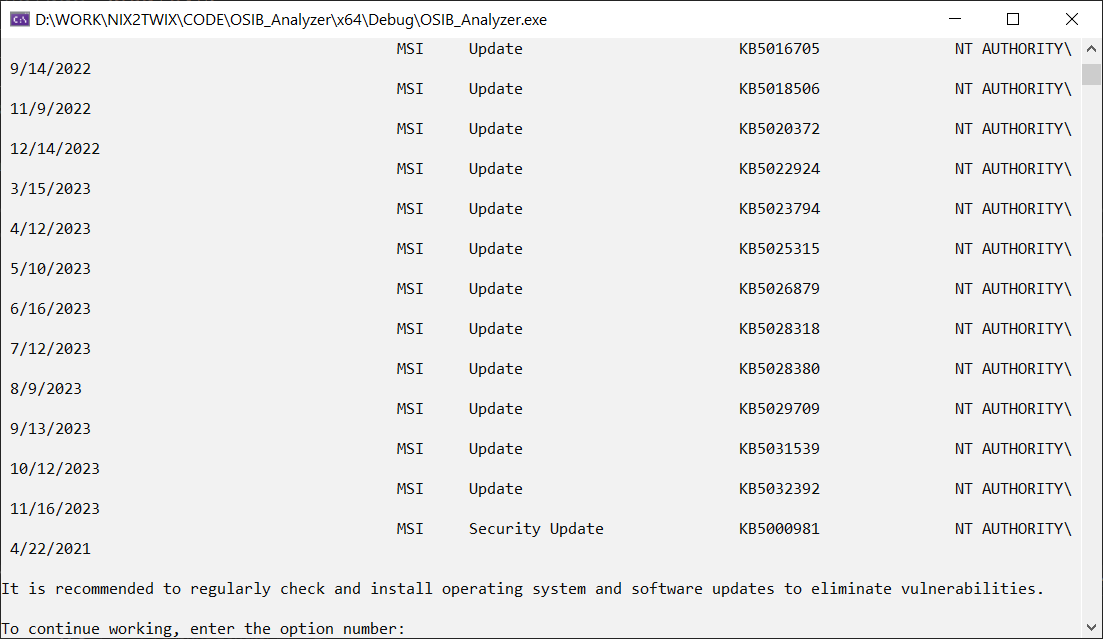


Рисунок 4 – Результат работы программы для проверки обновлений

1. **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.

1. **Парольная политика**

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

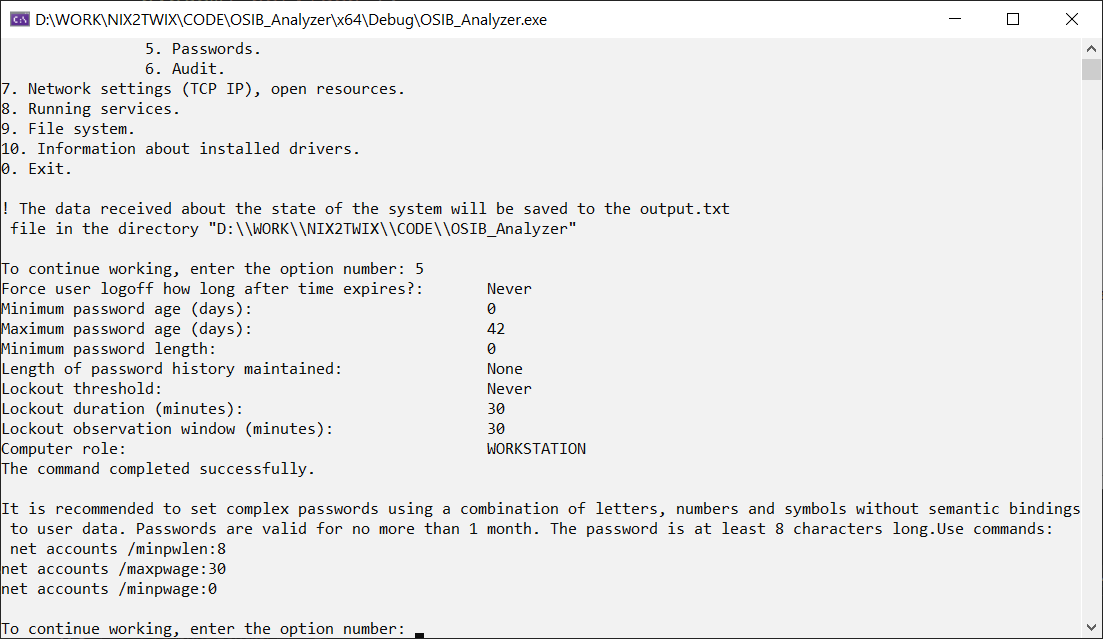


Рисунок 5 – Результат работы программы для проверки парольной политики

1. **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.

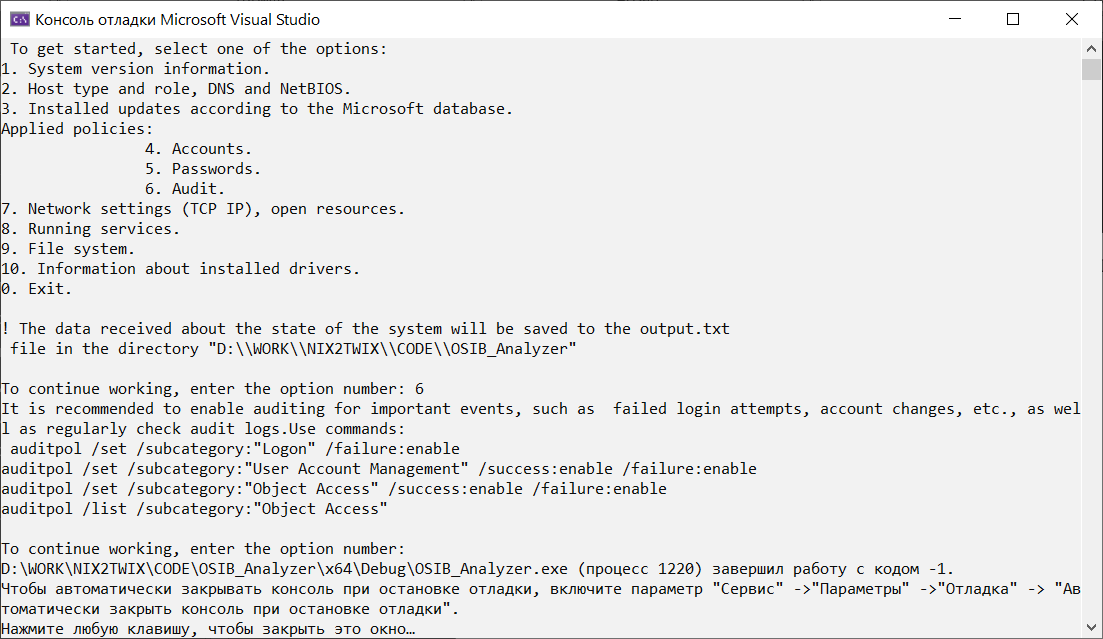


Рисунок 6 – Результат работы программы для проверки политики аудита

1. **Сетевые настройки (TCP IP):**

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

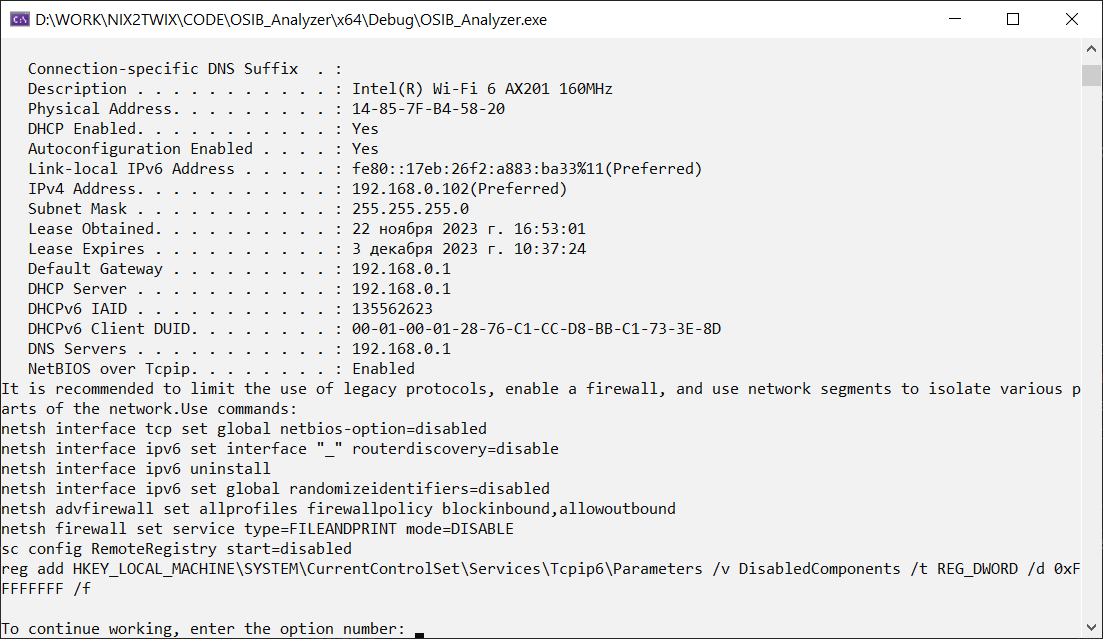


Рисунок 7 – Результат работы программы для проверки сетевых настроек

1. **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.

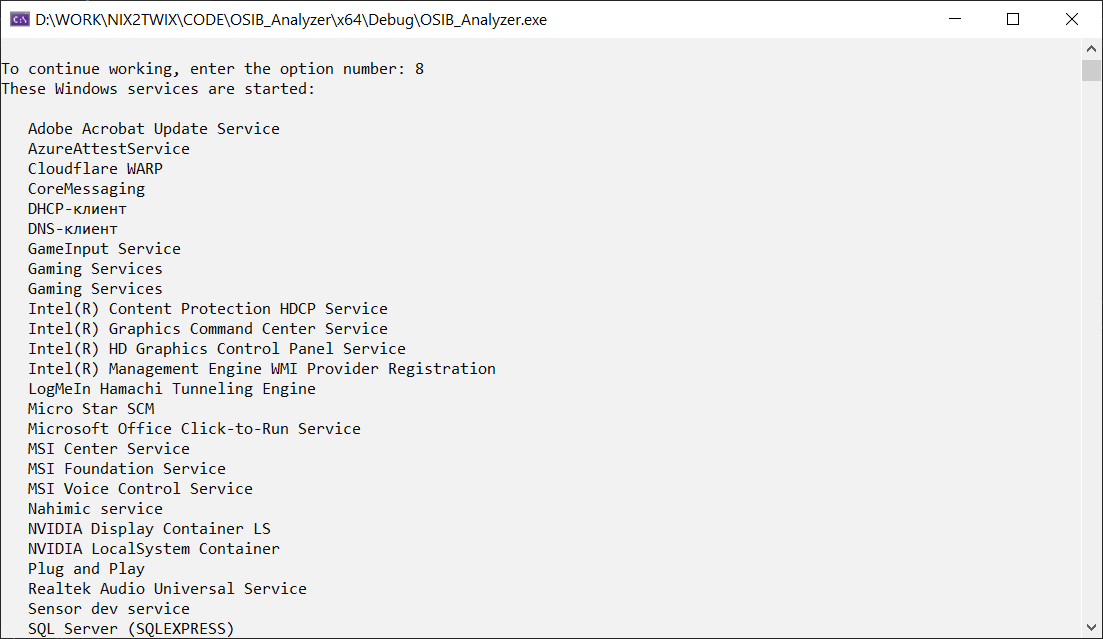


Рисунок 8.1 – Результат работы программы для анализа запущенных сервисов

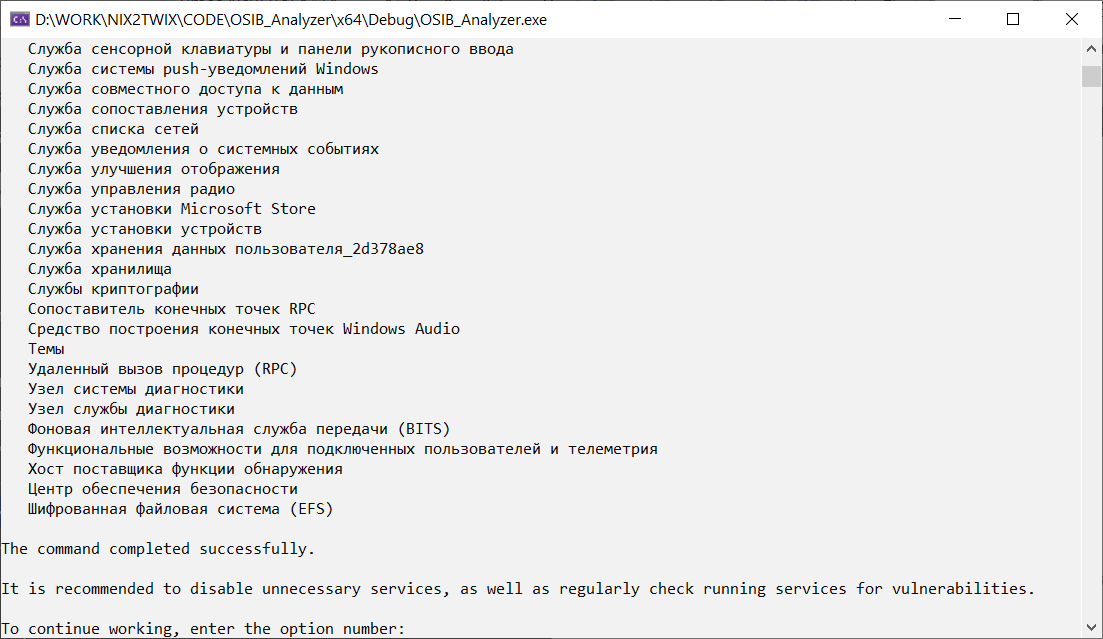


Рисунок 8.2 – Результат работы программы для анализа запущенных сервисов

1. **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.

1. **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 ркомендуется 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 непрямой 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, yастройка 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. Столлингс 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 С++. 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.

# **ПРИЛОЖЕНИЕ А**

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 << "Reconmmend 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;

}

# **ПРИЛОЖЕНИЕ Б**

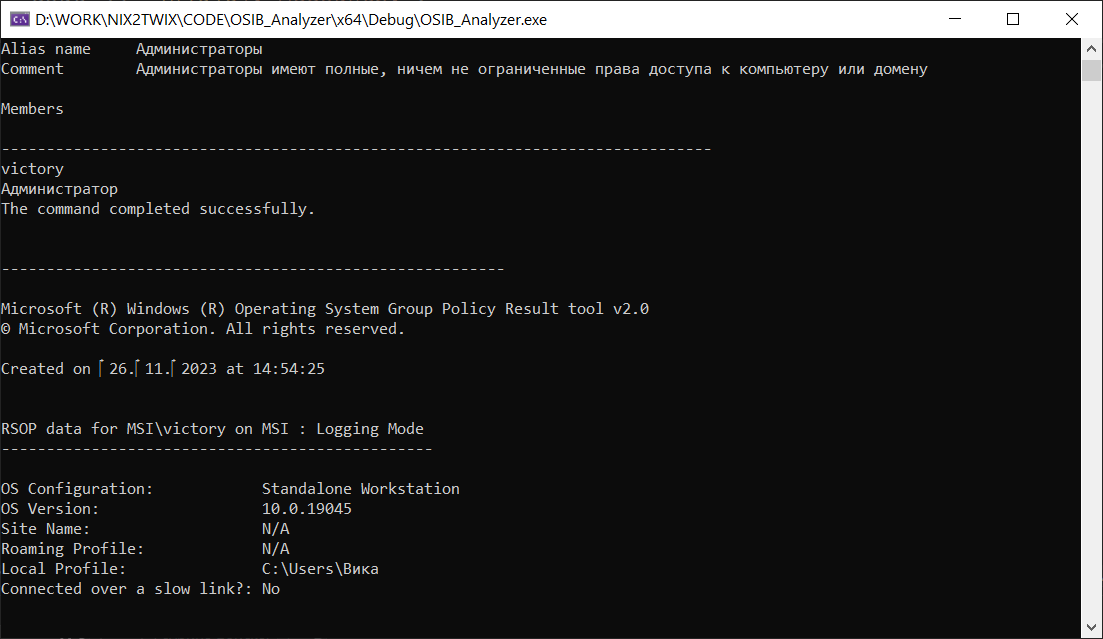


Рисунок 1.1 – Результат работы программы для проверки учетных записей

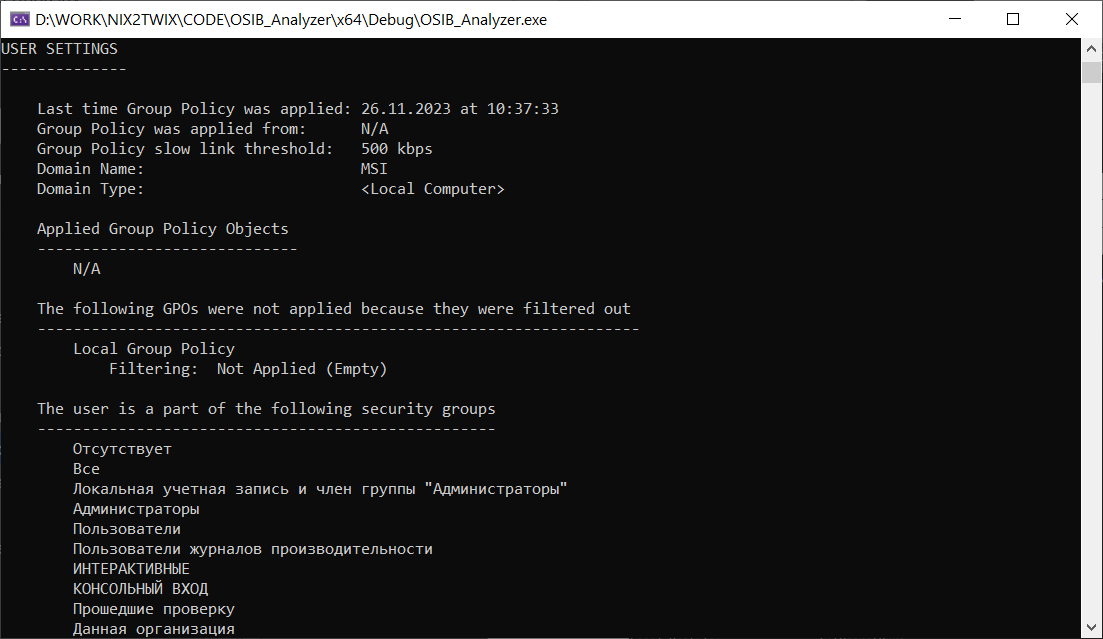


Рисунок 1.2 – Результат работы программы для проверки учетных записей (продолжение)

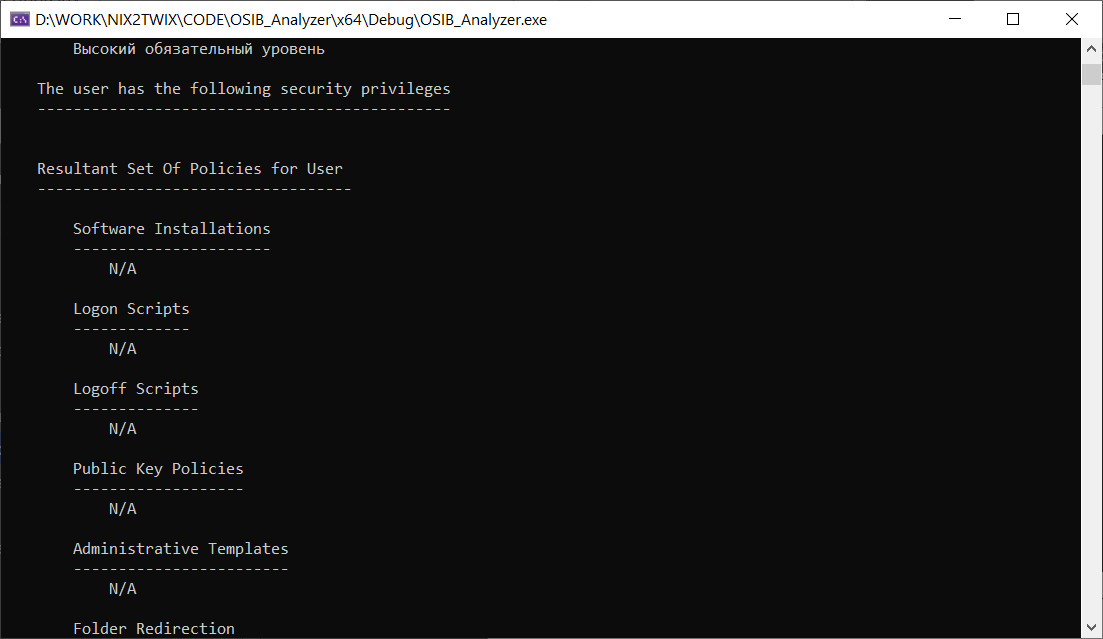


Рисунок 1.3 – Результат работы программы для проверки учетных записей (продолжение)

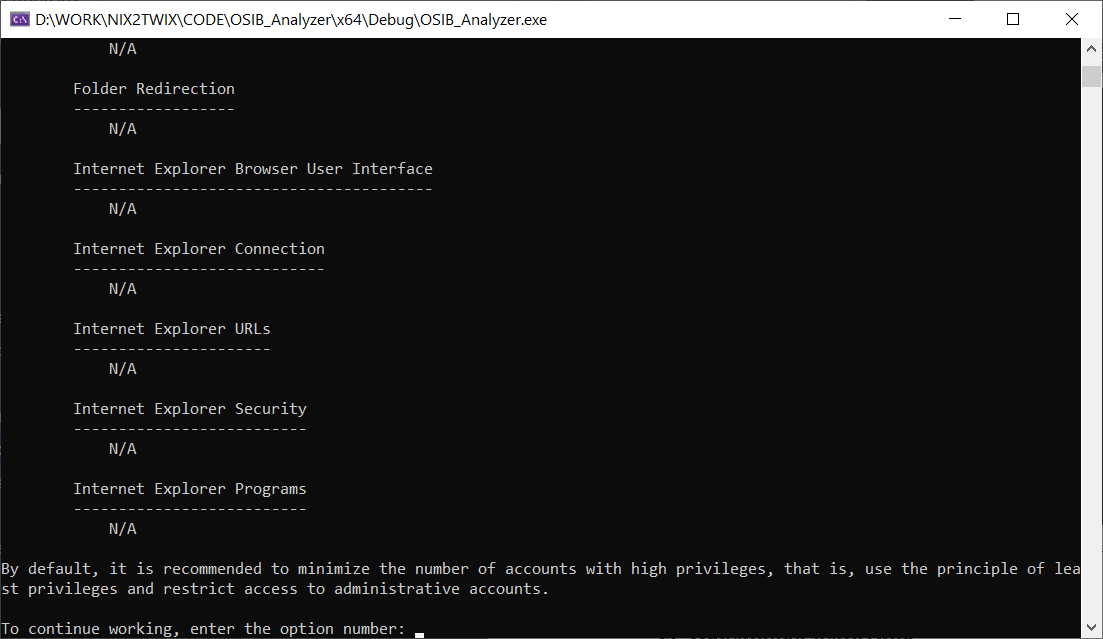
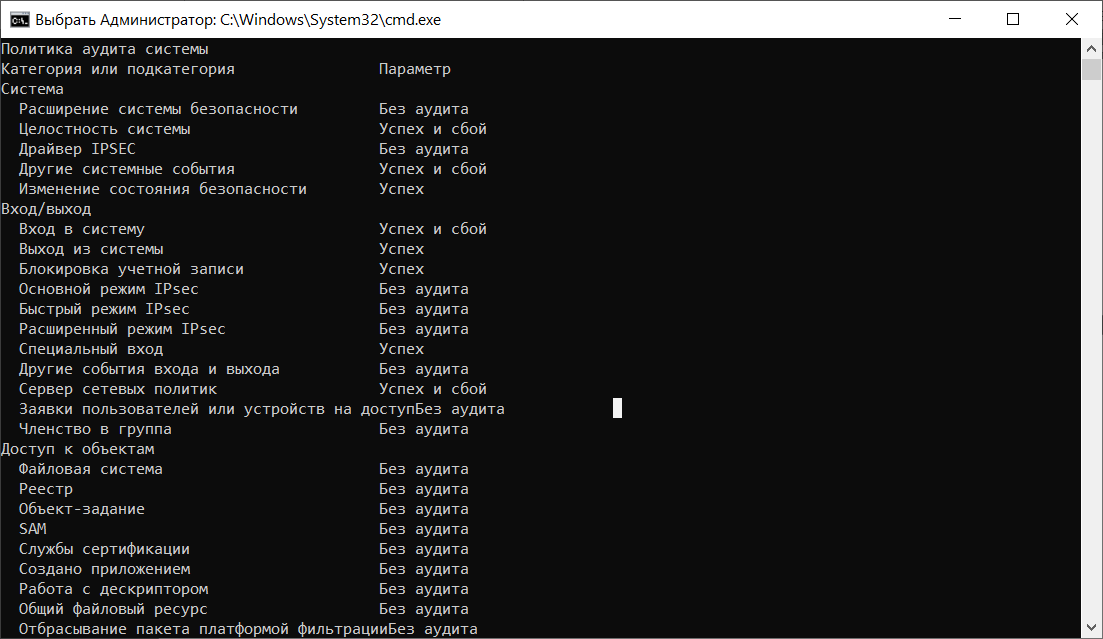
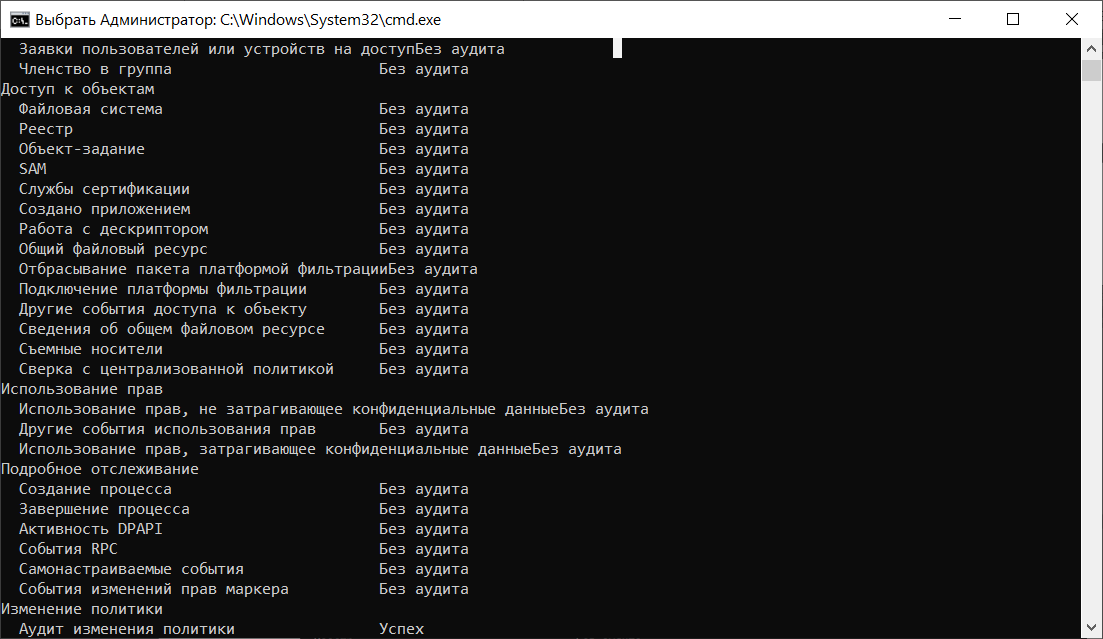


Рисунок 1.4 – Результат работы программы для проверки учетных записей (продолжение)

Рисунок 2.1 – Результат работы программы для проверки политики аудита

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

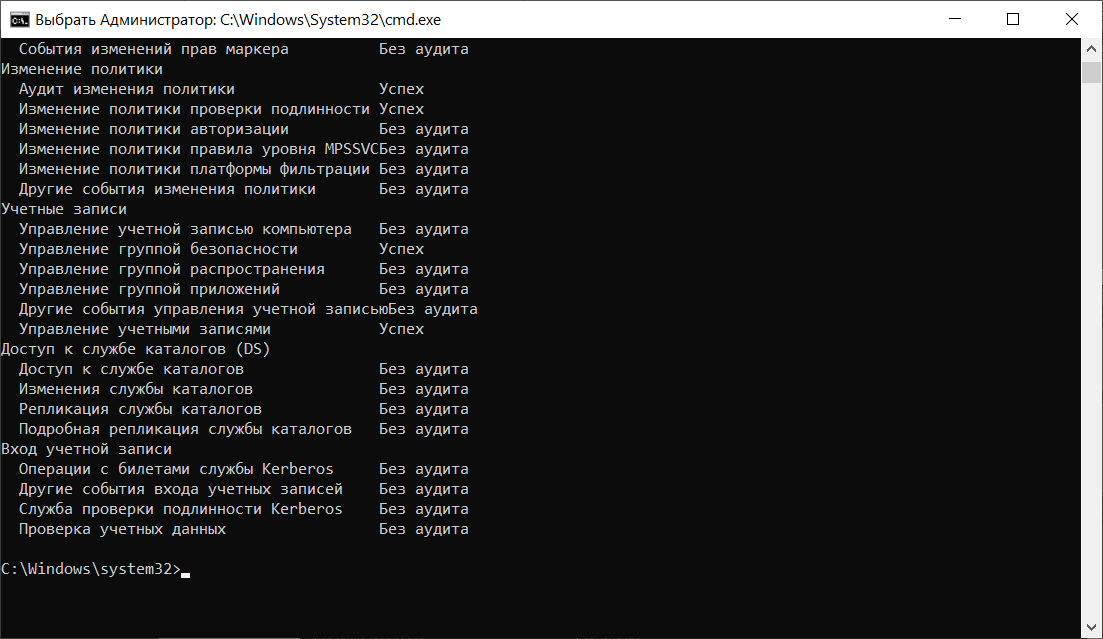


Рисунок 2.3 – Результат работы программы для проверки политики аудита (продолжение)

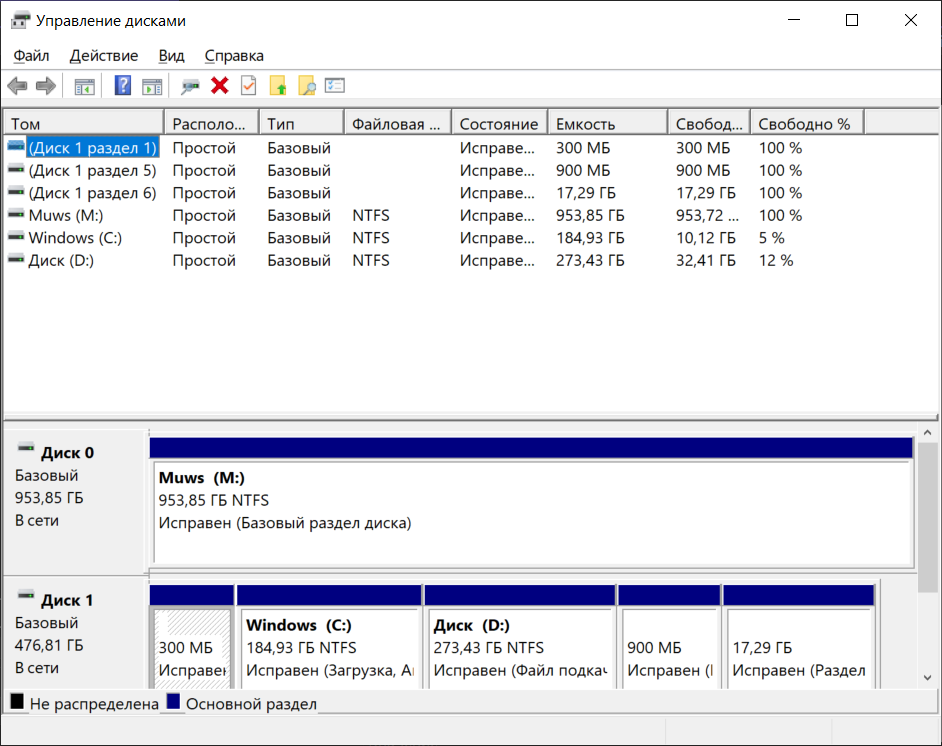


Рисунок 3.1 – Результат вызова метода анализа файловой системы

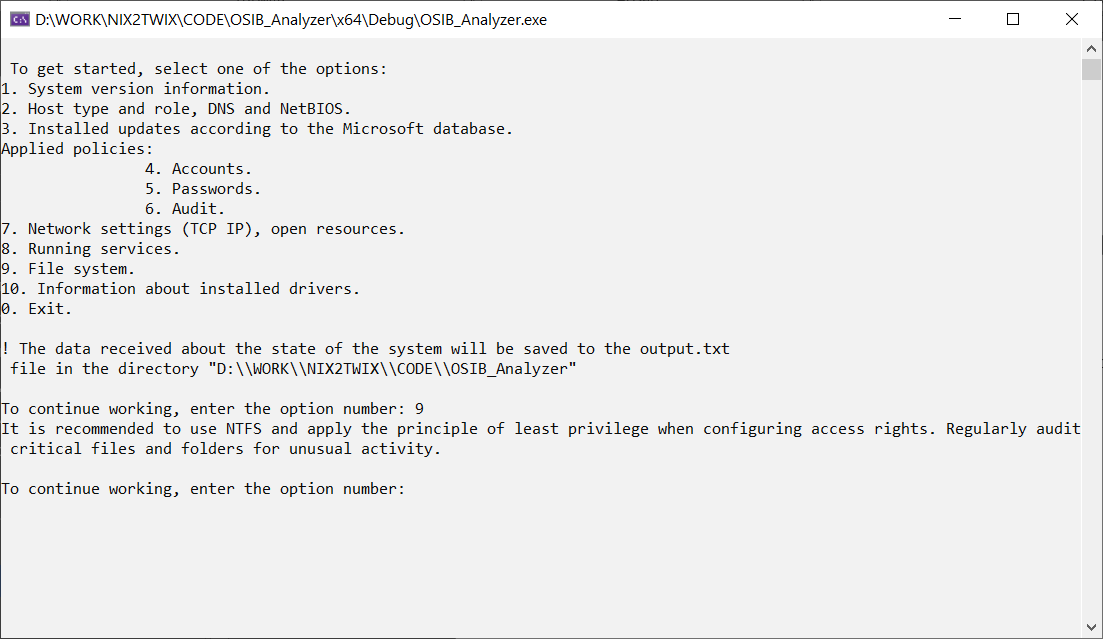
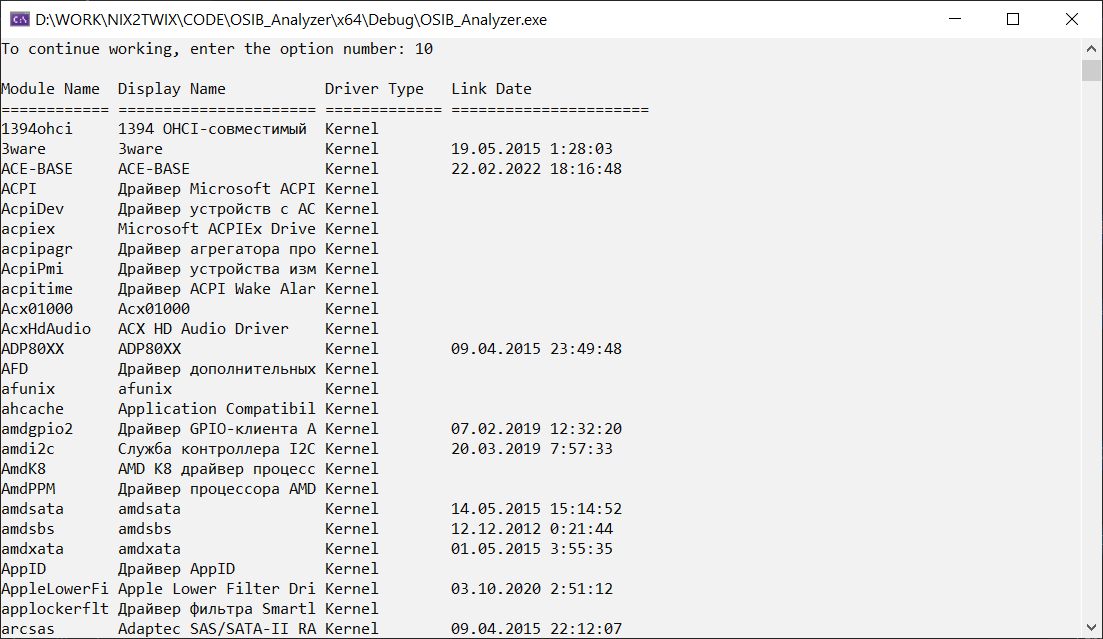


Рисунок 3.2 – Результат вызова метода анализа файловой системы (продолжение)

 Рисунок 4.1 – Результат вызова метода анализа драйверов

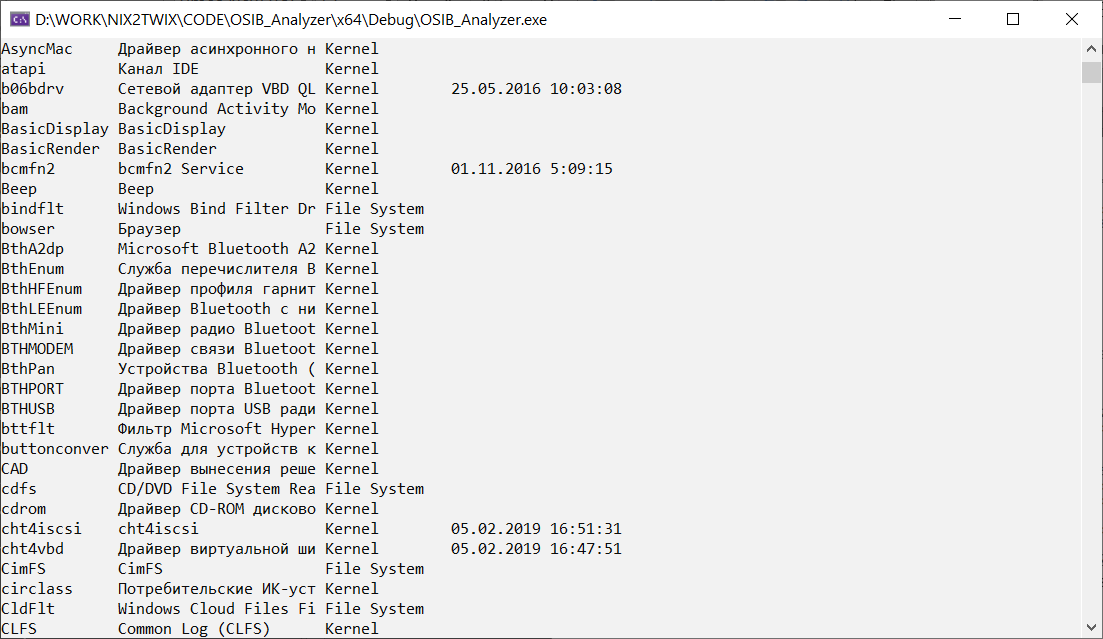
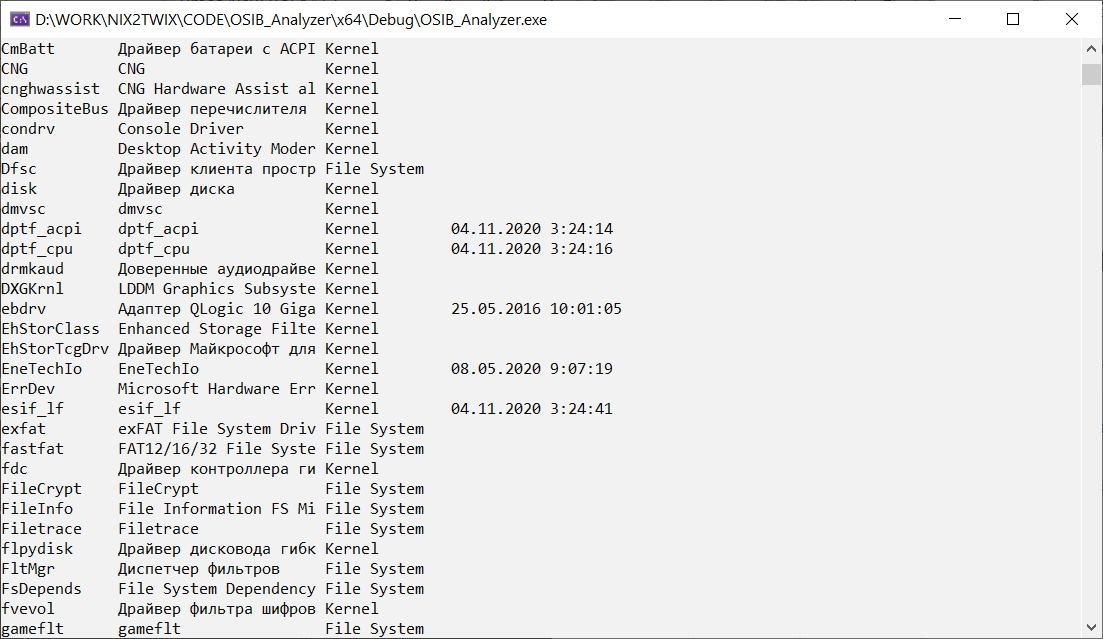


Рисунок 4.2 – Результат вызова метода анализа драйверов (продолжение)

 Рисунок 4.3 – Результат вызова метода анализа драйверов (продолжение)

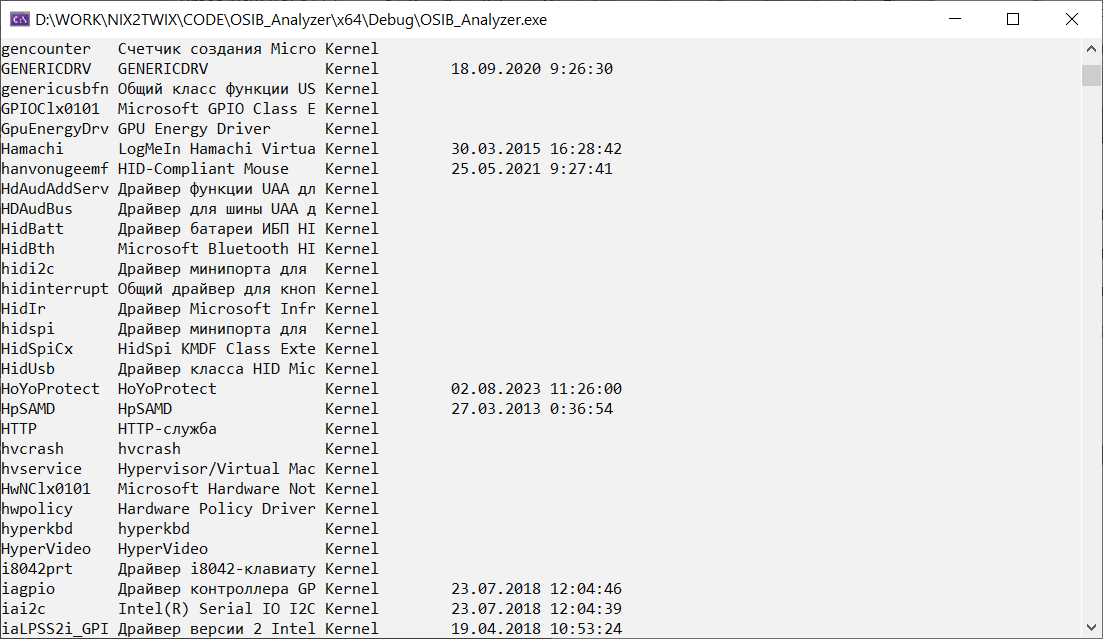


Рисунок 4.4 – Результат вызова метода анализа драйверов (продолжение)

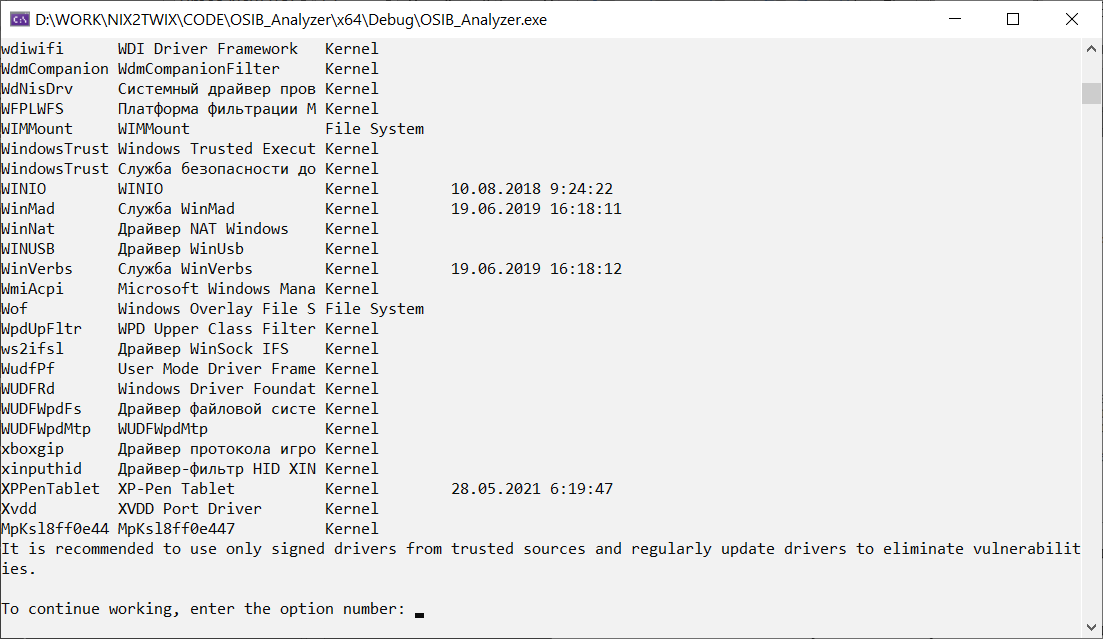


Рисунок 4.5 – Результат вызова метода анализа драйверов (продолжение)