**1.**

1) Прогнозирование, своевременное выявление и устранение угроз безопасности.

2) BitLocker, Windows Defender, Windows Firewall, User Account Control, резервное копирование и восстановление, родительский контроль.

3) В Microsoft Defender входит ряд модулей безопасности, таких как: изоляция ядра, целостность системы, безопасная загрузка, обработчик безопасности, отслеживающих подозрительные изменения в определённых сегментах системы в режиме реального времени.[6] Также программа позволяет быстро удалять установленные приложения ActiveX[7]. С помощью доступа к сети Microsoft SpyNet есть возможность отправлять сообщения о подозрительных объектах в Microsoft для определения его возможной принадлежности к spyware.

4) Все приложения, для работы которых требуется маркер доступа администратора, должны запрашивать подтверждение администратора. Существует только одно исключение — это взаимосвязь между родительским и дочерним процессами. Дочерние процессы наследуют маркер доступа пользователя от родительского процесса. При этом как родительский, так и дочерний процессы должны иметь один и тот же уровень целостности.

5) Рассматриваются способы защиты серверов и данных с помощью следующих двух технологий: архивация и «Теневые копии общих папок».

Архивация используется для защиты данных от случайной потери при сбоях серверного оборудования и съемных носителей. Например, можно использовать архивацию для создания запасной копии данных на жестком диске с последующей архивацией данных на другом запоминающем устройстве. Если исходные данные на жестком диске были случайно стерты или перезаписаны либо стали недоступными из-за сбоя жесткого диска, можно легко восстановить данные с помощью архивной копии.

«Теневые копии общих папок» представляют собой технологию сохранения файлов, которая обеспечивает доступ пользователей к мгновенным снимкам файлов, находящихся на общих сетевых ресурсах, таких как файловый сервер. С помощью средства «Теневые копии общих папок» пользователи могут быстро восстанавливать удаленные или измененные файлы, хранящиеся в сети, без помощи администратора, что повышает продуктивность и снижает административные затраты.

6)Одна из основных задач приложений – создание фильтра web-сайтов. Все очень просто: на одни страницы заходить можно, на другие – нельзя. Приложение работает с базой данных, где содержатся сайты для взрослых.

Еще один способ родительского контроля заключается в фильтрации сайтов по их содержимому. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается.

Программа может ограничивать время работы компьютера.

7) Брандмауэр способен анализировать абсолютно весь исходящий и входящий трафик, а также динамически открывать порты для конкретных приложений. Что конкретно из трафика будет блокировать брандмауэр, зависит от пользовательских настроек, а также внутренней базы, которая позволяет идентифицировать потенциально нежелательное содержимое.

Фильтры работают на нескольких уровнях модели OSI. Например, брандмауэр способен выполнять фильтрацию пакетов (сетевой уровень), контролировать шлюзы (сеансовый и прикладной уровни). Для каждого уровня используется свой гибкий фильтр. Например, на сетевом уровне брандмауэр анализирует заголовок IP-пакета: адреса получателя и отправителя, информацию о протоколе и приложении, номера портов. Собранная информация сравнивается с таблицей правил, после чего принимается решение — пропустить или отбраковать пакет.

8) BitLocker шифрует том, а не физический диск. Том может занимать часть диска, а может включать в себя массив из нескольких дисков. Для работы BitLocker’у в случае шифрования системного диска потребуется два NTFS-тома, один для ОС и один для загрузочной части. Последний должен быть не менее 1,5 Гб, и не быть зашифрован. Начиная с Windows Vista SP1 появилась возможность шифровать несистемные тома. После создания разделов необходимо инициализировать TPM-модуль в ПК, где он есть, и активировать BitLocker. В Windows 7 появился BitLocker To Go, позволяющий шифровать сменные носители, а также снижены требования для загрузочной части, для неё достаточно 100 Мб. При установке Windows 7 - 10 на пустой диск загрузочный раздел создаётся автоматически.

9) Компьютеры, включающие доверенный платформенный модуль, могут создавать криптографические ключи и шифровать их, чтобы их можно было расшифровать только с помощью доверенного платформенного модуля. Этот процесс, часто называемый «переносом » или «привязкой» ключа, может помочь защитить ключ от раскрытия. Каждый доверенный платформенный модуль имеет первичный ключ для переноса, называемый корневым ключом хранилища, который хранится в самом доверенном платформенном модуле. Частная часть ключа, созданного в доверенном платформенном модуле, никогда не предоставляется другим компонентам, программному обеспечению, процессу или человеку.

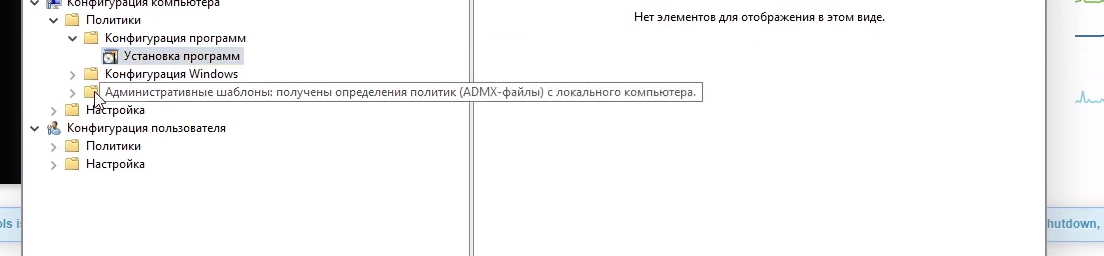
10) Это набор правил или настроек, в соответствии с которыми производится настройка рабочей среды приёма/передачи.

**2.**

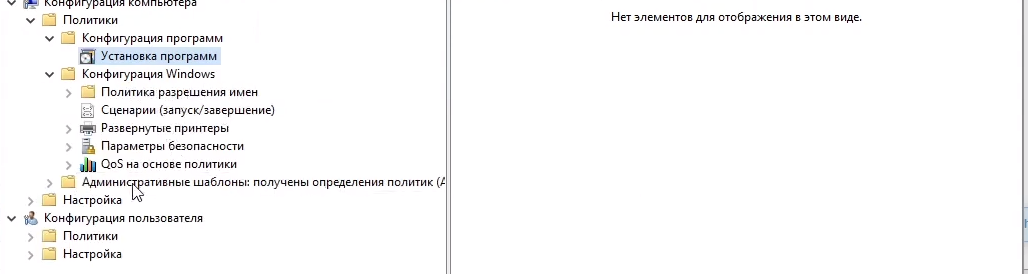
**Настройка групповой политики**

Объекты групповой политики (GPO) по умолчанию существуют для пользователей и компьютеров в управляемом домене. Компонент управления групповыми политиками позволяет просматривать и редактировать существующий объект групповой политики.

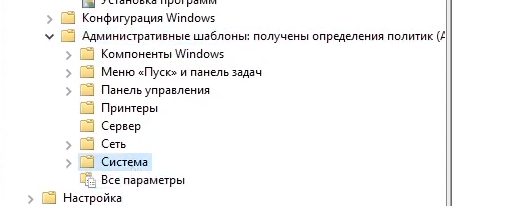
Можно установить программы для конкретного компьютера:



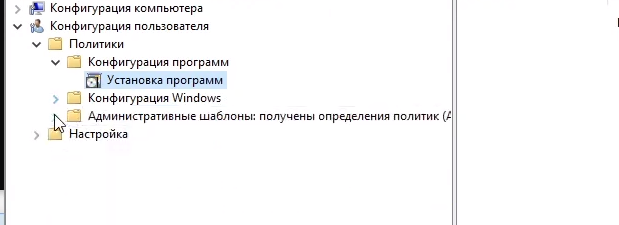
Можно прописать различные сценарии:



Можно настроить каждый компонент Windows (например, защиту от эксплойтов), настроить параметры, сеть, систему и т.д.:



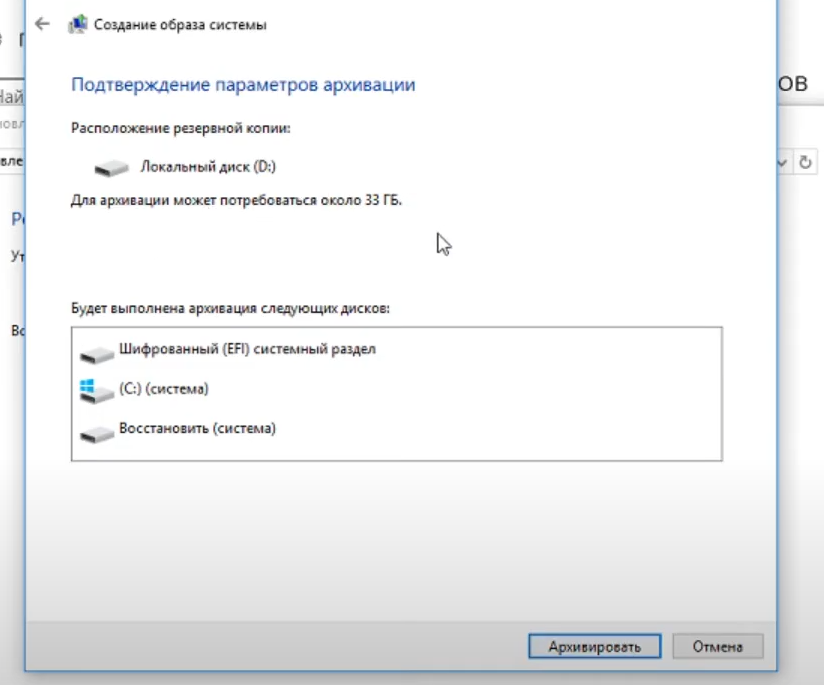
Можно настроить все это также для отдельного пользователя:



**Настройки архивирования и восстановления системы**

Все параметры – Обновление и безопасность – Служба архивации – Перейти в раздел «Архивация и восстановление» - Создание образа.

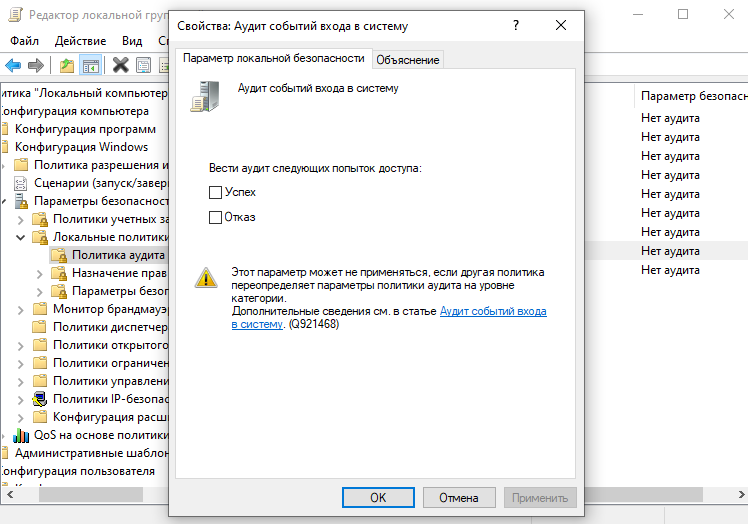
Далее создаем архив:



Далее, при установке windows мы сможем установить уже сохранённую нами версию.

**Работа защитника Windows, как и где можно отследить**

**кто и когда осуществлял вход в систему**



После включения этого параметра, Windows начнет регистрировать (в журнал безопасности) все события входа в систему, в том числе имя пользователя и время. Чтобы увидеть эти события, запустите инструмент «Просмотр событий» – откройте меню «Пуск», в строку поиска введите текст «Просмотр событий» и нажмите клавишу Enter.

Далее перейдите в «Журналы Windows» и выберите категорию «Безопасность». Нас интересуют события с кодом 4624 – это события успешного входа в систему. Я не включал ничего поэтому на скриншоте пусто:

