ТИТУЛЬНИК

Лабораторная работа №1.

**Система управления доступом** – механизм, который определяет, к каким ресурсам компьютерной системы имеют доступ пользователи или процессы.

**Система регистрации и учета** – механизм, который записывает события, действия и операции, происходящие в операционной системе и приложениях.

**Система криптографии** – механизм, отвечающий за обеспечение безопасности путем шифрования данных.

**Система обеспечения целостности** – механизм, следящий за неизменностью и неповрежденностью файлов и данных в системе на протяжении всей ее работы.

|  |  |
| --- | --- |
|  | OS WINDOWS |
| Управление доступом | **Local Security Policy (secpol.msc)**  Сведения о локальной политике безопасности включают следующее:  - Домены, которым доверяет проверка подлинности попыток входа.  - Какие учетные записи пользователей могут получать доступ к системе и как. Например, в интерактивном режиме, через сеть или в качестве службы.  - Права и привилегии, назначенные учетным записям.  - Политика аудита безопасности.  **Group Policy (gpedit.msc)**  Групповая политика - это инструмент, доступный для администраторов, работающих с архитектурой Active Directory. Он позволяет централизованно управлять настройками на клиентских компьютерах и серверах, подключенных к домену, а также обеспечивает простой способ распространения программного обеспечения.  Групповые политики позволяют настраивать параметры для определенного набора пользователей или компьютеров внутри домена Active Directory. Также позволяют указать политики в одном месте для группы и применить к целевому набору пользователей.  **User Account Control**  Контроль учетных записей пользователей (UAC) является ключевой частью безопасности Windows. Контроль учетных записей снижает риск вредоносных программ, ограничивая возможность выполнения вредоносного кода с правами администратора. |
| Регистрация и учет | **Security Auditing**  Аудит безопасности — это методическая проверка и проверка действий, которые могут повлиять на безопасность системы. В операционных системах Windows аудит безопасности — это функции и службы, которые администратор может регистрировать и проверять события для указанных действий, связанных с безопасностью.  Сотни событий происходят по мере того, как операционная система Windows и запущенные в ней приложения выполняют свои задачи. Мониторинг этих событий может предоставить ценные сведения, помогающие администраторам устранять неполадки и исследовать действия, связанные с безопасностью.  **Event Viewer**  Просмотр событий — компонент, включённый в состав операционных систем семейства Windows NT, разрабатываемых Microsoft, который позволяет администраторам просматривать лог событий на локальном компьютере или на удалённой машине. |
| Криптография | **BitLocker**  BitLocker — это функция безопасности Windows, которая обеспечивает шифрование для целых томов, устраняя угрозы кражи или раскрытия данных с потерянных, украденных или неправильно списанных устройств.  **EFS**  EFS работает, шифруя каждый файл с помощью алгоритма симметричного шифрования, зависящего от версии операционной системы и настроек. При этом используется случайно сгенерированный ключ для каждого файла, называемый File Encryption Key (FEK).  FEK (случайный для каждого файла ключ симметричного шифрования) защищается путём асимметричного шифрования, использующего открытый ключ пользователя, шифрующего файл, и алгоритм RSA. Зашифрованный таким образом ключ FEK сохраняется в альтернативном потоке $EFS файловой системы NTFS. Для расшифрования данных драйвер шифрованной файловой системы прозрачно для пользователя расшифровывает FEK, используя закрытый ключ пользователя, а затем и необходимый файл с помощью расшифрованного файлового ключа.  Поскольку шифрование/расшифрование файлов происходит с помощью драйвера файловой системы (по сути, надстройки над NTFS), оно происходит прозрачно для пользователя и приложений. Стоит заметить, что EFS не шифрует файлы, передаваемые по сети, поэтому для защиты передаваемых данных необходимо использовать другие протоколы защиты данных (IPSec или WebDAV).  **IPSEC**  IPsec — это набор протоколов по защите информации в сети, который позволяет подтверждать подлинность участников сетевого обмена, контролировать конфиденциальность и целостность сетевых пакетов.  **Windows Certificate Manager**  Диспетчер сертификатов (Certmgr.exe) предназначен для управления сертификатами, списками доверия сертификатов (CTL) и списками отзыва сертификатов (CRL). |
| Обеспечение целостности | **Windows File Protection**  Защита файлов Windows (WFP) служит для предотвращения перезаписи программами важных файлов операционной системы. Такие файлы нельзя перезаписывать, поскольку они используются как самой операционной системой, так и другими программами. Защита таких файлов необходима для предупреждения возможных неполадок в работе операционной системы и установленного программного обеспечения.  Механизм WFP отвечает за защиту важных системных файлов, устанавливаемых вместе с Windows (например, файлы с расширениями dll, exe, ocx и sys, а также некоторые шрифты True Type). Проверка правильности версии защищенных системных файлов производится с помощью подписей файлов и файлов каталога, созданных в процессе подписывания.  **Windows Resource Protection**  Защита ресурсов Windows (WRP) предотвращает замену основных системных файлов, папок и разделов реестра, установленных в составе операционной системы.  Приложения не должны перезаписывать эти ресурсы, так как они используются системой и другими приложениями. Защита этих ресурсов предотвращает сбои приложений и операционной системы.  **System File Checker**  Проверка системных файлов — это утилита Microsoft Windows, позволяющая пользователю находить и восстанавливать повреждения системных файлов Windows. |

Лабораторная работа №2.

Основные системные процессы в Windows:

• svchost.exe – системный процесс, отвечающий за управление разными службами, служит своего рода контейнером для подпроцессов, использующих библиотеки DLL. В Диспетчере задач представлен несколькими экземплярами, большинство из которых являются критически важными для работы Windows. Располагается в папке System32, часто служит мишенью для вирусов.

• lsass.exe – важный системный процесс, отвечающий за авторизацию в системе. Если последняя прошла успешно, он инициирует запуск Проводника с помощью специального маркера. В отличие от svchost.exe, процесс lsass.exe всегда запускается с правами SYSTEM. Для работы системы критически важен. Располагается в папке System32, часто избирается мишенью для вредоносного ПО.

• explorer.exe – наиболее известный процесс, отвечающий за отображение графической оболочки Windows 10, позволяет осуществлять навигацию. Отключение не приведет к завершению работы системы, но сделает использование GUI невозможным. Запускается процесс из папки Windows, может иметь несколько экземпляров.

• sihost.exe – данный системный хост-процесс участвует в обслуживании инфраструктуры оболочки, позволяет открывать центр действий, различные меню, в том числе меню Пуск. Исполняемый файл запускается из папки System32.

• ntoskrnl.exe или system – базовый, критически важный процесс ядра операционной системы, отвечающий за работу множества системных функций и драйверов устройств. Завершение процесса System не предусмотрено, функционирование системы без него невозможно. Исполняемый файл располагается в папке System32.

• wininit.exe – этот процесс управляет автозагрузкой приложений в Windows, кроме того, он запускает ряд важных служб как SCM LSASS и LSM (диспетчер управления службами). Исполняемый файл располагается в папке System32. Случаи подмены вирусом не замечены.

• dwm.exe или диспетчер окон десктопа – процесс управляет визуальными эффектами важных элементов оболочки: десктопа, меню, окон и так далее. Запускается из каталога System32. Вероятность заражения невелика.

• smss.exe – управляет подсистемой менеджера сеансов Windows (сеансом авторизовавшегося юзера). Инициирует старт процессов Winlogon и Win32, участвует в установке переменных системы. Для Windows критически важен, файл лежит в директории System32, вероятность заражения оценивается как высокая.

• services.exe – важный процесс, отвечающий за управление системными службами. Запускается из директории System32, владельцем является Система. Работа процесса под другим пользователем будет указывать на вероятное заражение или подмену.

• winlogon.exe – отвечает за авторизацию (вход) конкретного юзера в систему и выход из нее. Запускается из папки System32, случаи заражения и подмены вирусом встречаются нечасто.

• csrss.exe – этот процесс управляет работой консольных приложений, например, командной строкой, является подсистемой компонента клиент-сервер. Исполняемый файл лежит в папке System32, вероятность заражения оценивается как высокая.

Теперь перейдем к системным процессам, обозначаемых в Диспетчере задач как фоновые.

• RuntimeBroker.exe – один из основных процессов ядра Windows 8.1 и 10, управляющий разрешениями универсальных приложений, к примеру, доступом к камере или микрофону. Каждому запущенному UWP-приложению соответствует свой экземпляр процесса RuntimeBroker. Исполняемый файл находится в каталоге System32.

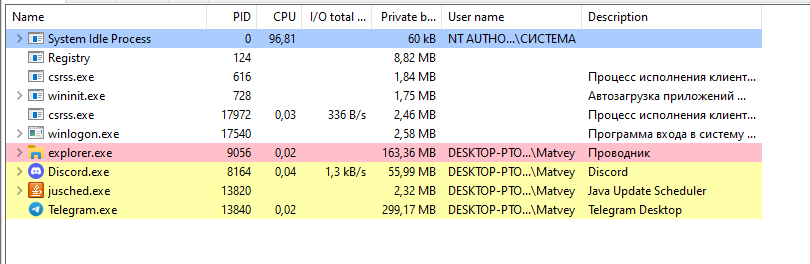
• ApplicationFrameHost.exe – еще один процесс, отвечающий за работу UWP-программ. В Windows 10 обеспечивает запуск универсальных приложений в окнах независимо от используемого режима. Процесс может быть закрыт принудительно, но при этом будут закрыты и все запущенные UWP-приложения, включая работающие в фоне. Обитает exe-файл процесса в System32.

• ctfmon.exe – процесс обеспечивает работу языковой панели, управляет вводом данных. Не является критическим, при завершении пользователем обычно перезапускается автоматически. Исполняемый файл лежит в System32, случаи использования вирусами редки.

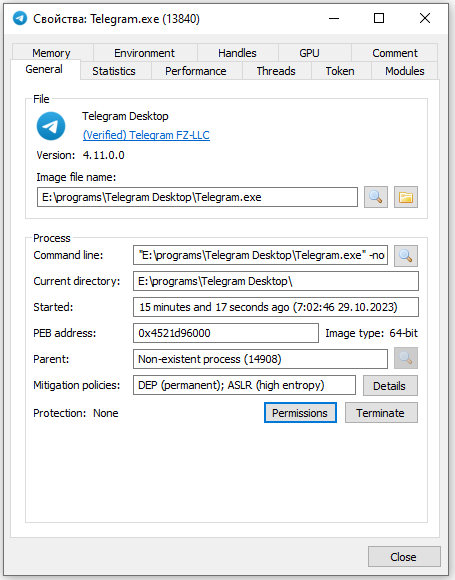
• SecurityHealthService.exe – системная служба, отвечающая в Windows 10 за работу Центра безопасности. Управляется Системой, завершение через Диспетчер задач не предусмотрено. Файл приложения находится в папке System32.

• spoolsv.exe – процесс, обеспечивающий вывод на печать с использованием принтера и других подобных устройств. Не является особо важным, может быть завершен из Диспетчера задач или отключен в службах. Файл находится в System32, заражение и использование вирусами маловероятно.

Разбор одного процесса:



Разберем процесс Telegram.exe



Во вкладке General написана основная информация о процессе:

Информация о файле:

* Версия
* Путь до исполняемого файла
* Название
* Сведения о цифоровой подписи

И информация о процессе:

* Command line – команда, при помощи которой был запущен файл

"E:\programs\Telegram Desktop\Telegram.exe" -noupdate

Указан путь до исполняемого файла и флаг -noupdate который отключает обновления программы после запуска

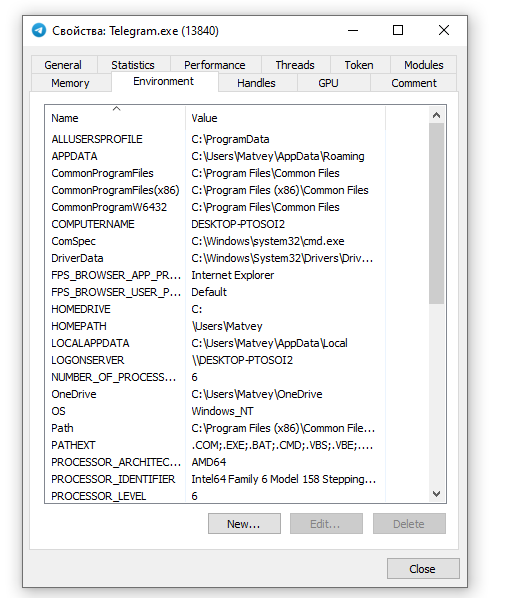
* Current directory - рабочий каталог, который ассоциирован с запущенным процессом. Это место в файловой системе, где процесс будет искать и сохранять файлы по умолчанию, если не указан полный путь.

E:\programs\Telegram Desktop\ - путь до директории, в которую были установлены файлы Telegram.

* Started – когда был запущен процесс.

15 minutes and 17 seconds ago (7:02:46 29.10.2023). первая часть – сколько времени назад был запущен процесс. В скобках указано точное время и дата запуска процесса

* PEB address: 0x4521d96000 – адресс в виртуальной памяти, где находятся данные об окружении и параметрах запуска процесса. Их можно посмотреть в вкладке Environment в Process Hacker



Parent – родительский процесс.

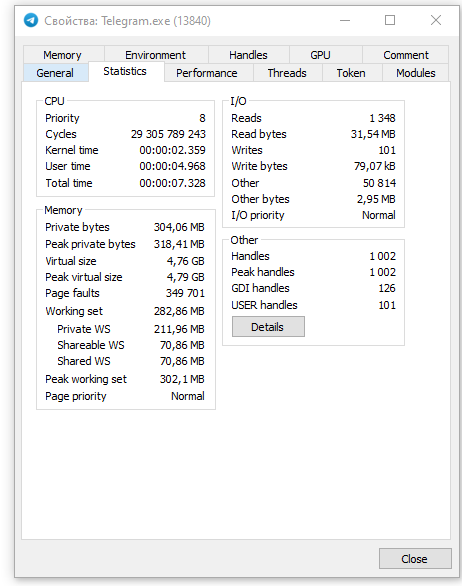
Non-existent process (14908) – это указывает нам на то, что родительский процесс, который запустил процесс Telegram.exe, прекратил свою работу. Его ID был 14908.

Mitigation polices – политики смягчения

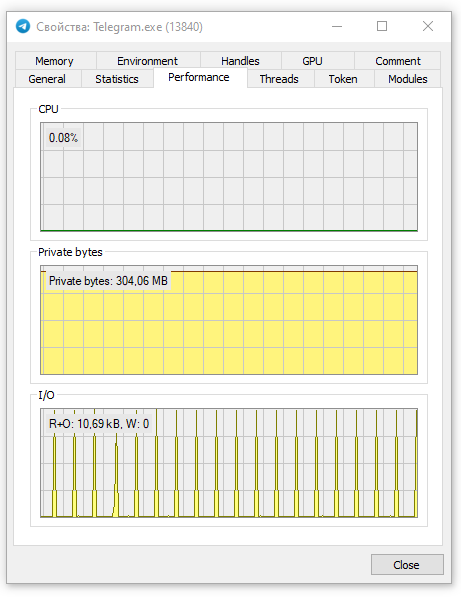
DEP (permanent) - "Data Execution Prevention" (предотвращение выполнения данных) – мера безопасности, которая запрещает исполнение кода из областей памяти, предназанченой только для хранения. (permanent) – указывает на то, что данная мера применяется ко всем процессам в опреационной системе

ASLR (high entropy) - "Address Space Layout Randomization", это мера, которая рандомизирует выделение виртуальных адресов внутри виртуальной памяти процесса, что усложняет поиск уязвимых участков памяти для атак. (high entropy) – указывает, что для рандомизации будут использованы случайные методы для определения адресов в виртуальной памяти

Во вкладке Statistics можно просмотреть данные о процессе: о работе процессора, памяти, вводы и вывода

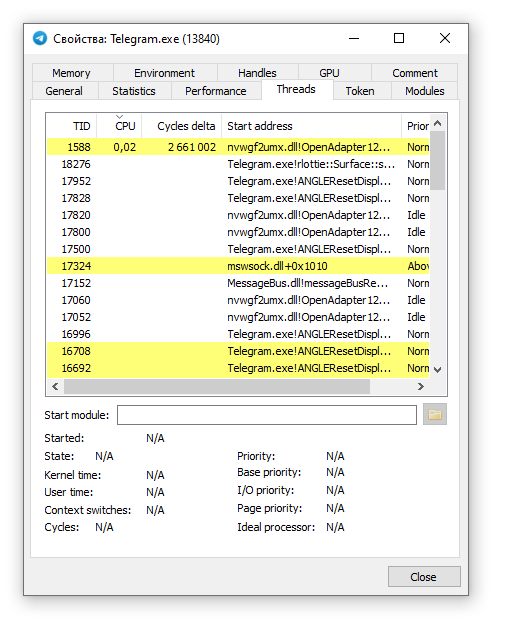


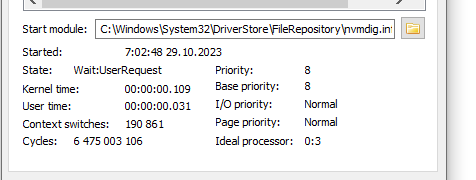
В performance можно изучить нагрузку, оказываемую процессом на ресурсы системы



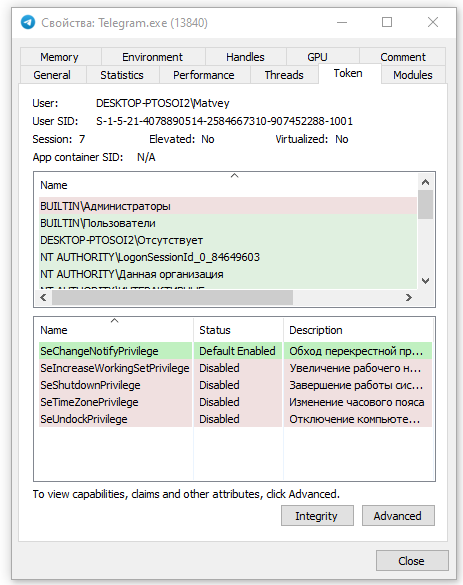
В threads можно узнать о потоках, связанных с этим процессом.

Потоки можно изучить поднобнее, в информации о потоке указан путь до исполняемого файла, время начала работы процесса, статус работы процесса, приоритет, информацию о работе с ресурсами процессора

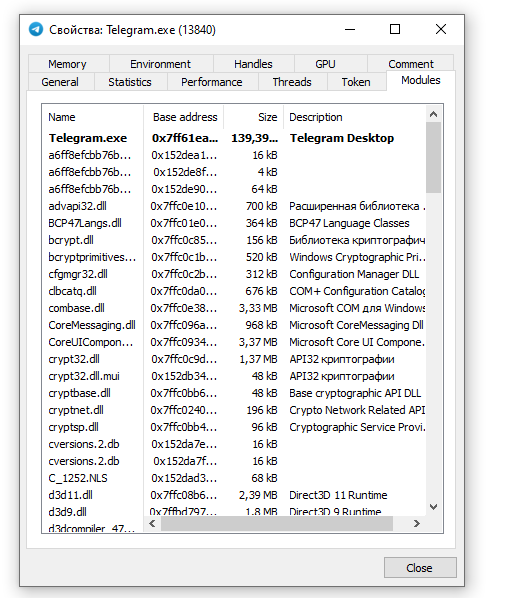




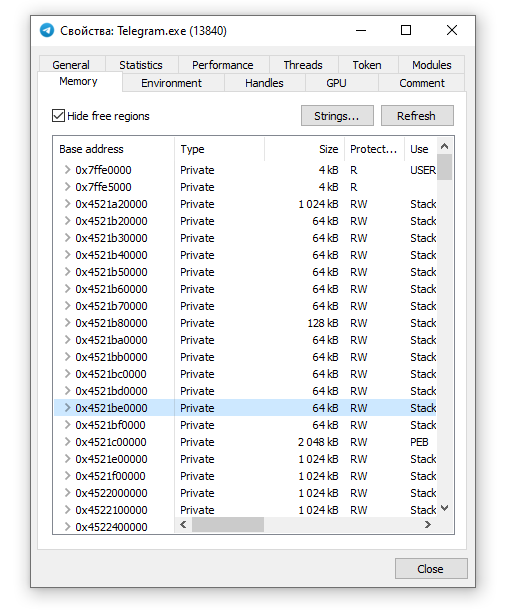
Во вкладке token указаны права процесса, и учетные записи, которые с ним ассоциированы



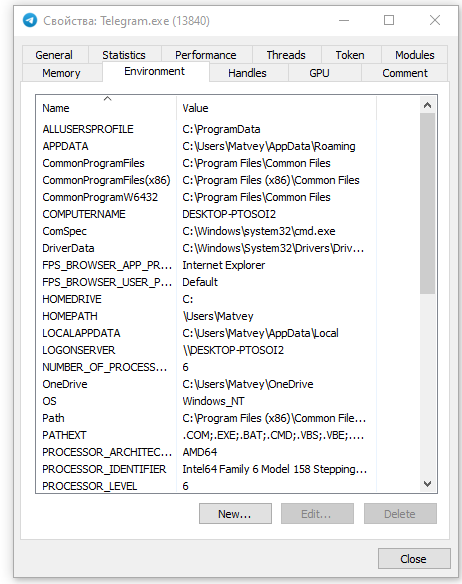
Во вкладке Modules указаны библиотеки, загруженные в процесс.



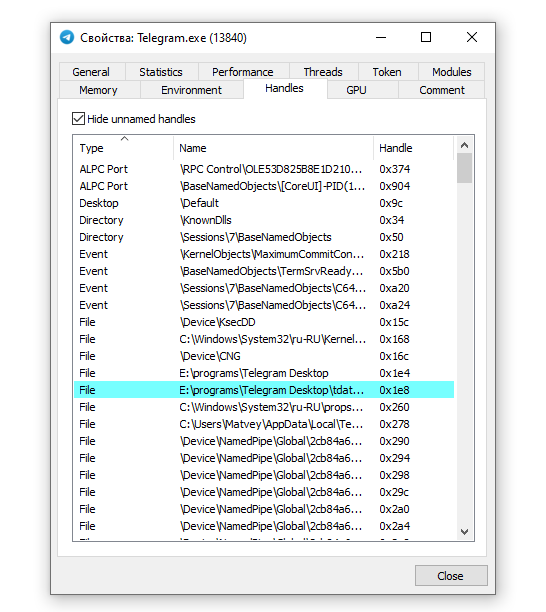
Во вкладке memory указано детальное распределение памяти



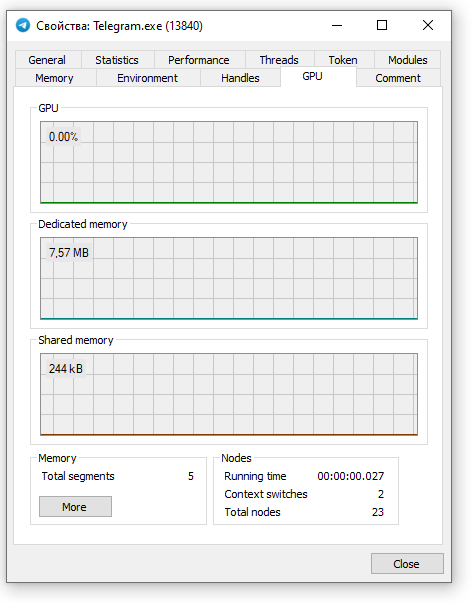
В Environment указаны параметры окружения и запуска процесса.



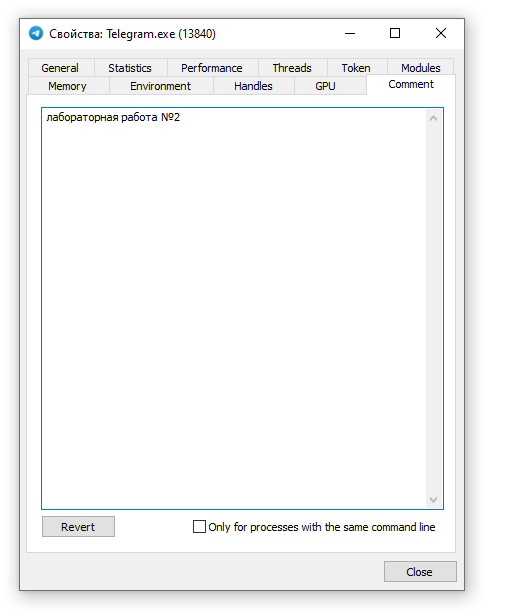
В handles указаны дескрипторы, которые ассоциированы с этим процессом.



Во вкладке GPU указана информация о затратах ресурсов графического процессора



И comment – в котором можно написать комментарий к процессу



Таким образом, Process hacker является мощной и удобной утилитой для мониторинга и управления ресурсами и процессами. При помощи него можно выявить вредоносное ПО и найти, где хранятся их исполняемые файлы.

Лабораторная работа №3.

| Название | Описание | Разработчик | Реестр | Название документов, требованиям которых соответствует |
| --- | --- | --- | --- | --- |
| Kaspersky OS | Микроядро написано с нуля и не использует код ядра ОС Linux. Ядро KasperskyOS содержит всего несколько десятков тысяч строк кода. А чем меньше размер ядра, тем меньше в нем потенциальных уязвимостей и тем проще провести его формальную верификацию. Для сравнения: монолитные ядра могут включать в себя десятки миллионов строк кода.  Кибериммунный подход «Лаборатории Касперского» позволяет создавать решения, которые практически невозможно скомпрометировать и в которых минимизировано число возможных уязвимостей. Разработка таких решений может стоить дешевле, чем аналогичные по уровню защищенности проекты с использованием операционных систем специального назначения более ранних поколений.  Операционная система KasperskyOS предоставляет необходимые интерфейсы, механизмы и инструменты для разработки кибериммунных решений, включая изоляцию доменов безопасности и контроль взаимодействий между ними. | АКЦИОНЕРНОЕ ОБЩЕСТВО "ЛАБОРАТОРИЯ КАСПЕРСКОГО" | Реестровая запись №5564 от 24.06.2019 | Запись в реестре ФСТЭК отсутствует |
| Astra Linux Special Edition | Cертифицированная ОС со встроенными средствами защиты информации (СЗИ) для стабильной и безопасной работы ИТ-инфраструктур любого масштаба и обработки информации различной степени конфиденциальности.  Успешно прошла комплекс испытаний в системе сертификации СЗИ ФСТЭК России по первому, высочайшему, уровню доверия. Единственная в стране имеет набор сертификатов регуляторов. | ООО «РусБИТех-Астра» | Реестровая запись №369 от 08.04.2016 | Соответствует требованиям документов: Требования доверия(1), Требования доверия(2), Требования к ОС, Профиль защиты ОС(А первого класса защиты. ИТ.ОС.А1.ПЗ), Профиль защиты ОС(А второго класса защиты. ИТ.ОС.А2.ПЗ), Требования к средствам контейнеризации(1), Требования к средствам виртуализации(1) |
| РЕД ОС | Российская операционная система общего назначения для серверов и рабочих станций. Соответствует требованиям Постановлений Правительства РФ №1236 от 16 ноября 2015 г. и №325 от 23 марта 2017 г.  РЕД ОС - составной программный продукт, построен на пакетной базе RPM-формата, соответствует требованиям POSIX и LSB 4.1 (Linux Standard Base).  При разработке РЕД ОС компания РЕД СОФТ опирается на опыт ведущих мировых сообществ Open Source и придерживается соглашений о наименовании и сборке пакетов.  РЕД ОС собирается из исходных кодов Open Source проектов и собственных разработок. Сборка пакетов выполняется по собственным спецификациям или спецификациям Open Source проектов. Все используемые спецификации адаптируются для обеспечения совместимости с пакетной базой РЕД ОС. | ООО «РЕД СОФТ» | Реестровая запись №3751 от 23.07.2017 | Соответствует требованиям документов: Требования доверия(4), Требования к ОС, Профиль защиты ОС(А четвертого класса защиты. ИТ.ОС.А4.ПЗ), Требования к средствам контейнеризации(4), Требования к средствам виртуализации(4) |
| ОС РОСА «КОБАЛЬТ» | Семейство операционных систем РОСА «КОБАЛЬТ» сертифицировано ФСТЭК России в клиентском и серверном вариантах. Рекомендуется для использования коммерческими структурами, промышленными предприятиями и органами государственной власти, работающими с конфиденциальной информацией, включая персональные данные.  Средства защиты информации ОС РОСА «КОБАЛЬТ» обеспечивают идентификацию и аутентификацию, управление доступом, регистрацию событий безопасности, ограничение программной среды, изоляцию процессов, защиту памяти, контроль целостности, надёжное функционирование и фильтрацию сетевого потока.  Существует также версия ОС под названием ROSA Enterprise Linux Desktop (RELD) 7.3 — почти полный функциональный аналог ОС РОСА «КОБАЛЬТ» для клиентских систем, отличающийся лишь отсутствием сертификата ФСТЭК России. ОС RELD 7.3 подходит для оснащения рабочих мест пользователей в корпоративной среде, где важна защита информации. Также в RELD дополнительно поддерживается окружение рабочего стола KDE. | АО «НПО Ангстрем» | Реестровая запись №1999 от 08.10.2016 | Соответствует требованиям документов: Требования доверия(4), Требования к ОС, Профиль защиты ОС(А четвертого класса защиты. ИТ.ОС.А4.ПЗ) |
| ICLinux | Защищенное компьютерное рабочее место терминального доступа.  Предпосылки возникновения решения обусловлены требованием российского законодательства обеспечить защиту персональных данных в соответствии с федеральным законом № 152-ФЗ «О персональных данных».  ПАК «ICLinux» представляет собой готовое, сертифицированное, защищенное «рабочее место», позволяющее обрабатывать информацию в соответствии с федеральным законом № 152-ФЗ «О персональных данных» и реализовывать системы обработки информации ограниченного доступа, не относящейся к государственной тайне.  ПАК «ICLinux» представляет собой тонкий клиент «ThinRAY» с установленной защищенной операционной системой «ICLinux». | АКЦИОНЕРНОЕ ОБЩЕСТВО "АЙСИЭЛ-КПО ВС" | Реестровая запись №1197 от 05.09.2016 | Запись в реестре ФСТЭК отсутствует |

Лабораторная работа №4.

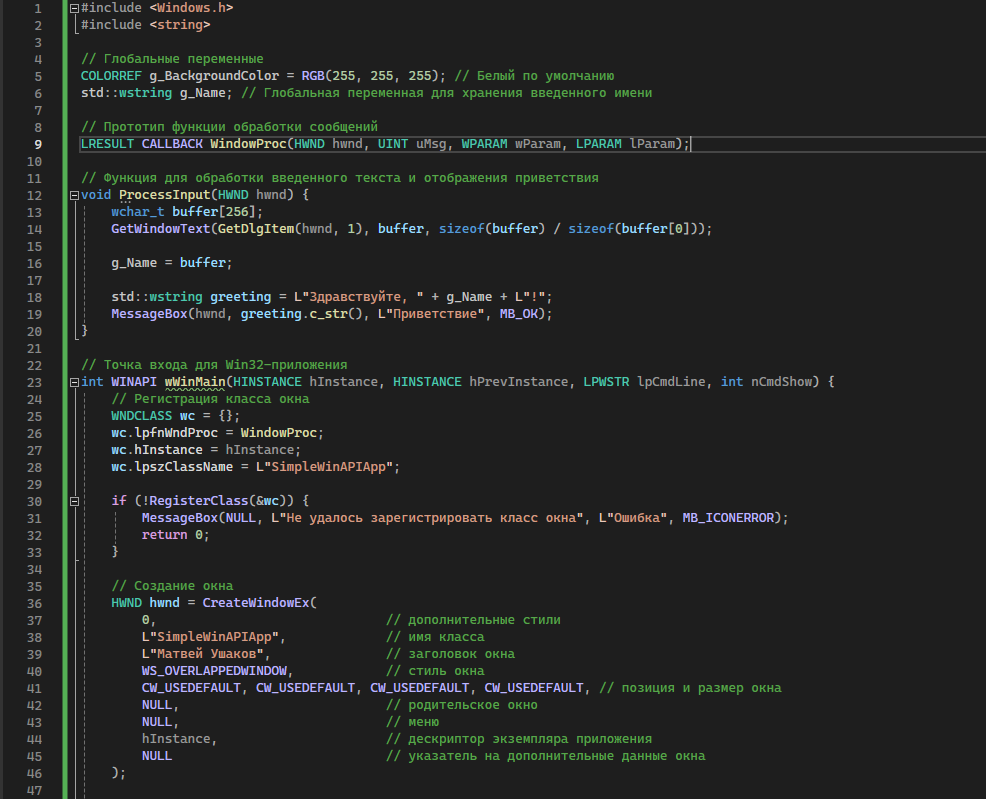
Для донастройки безопасности системы после установки требуется:

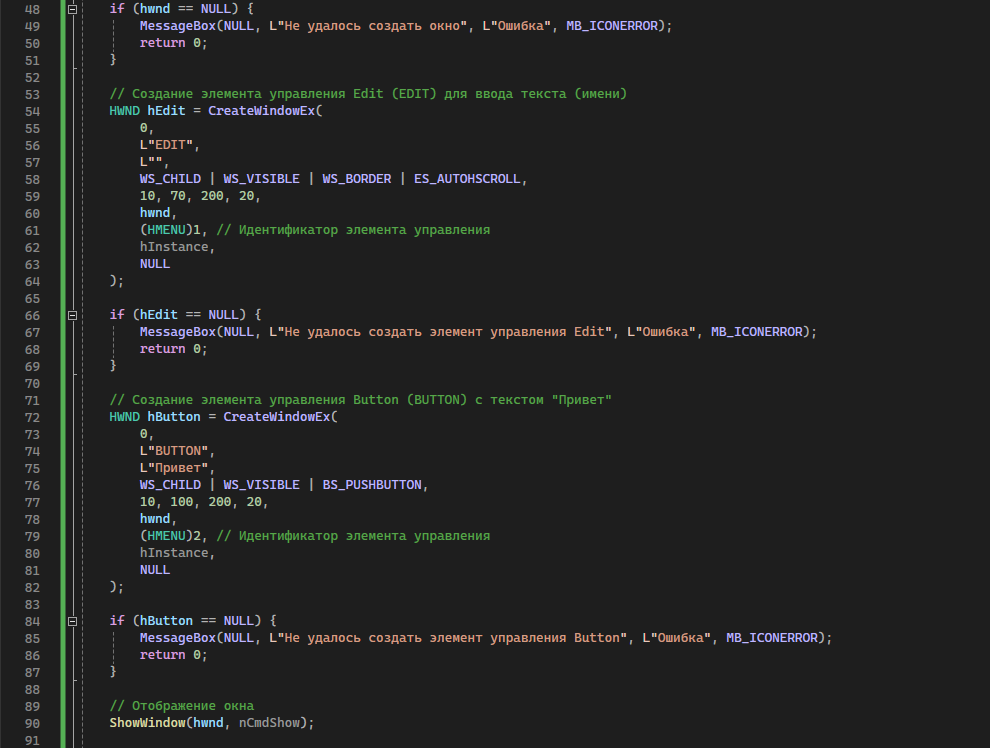
|  |  |
| --- | --- |
| Номер действия | Действие |
|  | **Обновление системы** |
| 1 | Установить последние обновления Windows |
| 2 | Включить уведомления о новых обновлениях системы |
|  | **Настройка пользователей** |
| 3 | Установить минимальную длину пароля |
| 4 | Установить требования к паролям |
| 5 | Отключить хранение паролей с использованием обратимого шифрования |
| 6 | Установить политику блокировки пользователя после нескольких неудачных вхождений |
|  | **Настройка прав пользователей** |
| 7 | Отключить возможность входа через интернет |
| 8 | Запретить использование функции работы в режиме операционной системы |
| 9 | Ограничить пользователям выполнение от имени администратора |
|  | **Настройки безопасности** |
| 10 | Установить текстовое предупреждение на экран блокировки |
| 11 | Запретить вход или ссоздание пользователей через аккаунты Mircrosoft |
| 12 | Отключить гостевой вход |
| 13 | Настроить лимит отсутствия активности компьютера |
| 14 | Настроить сетевой клиент на подписание всех коммуникаций |
| 15 | Запретить отправку незашифрованных паролей на сторонние сервера |
|  | **Настройка сетевых функций** |
| 16 | Запретить все действия для анонимных подключений к компьютеру |
| 17 | Включить firewall для всех профилей |
|  | **Настройки аудита** |
| 18 | Настроить политики аудита |
|  | **Настройки логирования** |
| 19 | Настроить длительность хранения логов и их размер |
|  | Дополнительные настройки |
| 20 | Отключить и удалить неиспользуемые сервисы и приложения |
| 21 | Удалить неиспользуемых пользователей |
| 22 | Настроить права досупа файловой системы |
| 23 | Установить системное время и дату |
| 24 | Установить антивирус |
| 25 | Устновить противошпионские программы |
| 26 | Настроить антивирус и противошпионские программы |
|  | **Физическая защита компьютера** |
| 27 | Установить пароль на BIOS |
| 28 | Запретить выключение комьютера без выхода из аккаунта |
| 29 | Настроить порядок загрузки в BIOS |

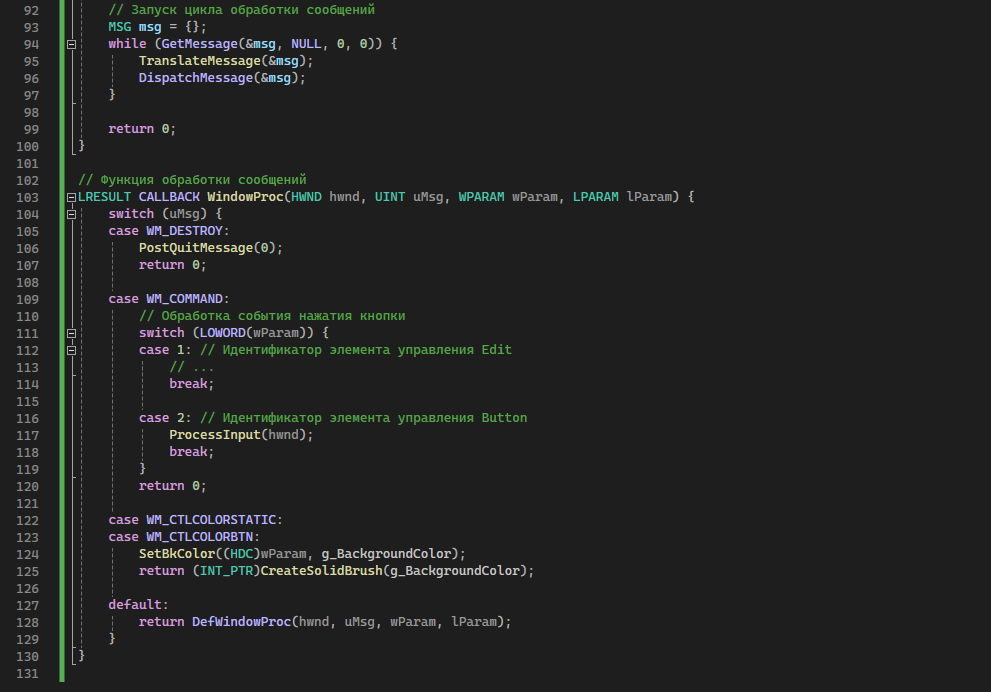
Лабораторная работа №5.

В IDE Microsoft Visual Studio создать простейшее однооконное WinAPI-приложение, РАЗОБРАТЬСЯ и описать его работу.

Программный код приложения:







Работа приложения:

