ЦЕЛЬ РАБОТЫ

Изучение основных механизмов обеспечения безопасности, встраиваемых в типовые ОС общего назначения, путем проведения частичного функционального тестирования выбранной ОС на соответствие требованиям безопасности.

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Функции безопасности операционных систем — это важный инструмент обеспечения безопасности ИТ-среды, так как они часто являются первым рубежом защиты. Определяя базовый набор функций безопасности в ОС, массово используемых на компьютерах пользователей, можно ориентироваться на профиль защиты с минимальными обоснованными требованиями, то есть на профиль А6.

В рамках выполнения лабораторной работы рассмотрим только функциональные компоненты в подсистеме безопасности ОС общего назначения, чтобы определить основные функции безопасности, которые должны быть в этих ОС.

Функции безопасности ОС профиля защиты А6 включают1:

1) идентификация и аутентификация;

2) управление доступом (на основе дискреционной модели);

3) регистрация событий безопасности;

4) ограничение программной среды;

5) изоляция процессов; защита памяти;

6) обеспечение надежного функционирования;

7) фильтрация сетевого потока.

Задачи работы состоят в том, чтобы познакомиться этими с функциями, реализующими основные требования безопасности в ОС. В качестве основы взят профиль защиты операционных систем общего назначения, самый низкий по требованиям в отечественной системе сертификации, которому должны соответствовать практически все массовые ОС.

Задание можно разделить на два уровня. В рамках базового уровня надо изучить функции 1)-4). Более сложные для исследования функции 5), 6), 7) на базовом уровне можно не рассматривать. Ниже перечислены функциональные требования безопасности (ФТБ) в ПЗ для ОС класса А6, детализирующие перечисленные выше функции. Можно опираться на эти требования, так как они написаны более конкретно, но если это сложно, то достаточно ориентироваться на обобщенный список, приведенный выше:

−возможность задания политики дискреционного и ролевого управления доступом для установленного множества операций, выполняемых субъектами доступа по отношению к объектам доступа;

−возможность реализации дискреционного и ролевого управления доступом на основе списков управления доступом (матрицы управления доступом) и (или) ролей;

−возможность осуществления резервного копирования объектов файловой системы; −возможность удаления объектов файловой системы;

−возможность восстановления объектов ОС из резервных копий, созданных с использованием ОС, и использования ассоциированных с ними атрибутов безопасности;

−возможность установки ПО (компонентов ПО) только администраторами;

−возможность задания правил автозапуска компонентов ПО при загрузке ОС;

−контроль запуска компонентов ПО и реагирование на попытки запуска компонентов ПО, произведенные в нарушение установленных правил запуска компонентов ПО;

−возможность осуществлять фильтрацию входящих и (или) исходящих сетевых потоков; −возможность осуществлять фильтрацию сетевых потоков, основанную на атрибутах безопасности субъектов доступа (сетевой адрес узла отправителя, сетевой адрес узла получателя) и информации (сетевой протокол, который используется для взаимодействия);

−возможность явно разрешать сетевой поток, базируясь на устанавливаемом администратором наборе правил фильтрации сетевого трафика, основанном на идентифицированных атрибутах;

1 Профиль защиты операционных систем типа А шестого класса защиты. ИТ.ОС.А6.ПЗ : Методический документ. (утв. ФСТЭК России 08.02.2017 г.)

−возможность запрещать сетевой поток, базируясь на устанавливаемом администратором наборе правил фильтрации сетевого трафика, основанном на идентифицированных атрибутах; −возможность поддерживать для каждого пользователя ОС список атрибутов безопасности; −возможность блокирования учетной записи пользователя ОС при превышении установленного администратором числа неуспешных попыток аутентификации;

−обеспечение идентификации объектов доступа;

−идентификация и аутентификация пользователя до выполнения основных действий по доступу в информационную систему или администратора до выполнения действий по управлению ОС; −исключение отображения действительного значения аутентификационной информации при ее вводе пользователем ОС в диалоговом интерфейсе;

−возможность ассоциировать атрибуты безопасности пользователя ОС с субъектами доступа (запускаемыми от его имени процессами);

−возможность проверки соответствия аутентификационной информации метрике качества, обеспечивающей адекватную защиту от нарушения безопасности нарушителем с потенциалом нападения, соответствующим классу защищенности;

−возможность со стороны администратора управлять атрибутами безопасности; −возможность со стороны администратора управлять выполнением функций безопасности ОС; −возможность со стороны администратора управлять параметрами функций безопасности ОС, данными аудита, правилами фильтрации сетевого потока;

−поддержка определенных ролей для ОС и их ассоциации с пользователями ОС; −обеспечение управления доступом к объектам ОС;

−защита хранимой аутентификационной информации от неправомерного доступа к ней и раскрытия;

−обеспечение защиты от переполнения буфера;

−постоянный контроль и проверка правомочности обращений субъектов доступа к объектам доступа;

−возможность предоставления надежных меток времени при проведении аудита, а также для ограничения срока действий атрибутов безопасности;

−возможность осуществлять ограничение максимального числа одновременных (параллельных) интерактивных сеансов доступа в операционную систему, предоставленных одному и тому же субъекту доступа;

−возможность осуществлять блокирование сеанса доступа пользователя ОС по истечении заданного интервала времени бездействия;

−возможность осуществлять блокирование (разблокирование) собственного сеанса доступа в ОС пользователем ОС;

−возможность обеспечения защиты от несогласованностей записей аудита;

−возможность выполнения действий, направленных на сохранение данных журнала регистрации событий безопасности ОС и обеспечивающих непрерывность процесса аудита, если журнал регистрации событий безопасности ОС превысит определенный администратором размер;

−возможность регистрации (аудита) событий безопасности, которые в соответствии с ГОСТ Р ИСО/МЭК 15408-2 включены в минимальный уровень аудита.

ВЫБОР ОС ДЛЯ ИССЛЕДОВАНИЯ И СЦЕНАРИЯ РАБОТЫ

Для исследования можно выбрать любую ОС на базе Microsoft Windows не ниже Windows 7. Наиболее удобно рассматривать функции в дружественном интерфейсе ОС Windows 10.

Приведенное ниже описание основ настройки и администрирования Windows 10 помогут в изучении функций безопасности.

ОСНОВЫ АДМИНИСТРИРОВАНИЯ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В WINDOWS 10. Windows 10 была создана для интеграции и использования в средах, которые должны отвечать требованиям высокого уровня безопасности, вплоть до профилей правительственных систем, в силу чего обладает развитой подсистемой безопасности. Это очень гибкая система, и ее многие опции позволяют настроить ее для использования всех её функций (минимальная безопасность), или использования только базовых возможностей, и тех операций, которые настроены пользователем (максимальный уровень безопасности).

Определённый уровень гибкости нужен и при использовании настроек безопасности. Это позволяет соответствовать целям и требованиям корпоративных политик или потребностям пользователя, поддерживая при этом достаточный уровень безопасности. Примером является инструмент управления пользовательскими учетными записями (User Account Control – UAC), который при правильной настройке может обеспечивать высокий уровень безопасности или может быть совсем отключен.

Инструмент UAC используется для того, чтобы не позволять программам или приложениям вносить изменения в ОС. Он работает посредством ограничения доступа в ядре ОС, и затем предоставляет подробную информацию пользователям о той программе, которая пыталась себя установить или внести изменения в ОС.

Установка и настройка безопасности Windows 10

Во время установки ОС всегда рекомендуется выполнять свежую установку ОС на недавно приобретённое (или обновлённое) совместимое аппаратное оборудование и затем производить настройку её средств безопасности. Укрепление системы представляет собой процесс повышения уровня безопасности на только что установленной базовой операционной системе путём настройки необходимых параметров безопасности, удаления ненужного ПО и настройки дополнительных параметров политики.

После корректной установки ОС и её базовой настройки происходит процесс настройки компонентов безопасности.

Конфигурирование средств безопасности ОС состоит из нескольких этапов, которые опционально могут быть расширены. Ниже приведены некоторые этапы настройки. Шаг 1. Установка базовой ОС с выбором необходимых опций для повышения безопасности во время установки и отключением ненужных сервисов, опций и программ.

Шаг 2. Установка всех рабочих комплектов администратора, инструментов безопасности и необходимых программ.

Шаг 3. Удаление ненужных сервисов, программ и приложений. Отключение или удаление неиспользуемых учётных записей пользователей и групп.

Шаг 4. Установка Service Pack, исправлений и обновлений. Обновление всех установленных программ.

Шаг 5. Запуск аудита безопасности (сканер, шаблоны, MBSA, и т.д.) для получения информации о текущем уровне безопасности.

Шаг 6. Запуск восстановления системы (System Restore) и создание точки восстановления. Приложения резервного копирования и восстановления для восстановления после крушений системы. Шаг 7. Резервное копирование системы с возможностью её быстрого восстановления после краха.

В центре действий ОС Windows (Action Center), доступны различные инструменты и можно указывать действия, которые ОС будет выполнять, в том числе связанные с безопасностью. Для входа в данный компонент нужно в правой нижней части экрана выбрать значок центра действий .

Опции интернета (Internet Options) – веб просмотр В приложении опций интернета в панели управления (Internet Options Control Panel) можно указывать зоны безопасности, разрешать доступ только к определённым URL адресам, разворачивать расширенные параметры безопасности в закладке «Дополнительно» (Advanced) и многое другое. Сам браузер оснащён фильтром фишинга, который предотвращает атаки фишинга (Phishing), а также имеет другие настраиваемые опции, такие как InPrivate Browsing, которая не позволяет хранить нашу личную информацию, что особенно полезно при использовании компьютера в публичных интернет-кафе.

Брандмауэр Windows Firewall, как и любой другой программный или аппаратный межсетевой экран, может предотвращать базовые атаки по умолчанию, и его можно настраивать многогранно для высокого уровня контроля над тем, что может входить и исходить с рассматриваемого компьютера, когда он подключен к публичной или частной сети. Перейдя в панель управления и выбрав брандмауэр Windows, можно получить доступ к большинству параметров конфигурации брандмауэра. Если на нажать на кнопку дополнительных параметров (Advanced) в диалоге для доступа к дополнительным параметрам и опциям конфигурации. В Windows 10 пользователь может разворачивать несколько политик брандмауэра одновременно и использовать обозначение домена (Domain designation) для более простой настройки и управления брандмауэром Windows.

Персонализация (Personalization) – опции персонализации представляют собой то место, где можно изменять внешний вид Windows, но здесь же пользователь может настраивать пароли своей экранной заставки. Если Windows 10 используется на предприятии, пользователей необходимо научить тому, как блокировать свои рабочие станции всякий раз, когда они покидают свое рабочее место, или создать параметры политики, которые бы делали это автоматически после определенного периода бездействия системы; экранная заставка, если настроить ее на запрос повторного входа после такого периода, может быть очень полезной. Это также полезно и для домашнего компьютера во избежание случайных действий, если пользователь ушел, не выключил его.

Обновления Windows Update – все версии программного обеспечения требуют определённый уровень исправлений. Обновления и новые выпуски программ требуются для улучшения их основной функциональности. Часто они выпускаются для устранения выявленных уязвимостей, которые могут быть высоко критичными.

Windows (и Microsoft) Update или производственные версии управления исправлениями (например, WSUS) используются для централизованного управления и установки обновлений. Эти инструменты используются для контроля, отслеживания и мониторинга наших текущих и будущих потребностей в обновлениях. Можно настроить автоматическое обновление, или делать это вручную по мере необходимости. Если система долго не обновляется, риск атак растет.

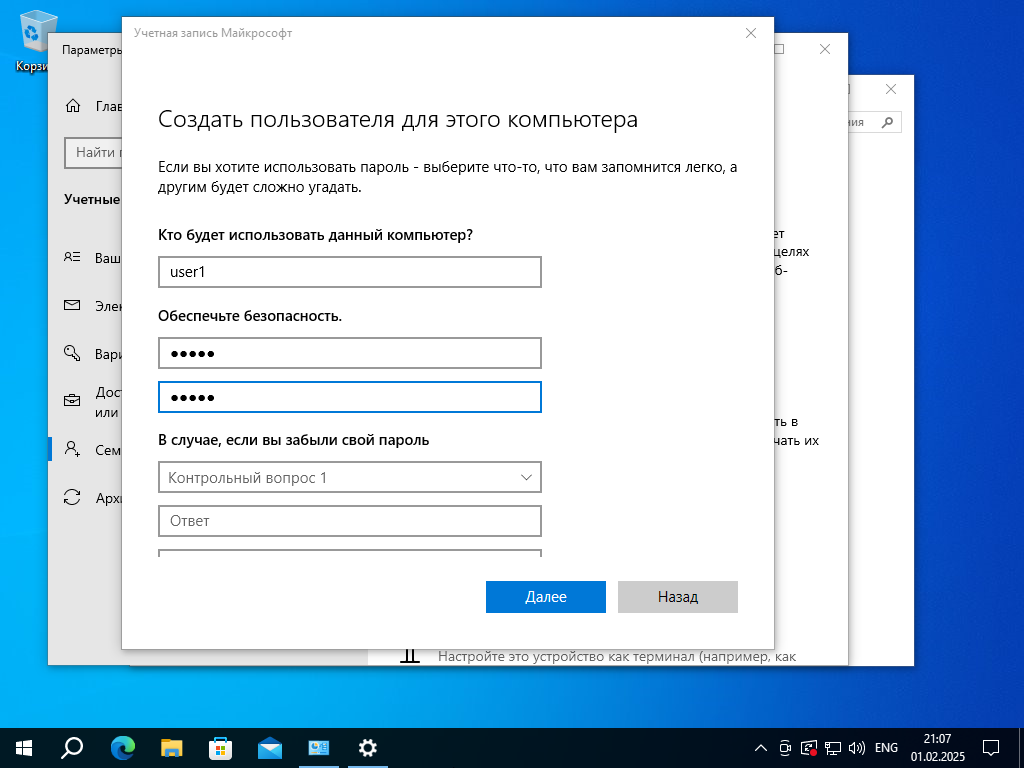
Программы и функции (Programs and Features) – помимо обновлений Windows Updates необходимо проверять, что установлено в системе, особенно если пользователь часто работает в интернете и/или загружает программные продукты с интернет серверов.

Windows Defender - встроенная утилита ОС Windows 10 (в более ранних версиях приложение "Безопасность Windows" называлось "Центр безопасности Защитника Windows"). Антивирусная программа Defender автоматически отключается при установке и включении другого антивирусного приложения. При удалении другого приложения антивирусная программа в Microsoft Defender включится автоматически. Позволяет выполнять проверку файлов на предмет вредоносного ПО, планировать полное сканирование компьютера, а также обеспечивать защиту компьютера в режиме реального времени.

Пользовательские учётные записи (User Accounts) - управление учётными записями пользователей является основой защиты доступа к конкретному компьютеру, а также ко всему, что работает под его управлением. Например, если создаётся новая учётная запись пользователя и включается в группу администраторов, то у работающего под этой учётной записью пользователя будет полный доступ к системе компьютера. Если настроить учётную запись в качестве обычного пользователя, то её разрешения будут очень ограниченными и позволят выполнять лишь ряд базовых функций пользователя. В Windows предусмотрена гибкая настройка парольных политик, которые заставляют пользователей создавать сложные для взлома пароли, что предотвращает большинство базовых атак.

Опции питания (Power Options) – приложение Power Options Control Panel является тем местом, где мы настраиваем стандартное поведение операционной системы, когда она отключена, закрыта или находится в спящем режиме. Для большей степени безопасности рекомендуется устанавливать параметр на запрос пароля при выходе машины из спящего режима. Всякий раз, когда появляется возможность включения контроля доступа пользователей, следует её использовать.

1. Создаём двух новых пользователей в системе:

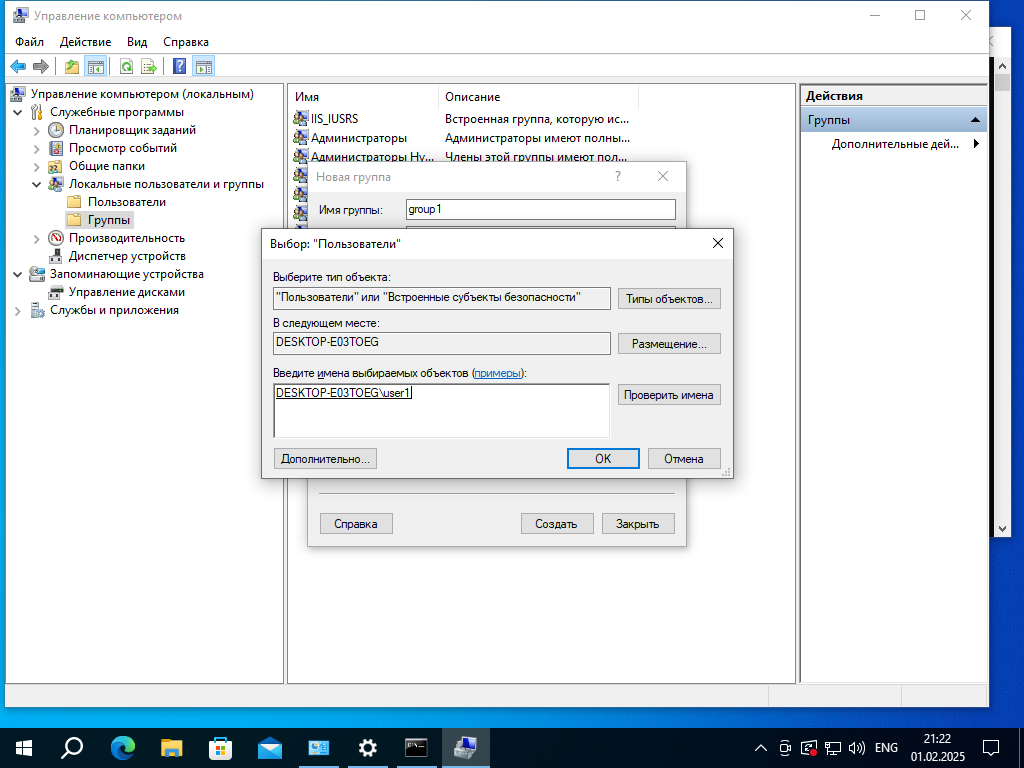


Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

2. Создаём две группы безопасности, включаем каждого пользователя в свою группу:

Первая группа:



Вторая группа:

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

3. Создаём 4 каталога со следующими правами:

- каталог1 - только чтение для пользователя1, чтение, создание и изменение файлов для пользователя2:

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

- каталог2 - нет доступа для пользователя1, только чтение для пользователя2:

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

- каталог3: только чтение для группы1, только чтение для группы2:

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

- каталог4 - полный доступ для группы1, создание и изменение файлов для группы2:

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

4. Создаём шаблон безопасности системы, указав параметры (secpol.msc):

- политики учетных записей>Политики паролей>Вести журнал паролей [1 сохраненный пароль];

- политики учетных записей>Политики паролей>Минимальная длина пароля [7 знаков];

- политики учетных записей>Политики паролей>Пароль должен отвечать требованиям сложности [Включен];

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

- политики учетных записей>Политики блокировки учетной записи>Пороговое значение блокировки [3 ошибок входа в систему];

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

- локальные политики>Политики аудита>Аудит входа в систему [Успех, Отказ];

- локальные политики>Политики аудита>Аудит доступа к объектам [Успех, Отказ];

- локальные политики>Политики аудита>Аудит событий входа в систему [Успех, Отказ];

- локальные политики>Политики аудита>Аудит управления учетными записями [Успех, Отказ];

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

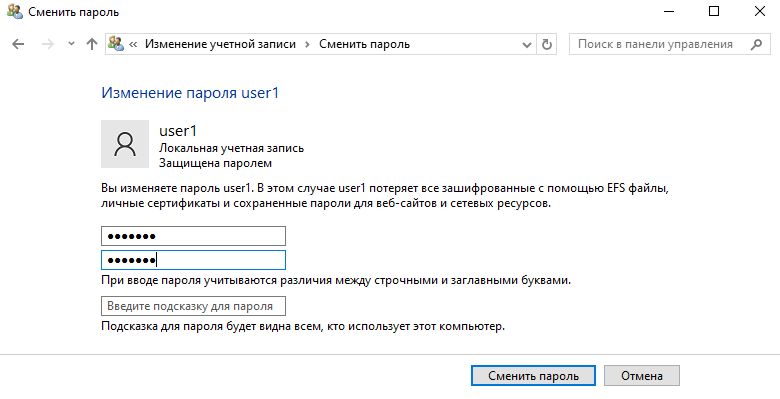
Посмотреть события безопасности можно с помощью “просмотра событий” (eventvwr.msc):

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

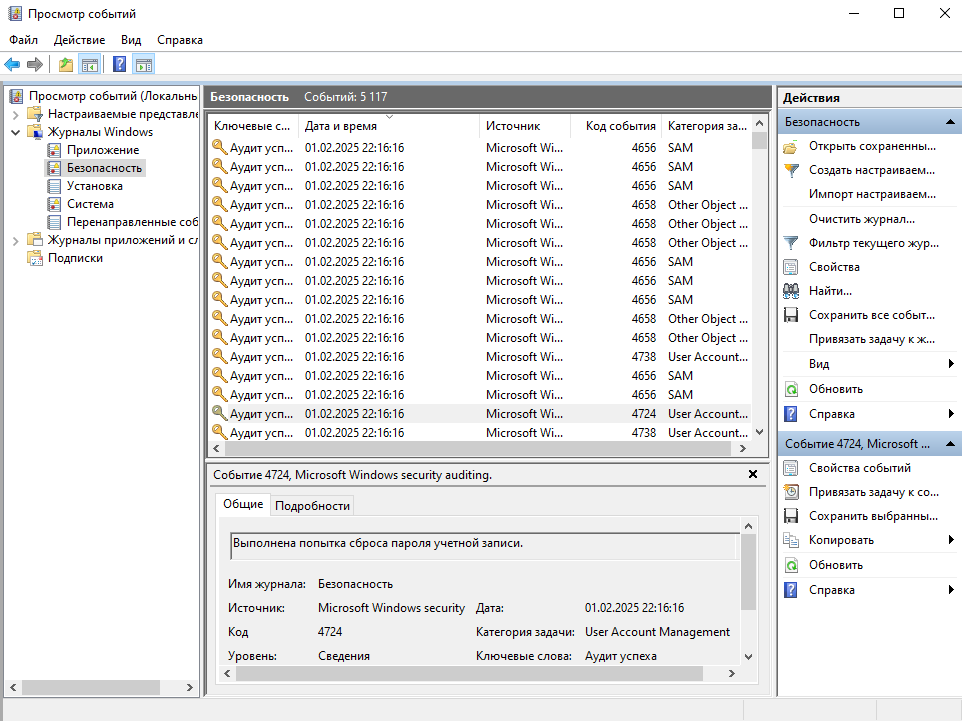
Автоматически созданное описание

5. Работа с журналом безопасности и параметрами безопасности:

- изменяем пароль пользователя в соответствии с требованиями сложности локальной политики безопасности:



Находим связанное с этим событие в журнале безопасности операционной системы:

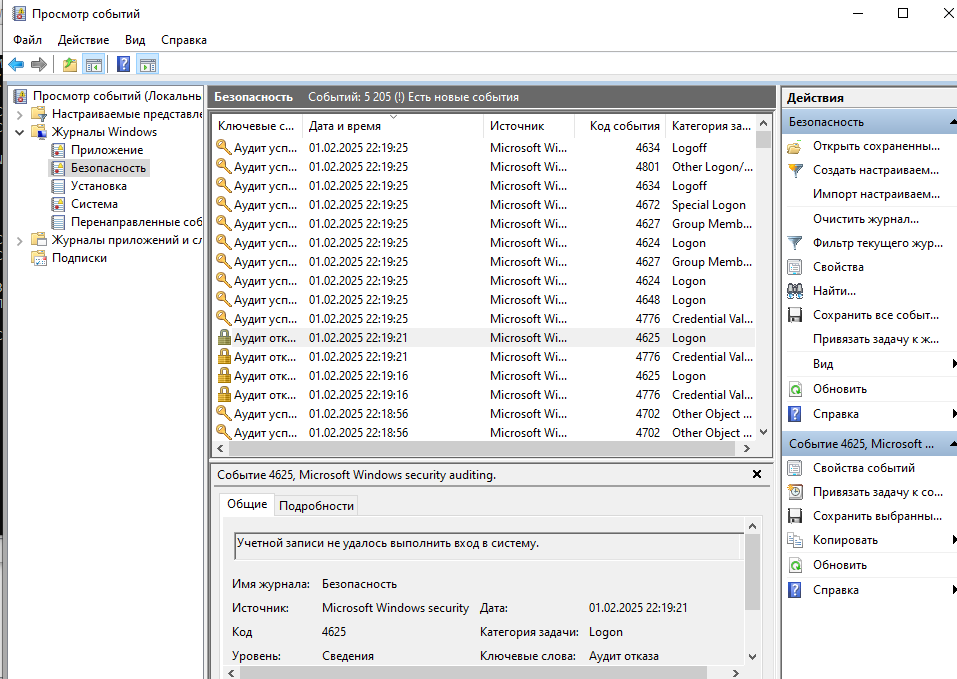


- производим вход в систему под учетной записью пользователя user2 с ошибочными данными (неправильным паролем):

Изображение выглядит как небо, снимок экрана, часы, на открытом воздухе

Автоматически созданное описание

Находим связанное с этим событие в журнале безопасности операционной системы:



Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

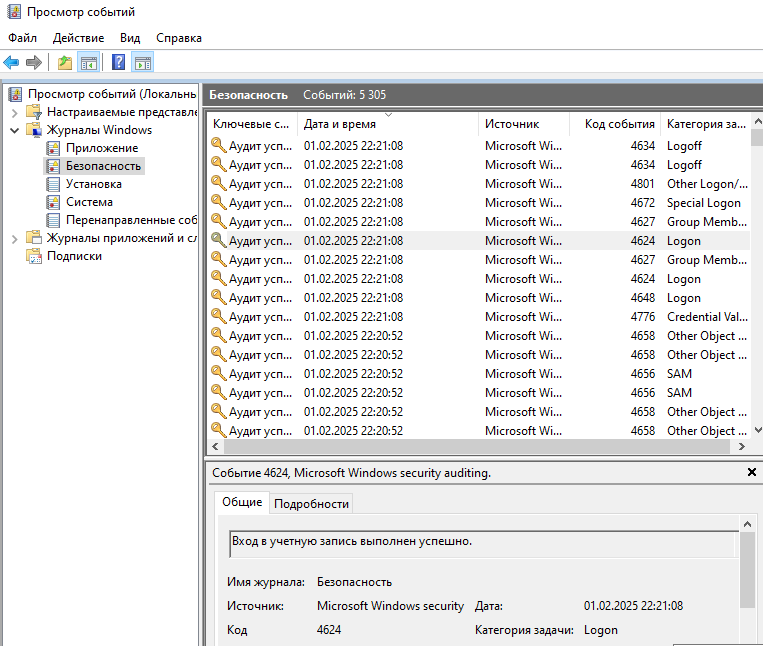
Автоматически созданное описание

- производим вход в систему под учетной записью пользователя admin верными данными:

Изображение выглядит как текст, облако, вода, снимок экрана

Автоматически созданное описание

Находим связанное с этим событие в журнале безопасности ОС:

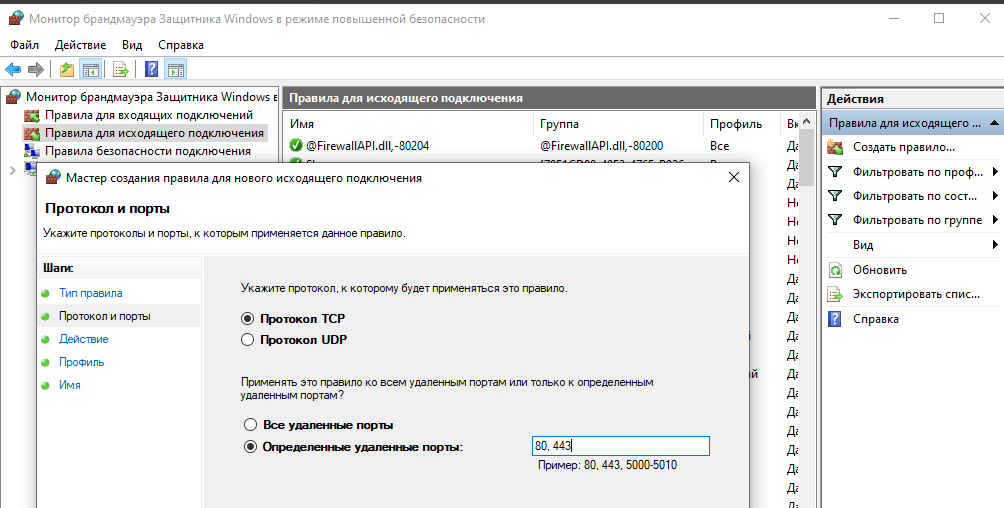


Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

8. Настраиваем следующие правила в брандмауэре Windows:

- запрет исходящего трафика для подключения к сайтам:



До создания правила:

Изображение выглядит как текст, электроника, компьютер, снимок экрана

Автоматически созданное описание

После создания правила:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

- (html-страницам); запрет входящего трафика для удалённого подключения к рабочей станции по протоколу RDP (утилита mstsc):

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Автоматически созданное описание

9. Настраиваем параметры управления учетными записями пользователей на уведомление при любом изменении параметров Windows пользователями:

- параметры управления учетными записями находятся в: Панель управления > Учетные записи пользователей> Изменение параметров контроля учетных записей:

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

проверяем правильность настройки, открыв диалог «управление компьютером» из контекстного меню «моего компьютера»:

Изображение выглядит как текст, снимок экрана, на открытом воздухе, гора

Автоматически созданное описание

10. С помощью инструмента «Архивация и восстановление» выполнить архивацию (резервное копирование) каталога с файлами:

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание