МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

Кафедра «Обеспечение информационной безопасности»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ по дисциплине

"Организационные и технические методы защиты информации"

для студентов бакалавриатуры по направлению 5330300- "Информационная безопасность"

Ташкент – 2021

В методических указаниях рассматриваются такие вопросы, как виды и характеристики угроз информационной безопасности на предприятиях, в организациях и различных компаниях, принципы организации служб безопасности, основные критерии найма специалистов для обеспечения конфиденциальности предприятия, защита от промышленного шпионажа, а также, защита от утечки информации и защита от перехвата данных по техническим каналам.

Каждая лабораторная работа сопровождается заданиями и вопросами для самопроверки, что способствует закреплению материала.

Составители:

Муминова С.Ш. — ассистент кафедры «Обеспечение информационной безопасности», ТУИТ

Агзамова М.Ш. — ассистент кафедры «Обеспечение информационной безопасности», ТУИТ

Рецензенты:

Ахмедова О.П — начальник научно-исследовательского отдела "Информационная безопасность и криптография" ГУП "UNICON.UZ" к.т.н.

Самаров Х.К — к.т.н., доцент кафедры «Обеспечение информационной безопасности», ТУИТ имени Мухаммад ал-Хоразмий

ВВЕДЕНИЕ

Методические указания способствуют развитию знаний по защите от компьютерных вирусов и компьютерной информации на уровне доступа в систему, применения систем обнаружения вторжений и шифрования файлов операционной системы. В результате, студенты получат навыки о настройках политики учетных записей, использования и настройки антивируса, межсетевого экрана, клиентов электронной почты, IDS и IPS систем, а также шифровании файлов системы с помощью EFS и Bitlocker.

Курс «Организационные и технические методы защиты информации» является предметом по специальности и преподается на 4 курсе обучения. Изучение данного курса требует знания и навыки по дисциплинам связанных с защитой информации, таких как «Информационная безопасность», «Сетевая безопасность» и «Безопасность баз данных».

Задача предмета – сформировать у студентов знания по защите конфиденциальной информации предприятия с использованием организационных и технических методов защиты информации, а также, осветить проблемы инженерно-технической защиты информации.

Методические указания состоят из таких компонентов, как тема практической работы, цель работы, порядок практической работы, задания для практической работы и контрольные вопросы.

В течение академического семестра студенты должны выполнять задания и представлять письменные отчеты на основе лабораторных рабочих инструкций. Каждый отчет, независимо от темы лабораторной работы, должен состоять из следующих компонентов:

1. Заглавная часть
2. Тема и цель работы.
3. Основная часть.
4. Ответы на контрольные вопросы
5. Литература

Лабораторная работа №1

Защита компьютерной информации на уровне доступа в систему.

Цель работы:

Получение навыков по настройке локальной политики безопасности: пользователей, паролей, блокировки учетной записей, прав пользователей и настроек безопасности операционной системы.

Порядок выполнения работы:

1. Настройка политики учетных записей.
2. Настройка локальной политики безопасности для пользователя.

В операционных системах семейства Windows присутствует множество оснасток и политик, представляющих собой набор параметров для настройки различных функциональных составляющих ОС. Среди них находится оснастка под названием *«Локальная политика безопасности»* и отвечает она за редактирование защитных механизмов Windows. В рамках этой лабораторной работы обсуждаются компоненты упомянутого инструмента и расскажем о их влиянии на взаимодействие с системой.

1.Настройка политики учетных записей

Первая категория называется *«Политики учетных записей»*. Разверните ее и откройте раздел *«Политика паролей»*. Справа находится перечень параметров, каждый из которых отвечает за ограничения или выполнение действий. Например, в пункте *«Минимальная длина пароля»* вы самостоятельно указываете количество знаков, а в *«Минимальный срок действия пароля»* — количество дней на блокировку его изменения (рис. 1.).

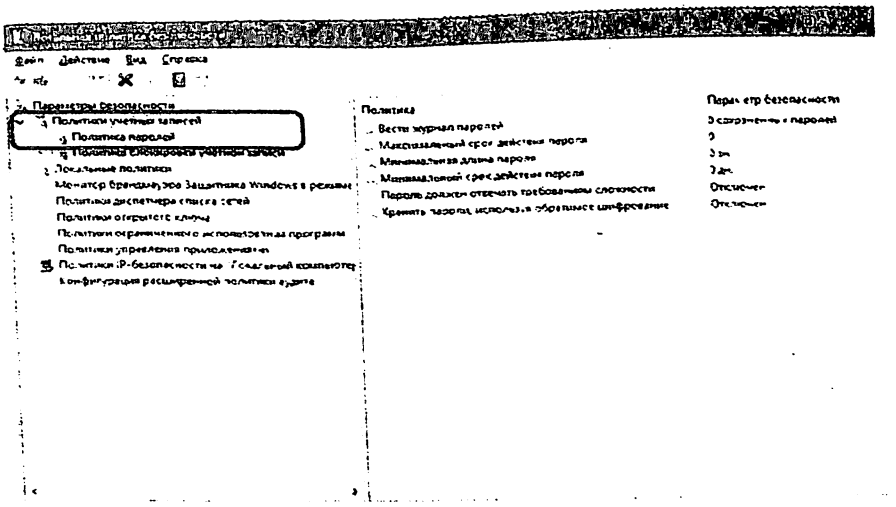


Рис.1. Политика учетных записей.

Дважды щелкните на одном из параметров, чтобы открыть отдельное окно с его свойствами. Как правило, здесь присутствует ограниченное количество кнопок и настроек. Например, в *«Минимальный срок действия пароля»* вы только выставляете количество дней (рис.2.).

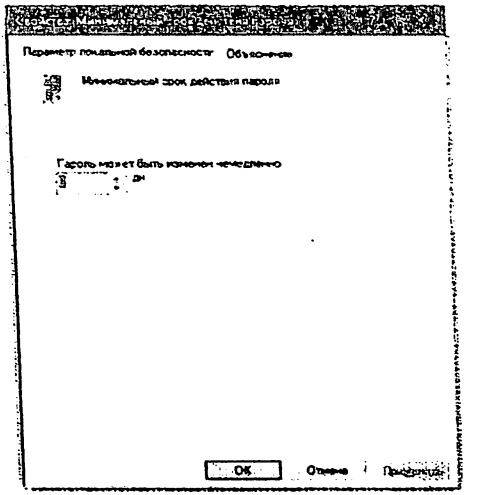


Рис.2. Параметр локальной безопасности

Во вкладке *«Объяснение»* находится детальное описание каждого параметра от разработчиков (рис.3.). Обычно оно расписано достаточно широко, но большая часть информации является бесполезной или же очевидной, поэтому ее можно опустить, выделив только основные моменты лично для себя.

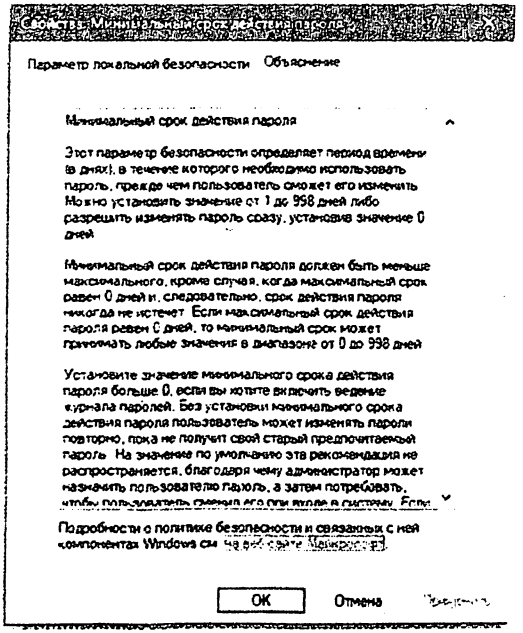


Рис.3. Вкладка «Объяснение»

Во второй папке *«Политика блокировки учетной записи»* присутствует три политики. Здесь доступна установка времени до сброса счетчика блокировки, пороговое значение блокировки (количество ошибок ввода пароля при входе в систему) и продолжительность блокировки профиля пользователя (рис.4).

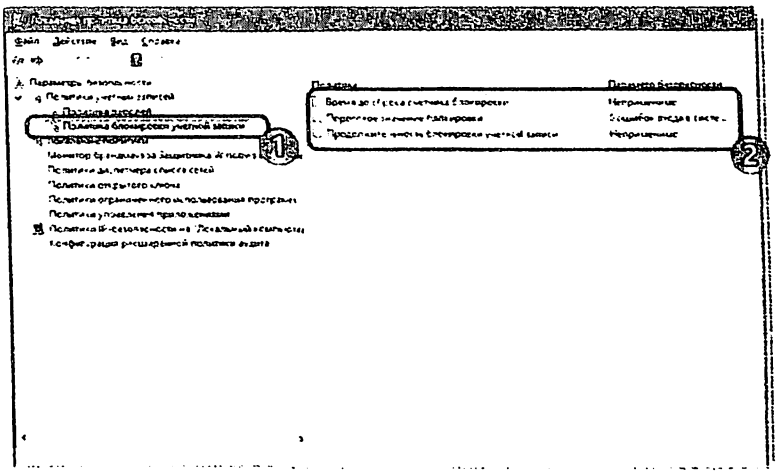


Рис.4. Политика блокировки учетной записи

2.Настройка локальной политики безопасности для пользователя.

Локальные политики. В разделе *«Локальные политики»* собрано сразу несколько групп параметров, разделенных по директориям. Первая имеет название *«Политика аудита»* (рис.5.). Если говорить просто, аудит — процедура слежения за действиями пользователя с дальнейшим занесением их в журнал событий и безопасности.

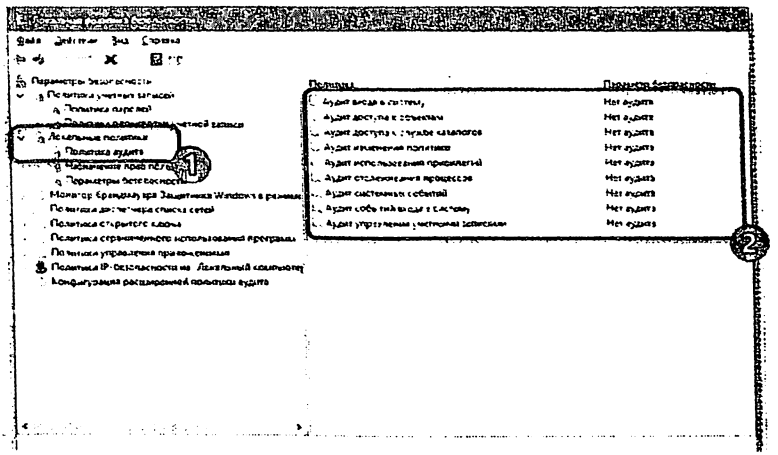


Рис.5. Раздел «Политика аудита»

Если значение установлено *«Нет аудита»*, действия отслеживаться не будут. В свойствах же на выбор предоставляется два варианта — *«Отказ»* и *«Успех»*. Поставьте галочку на одном из них или сразу на обоих, чтобы сохранять успешные и прерванные действия (рис.6.).

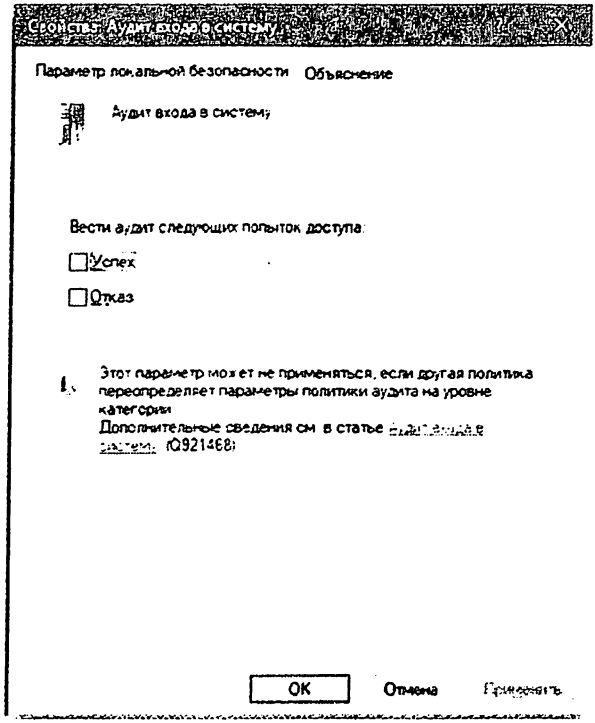


Рис.6. Параметр аудита входа в систему

В папке *«Назначение прав пользователя»* собраны настройки, позволяющие предоставить группам пользователей доступ для выполнения определенных процессов, например, вход в качестве службы, возможность подключения к интернету, установка или удаление драйверов устройств и многое другое (рис.7.). Ознакомьтесь со всеми пунктами и их описанием самостоятельно.

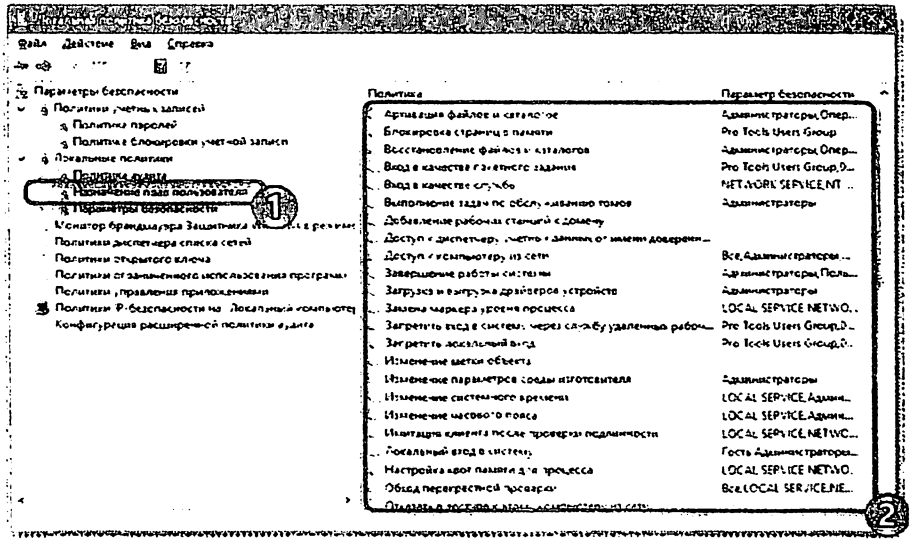


Рис.7. Назначение прав пользователя

В *«Свойства»* вы видите перечень групп пользователей, которым разрешено осуществление заданного действия (Рис.8.).

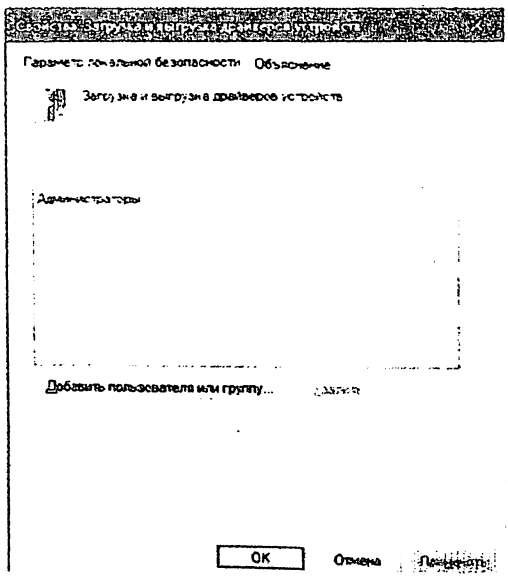


Рис.8. Свойства загрузки и выгрузки драйверов устройств

В отдельном окне происходит добавление групп пользователей или только некоторых учетных записей из локальных компьютеров (рис.9.). От вас требуется лишь указать тип объекта и его размещение, а после перезагрузки компьютера все изменения вступят в силу.

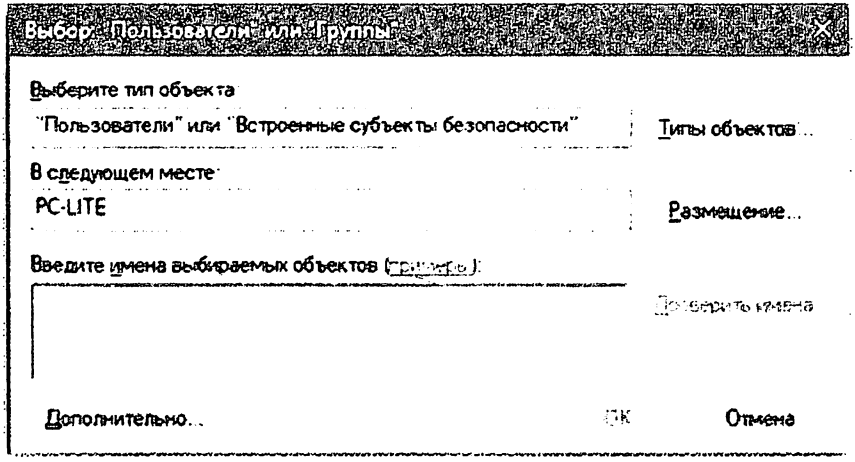


Рис.9. Добавление групп пользователей или учетных записей

Раздел *«Параметры безопасности»* посвящен обеспечению защищенности двух предыдущих политик. То есть здесь вы можете настроить аудит, который будет отключать систему при невозможности добавления соответствующей записи аудита в журнал, либо же установить ограничение на количество попыток ввода пароля. Параметров здесь насчитывается более тридцати. Условно их можно разделить на группы — аудиты, интерактивный вход в систему, контроль учетных записей, сетевой доступ, устройства и сетевая безопасность. В свойствах вам разрешено активировать или отключать каждую из этих настроек (рис.10.).

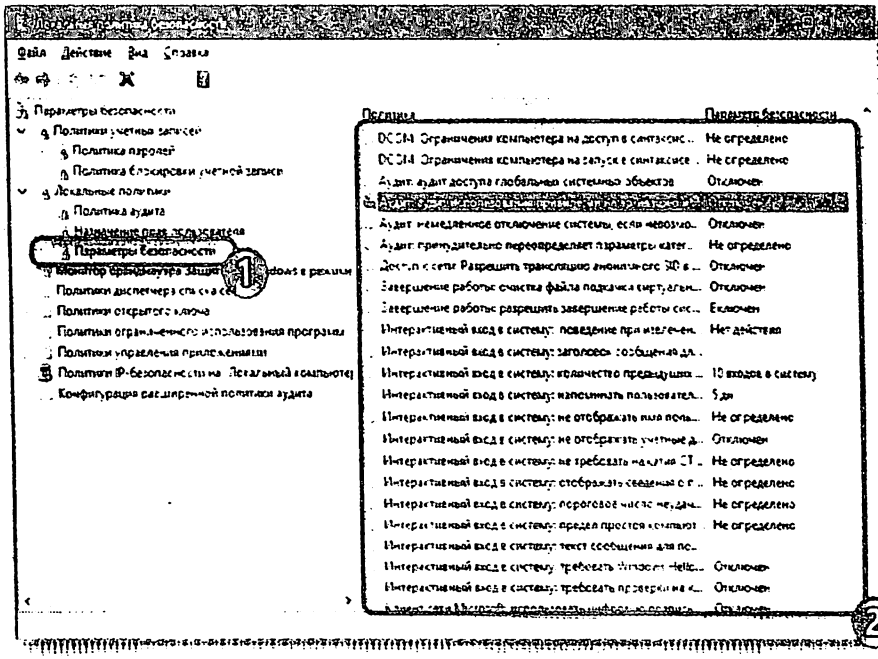


Рис.10. Раздел *«Параметры безопасности»*

Монитор брандмауэра Защитника Windows в режиме повышенной безопасности. *«Монитор брандмауэра Защитника Windows в режиме повышенной безопасности»* — один из самых сложных разделов *«Локальной политики безопасности»*. Разработчики попытались упростить процесс наладки входящих и исходящих подключений с помощью добавления Мастера настройки, однако начинающие пользователи все равно с трудом разберутся со всеми пунктами, но эти параметры и крайне редко нужны такой группе пользователей. Здесь доступно создание правил для программ, портов или предопределенных соединений. Вы блокируете либо разрешаете подключение, выбрав при этом сеть и группу (рис.11.).

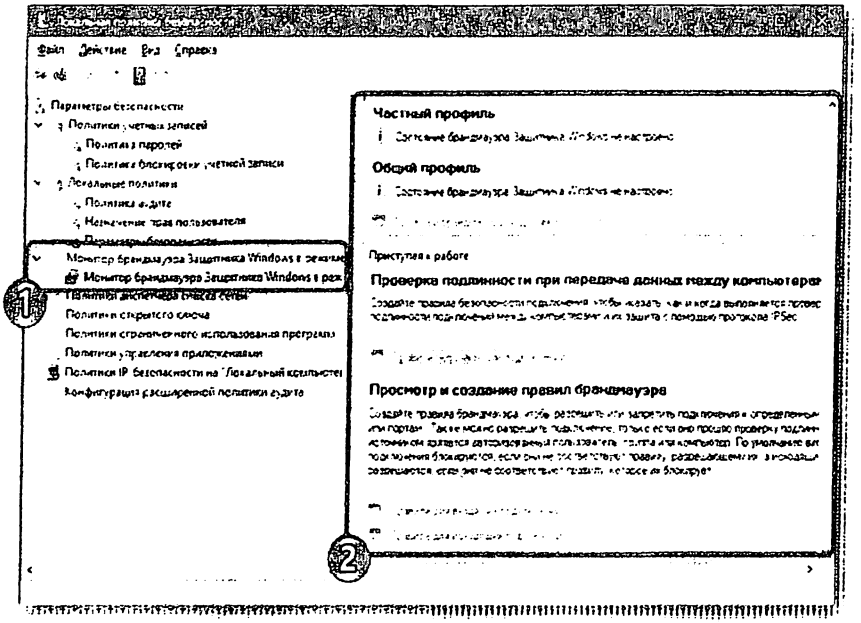


Рис.11. «Монитор брандмауэра Защитника Windows в режиме повышенной безопасности»

В этом же разделе происходит определение типа безопасности подключения — изоляция, сервер-сервер, туннель или освобождение от проверки подлинности. Останавливаться на всех настройках нет смысла, ведь это пригодится только опытным администраторам, а они в состоянии самостоятельно обеспечить надежность входящих и исходящих соединений.

Политики диспетчера списка сетей. Обратите внимание на отдельную директорию *«Политики диспетчера списка сетей»*. Количество отображаемых здесь параметров зависит от активных и доступных интернет-соединений. Например, пункт *«Неопознанные сети»* или *«Идентификация сетей»* будет присутствовать всегда, а *«Сеть 1»*, *«Сеть 2»* и так далее — в зависимости от реализации вашего окружения (рис. 12.).

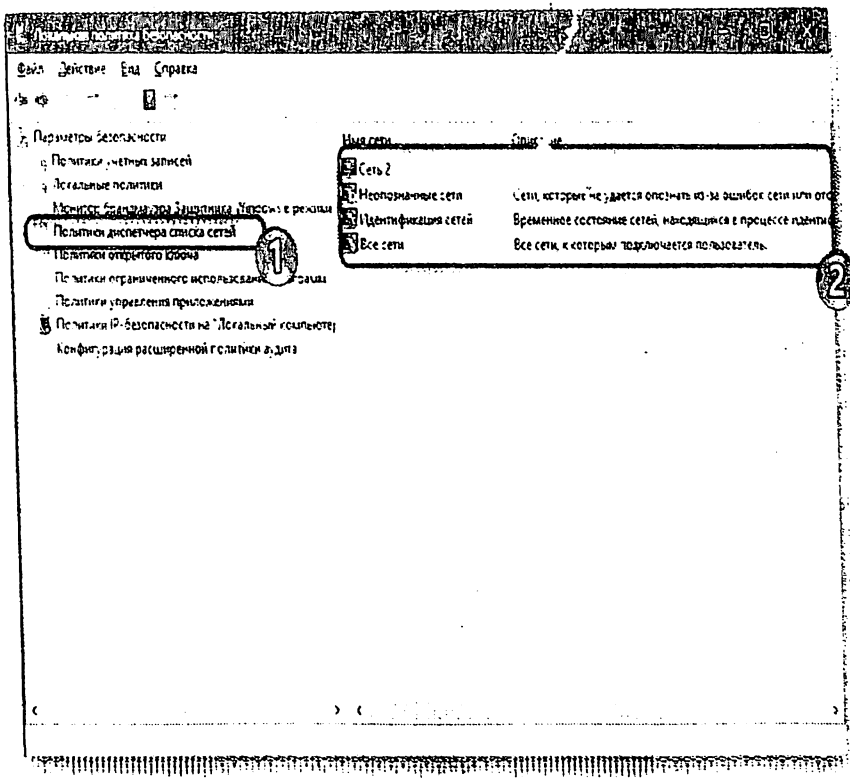


Рис.12. *«Политики диспетчера списка сетей»*

В свойствах вы можете указать имя сети, добавить разрешения для пользователей, установить собственный значок или задать расположение. Все это доступно для каждого параметра и должно применяться отдельно (рис.13.). После выполнения изменений не забывайте их применять и перезагружать компьютер, чтобы они вступали в силу. Иногда может потребоваться и перезагрузка роутера.

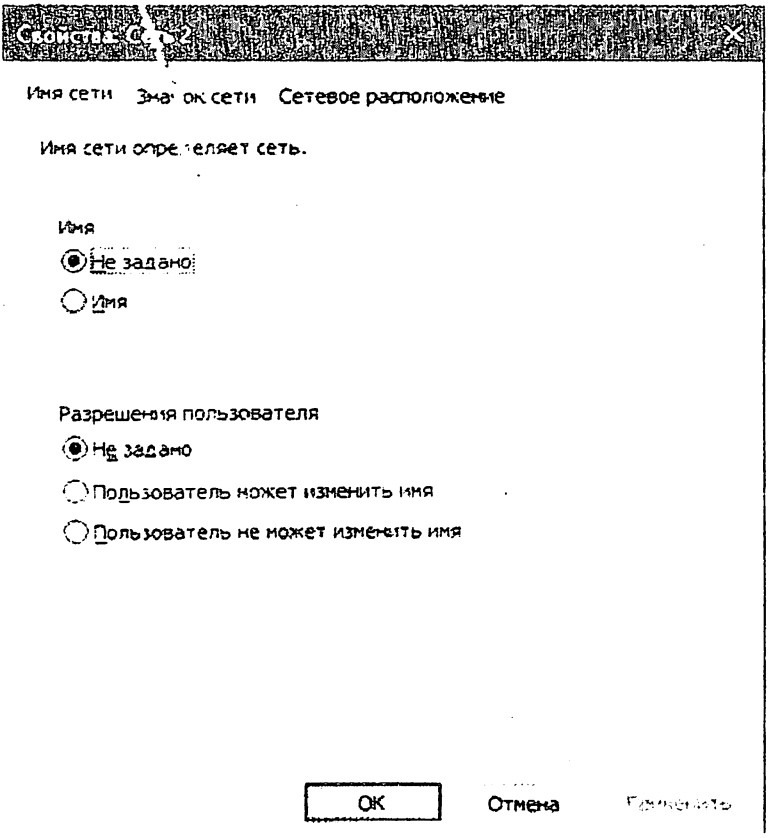


Рис.13. Свойства сети

Политики открытого ключа. Полезным раздел *«Политики открытого ключа»* будет только для тех, кто использует компьютеры на предприятии, где для осуществления криптографических операций или других защищенных манипуляций задействованы открытые ключи и центры спецификаций (рис.14.). Все это позволяет гибко производить контроль доверительных отношений между устройствами, обеспечив стабильную и безопасную сеть. Внесения изменений зависят от активного на предприятии центра доверенности.

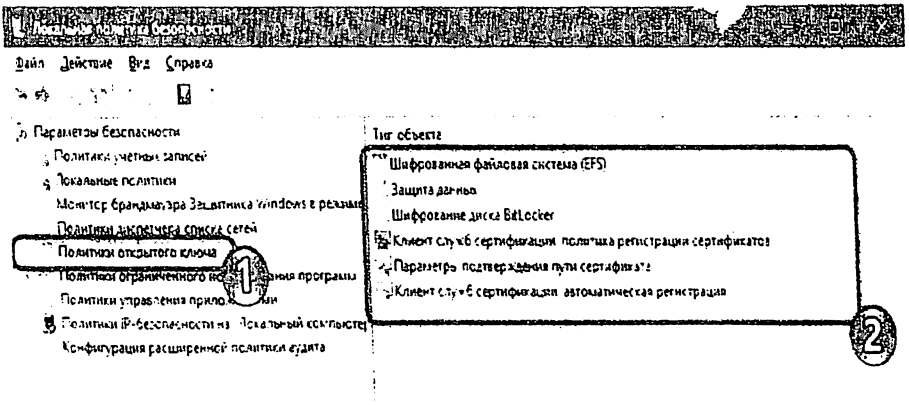


Рис.14. Раздел *«Политики открытого ключа»*

Политики управления приложениями. В *«Политики управления приложениями»* находится инструмент *«AppLocker»* (рис.15). Он включает в себя множество самых разнообразных функций и настроек, позволяющих регулировать работу с программами на ПК. Например, он позволяет создать правило, ограничивающее запуск всех приложений, кроме указанных, либо установить ограничение на изменение файлов программами, задав отдельные аргументы и исключения. Полную информацию по поводу упомянутого инструмента вы можете получить в официальной документации компании Microsoft, там все расписано максимально детально, с объяснением каждого пункта.

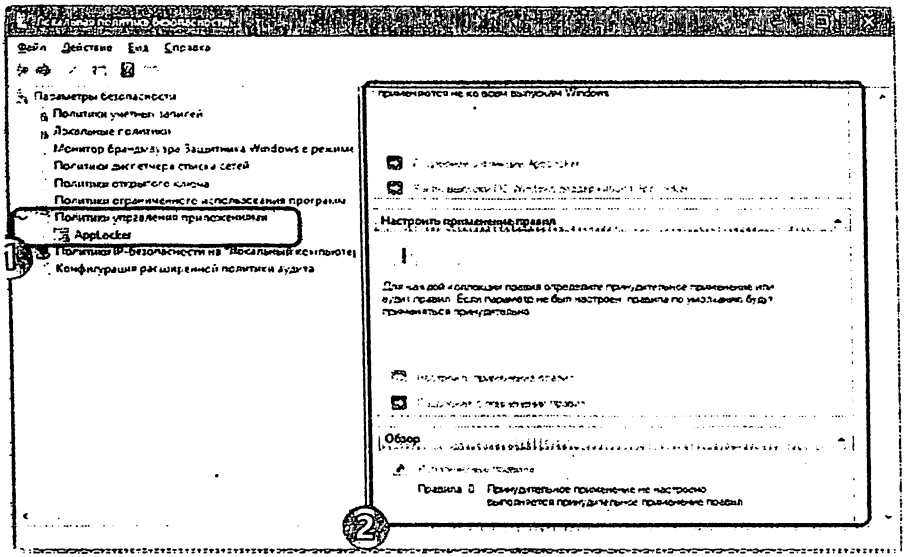


Рис.15. *«Политики управления приложениями»*

Что же касается меню *«Свойства»*, то здесь применение правил настраивается для коллекций, например, исполняемые файлы, установщик Windows, сценарии и упакованные приложения(рис.16.). Каждое значение может применяться принудительно, в обход другим ограничениям *«Локальной политики безопасности»*.

Политики IP-безопасности на «Локальный компьютер». Настройки в разделе *«Политики IP-безопасности на «Локальный компьютер»»* имеют некое сходство с теми, что доступны в веб-интерфейсе роутера, например, включение шифрования трафика либо его фильтрация (рис.17.). Пользователь сам создает неограниченное количество правил через встроенный Мастер создания указывает там методы шифрования, ограничения на передачу и прием трафика, а также активирует фильтрацию по IP-адресам (разрешение или запрет на подключение к сети).

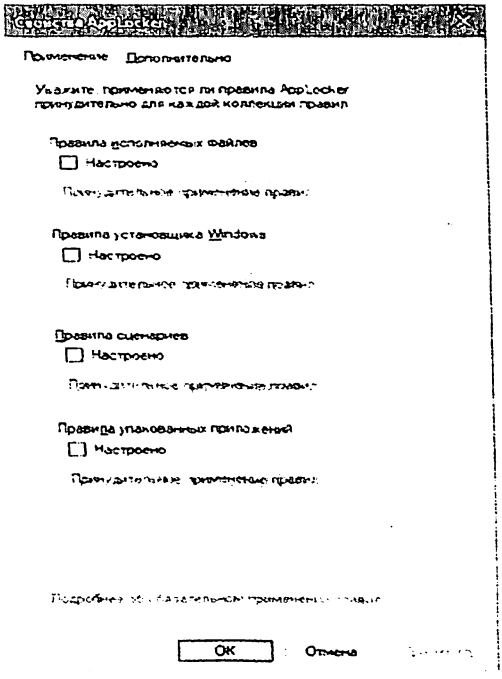


Рис. 16. Свойства Applocker

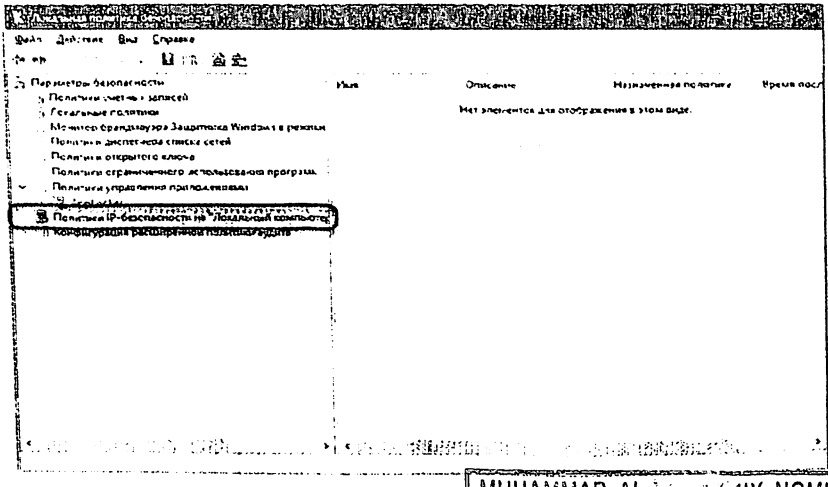


Рис.17. Раздел «*Политики IP-безопасности на «Локальный компьютер»*»

На рисунке ниже вы видите пример одного из таких правил связи с другими компьютерами. Здесь присутствует список IP-фильтров, их действие, методы проверки, конечная точка и тип подключения. Все это задается пользователем вручную, исходя из его потребностей в обеспечении фильтрации передачи и приема трафика с определенных источников(рис.18).

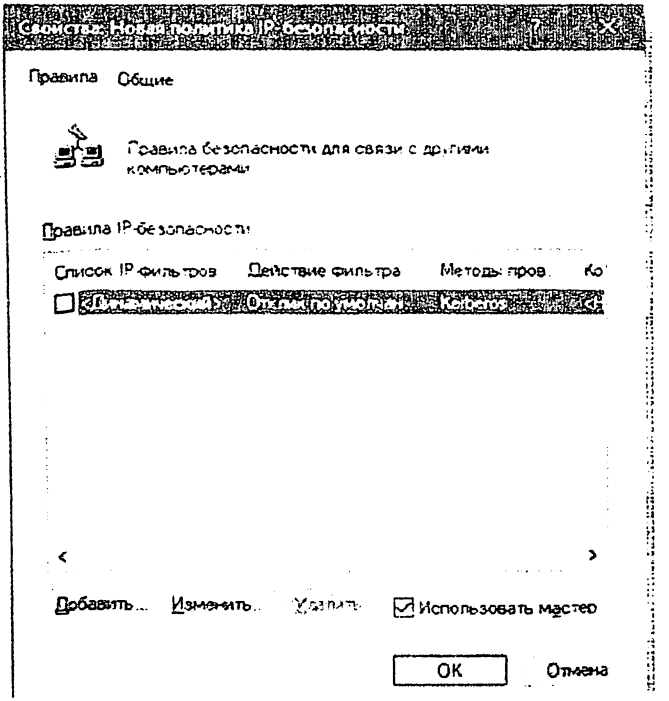


Рис.18. Свойства политики IP-безопасности

Конфигурация расширенной политики аудита. Существуют еще дополнительные параметры, которые вынесены в отдельный раздел. Здесь уже вы видите более обширное действие аудитов — создание/завершение процессов, изменение файловой системы, реестра, политик, управление группами учетных записей пользователей, приложений и многое другое, с чем можете ознакомиться самостоятельно (рис.19).

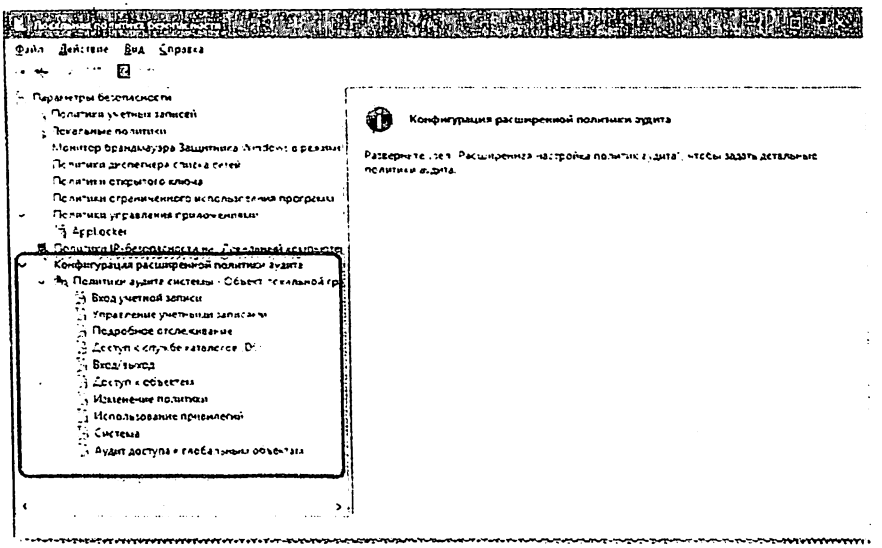


Рис.19. Конфигурация расширенной политики аудита

Корректировка правил осуществляется точно так же — нужно лишь отметить галочкой *«Успех»*, *«Отказ»*, чтобы запустить процедуру слежения и записи в журнал безопасности.

Перед внесением определенных изменений нужно внимательно изучить описание самого параметра, чтобы понять его принцип работы. Редактирование некоторых правил иногда приводит к серьезным проблемам работы ОС, поэтому делать нужно все крайне осторожно.

Задание:

1. Ознакомьтесь с ходом лабораторной работы;
2. Создайте пользователя с именем вашей учетной записи.
3. Настройте на ПК политику паролей и политику блокировки учетной записи.
4. Подготовьтесь к контрольным вопросам.

Контрольные вопросы:

1. Поясните параметр «Потребовать смену пароля при следующем входе в систему».
2. При помощи какой функции можно сбросить забытый пароль и кто может воспользоваться этой функцией?
3. Поясните параметр «Требовать не повторяемости паролей»
4. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если политика включена.
5. Какие параметры входят в политику блокировки учетной записи?
6. Возможно ли, что учетная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?
7. В каком разделе предоставляется возможность назначать пользователям права, связанные с информационной безопасностью?
8. В каком разделе предоставляется возможность устанавливать параметры операционной системы, связанных с информационной безопасностью?
9. Перечислите другие функции и параметры локальной политики безопасности.
10. Какие расширенные конфигурации имеет политику аудита?

Лабораторная работа №2

Защита от компьютерных вирусов.

Цель работы: Получение навыков по работе штатных средств защиты от компьютерных вирусов ОС и антивирусных программ.

Порядок выполнения работы:

1. Настройка параметров Защитника Windows
2. Установка и настройка антивирусной программы

1. Настройка параметров Защитника Windows в ОС Windows 10.

Windows Defender — встроенное в операционную систему программное обеспечение, которое защищает пользователя от вирусов и шпионских программ. В принципе он обеспечивает неплохой уровень защиты, но иногда мешает установить новое ПО, даже лицензионное и от известных разработчиков. В этом случае Защитника можно на время отключить.

Windows 10 еще больше упрощает взаимодействие с настройками Защитника Windows и использует универсальное приложение "Параметры" для настройки (Рис.20.).

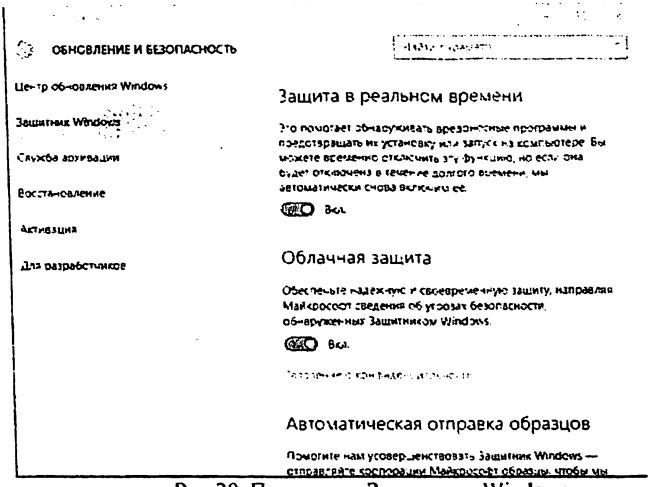


Рис.20. Параметры Защитника Windows

Включите параметр "Защита реального времени" для того, чтобы включить Защитник Windows. При отключении опции остальные параметры будут недоступны (выделены серым цветом).

"Облачная защита" позволяет усилить безопасность для большинства пользователей. Только если пользователь очень беспокоится о конфиденциальности можно отключить данную опцию.

"Автоматическая отправка образцов" очень схожа с предыдущей настройкой, поэтому стоит оставить эту опцию включенной.

Если пользователь не является профессиональным IT-специалистом, лучше не трогать Исключения. Для завершения нужно закрыть приложение.

Сообщения Защитника Windows в Windows 8, 8.1 и 10. В Windows 8 и 8.1 Защитник Windows не имеет иконки в области уведомлений панели задач, поэтому лучшим решением будет являться периодическая проверка состояния иконки Центра Поддержки. Если у флажка появился красный круг с меткой "X", что-то пошло не так. Нажмите на иконку для просмотра списка обнаруженных проблем - это может быть не связано с Защитником Windows.

В Windows 10 иконка Защитника Windows была возвращена. Иконка работает стабильно, ее ничто не перекрывает. Для открытия самой программы нужно нажать правой кнопкой мыши по иконке и выбрать пункт "Открыть"(рис.21.).

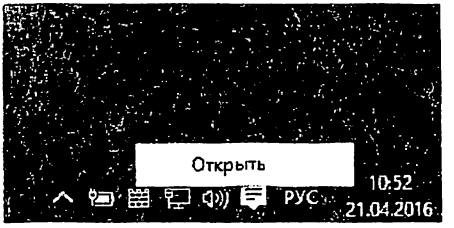


Рис.21. Иконка Защитника Windows

Если у иконки появился красный круг с белым крестиком, что-то пошло не так, например произошло вредоносное заражение и для очистки требуется внимание пользователя. Если рядом с иконкой отображается зеленый круг, то выполняется сканирование - не нужно предпринимать никаких действий(рис.22.).

Рис.22. Выполняется сканирование

В случае, если Защитнику Windows потребуется просканировать компьютер в Центре действия появится соответствующее оповещение, просто нажмите на него для запуска проверки. Программа проводит автоматическое сканирование каждый день в 3:00 по умолчанию, и пользователь увидит уведомления, если системный антивирус пропустил несколько проверок.

Если Центр действия отображает оповещений "Обновите антивирусную защиту (Важно)" и "Обновите защиту от шпионских программ (Важно)" нужно нажать по ним для открытия Защитника Windows для загрузки новейших сигнатурных определений.

Если показаны сообщения "Включение защиту от вирусов (Важно)" или "Включение защиту от программ-шпионов (Важно)", нужно нажать на любое из них и дождаться загрузки Защитника Windows (Рис.23). Статус компьютера в главном окне Защитника Windows должен вскоре стать зеленым, после чего можно закрыть окно. Данные сообщения обычно появляются при отключении служб или защиты реального времени Защитника Windows.

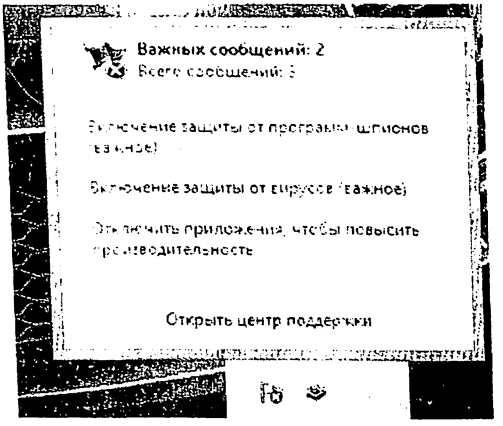


Рис.23. Показаны важные сообщения Защитника Windows

Если появилось сообщение "Невозможно запустить службу Защитника Windows", служба антивирусной защиты была остановлена или отключена. Нажмите кнопку "Закрыть".

В Windows 8 и 8.1 нужно открыть поиск (клавиша Windows + W), ввести фразу "служб" и выбрать утилиту "Просмотр локальных служб". В Windows 10 нужно открыть меню Пуск или поиск Cortana (клавиатурное сочетание Windows + S). После этого найти со списка служб "Служба Защитника Windows" и проверить, не стоит ли в поле "Тип запуска" значение "Отключена".

Только в Windows 8: нужно вызвать контекстное меню отключенной службы и выбрать пункт меню "Свойства" (рис.24.).

В Windows 8.1 и 10 Вы не можете изменять настройки службы Защитника Windows в обычном режиме.

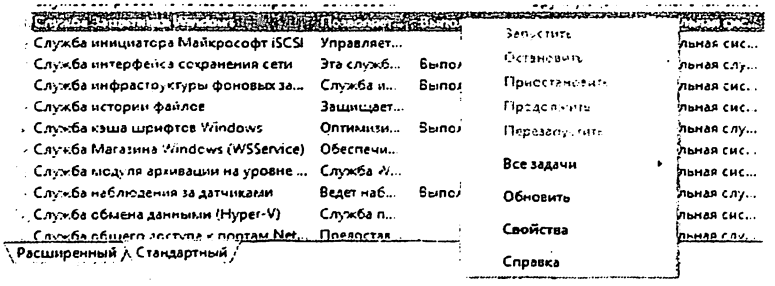


Рис.24. Вызов контекстного меню

Затем только в Windows 8 в окне настроек службы Защитника Windows измените тип запуска на "Автоматически"(рис.25.). Затем нажмите кнопку "Запустить", а затем "ОК".

В Windows 8.1 и 10 нужно загрузиться в Безопасном режиме. После авторизации откроется стартовый экран и стартовое меню, нужно ввести команду *regedit*, щелкнуть правой кнопкой мыши по результату и выбрать опцию "Запустить от имени администратора". После этого нужно перейти в раздел *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services* и нажать по записи *WinDefend*.

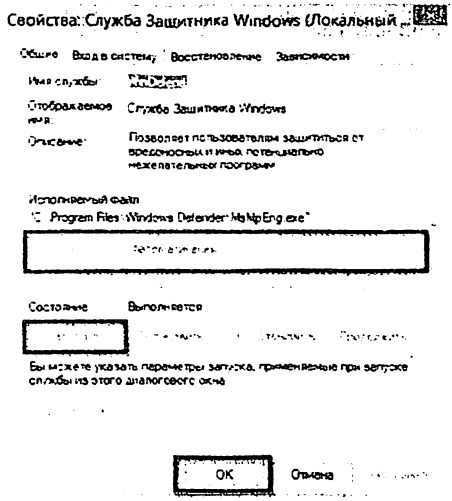


Рис.25. Настройки службы Защитника Windows

Выбрать запись *Start* в правой панели. Если значение параметра равняется 0x00000004 (4), служба была отключена. Нужно нажать дважды по записи *Start* (рис. 26.).

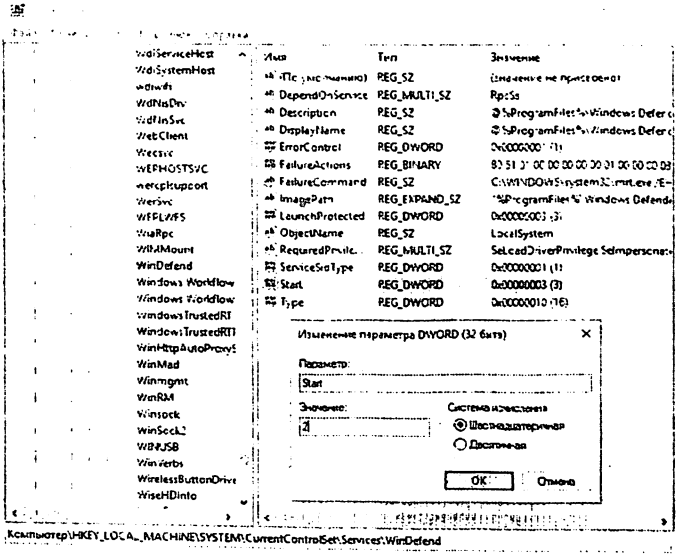


Рис.26. Запуск программы от имени администратора

ключевые фразы, сигнальные строки и прочие настройки системы фильтрации, можно управлять письмами (критерии которых удовлетворяют правилам) непосредственно на сервере. Это может быть очень полезным для экономии трафика либо в случае использования низкоскоростного сетевого соединения, затрудняющего скачивание писем с прикрепленными файлами большого размера.

Задание:

1. Ознакомиться ходом лабораторной работы.
2. Установить программу "The Bat!".
3. Изучить принципы работы и основные сервисы почтовых серверов и файлообменных сетей.
4. Настроить параметры защиты.

Контрольные вопросы:

1. Дайте определение термину спам. Назовите известные вам виды спама и способы борьбы с ним
2. Что такое почтовый клиент? Перечислите наиболее популярные почтовые клиенты
3. Опишите преимущества почтового клиента The Bat перед другими почтовыми клиентами.
4. Перечислите и опишите наиболее популярные плагины для почтового клиента The Bat
5. Какие протоколы используются при передаче файлов в Интернет?

Лабораторная работа №5.

Система обнаружения вторжений IPS/IDS.

Цель работы:

Совершенствование базовых навыков по установке систем обнаружения и предотвращения вторжений на примере программы SNORT.

Порядок выполнения работы:

1. Установка программы
2. Изучение программы и его режимы

Snort является свободно распространяемой программой с открытым исходным кодом под лицензией GPL. Изначально Snort был создан одним из известнейших людей в мире информационной безопасности, автором многих: книг Мартином Рошем в 1998 году. Основной причиной создания этой IDS было отсутствие на тот момент достаточно эффективного, тем более бесплатного, инструмента оповещения об атаках.

Программа совместима с ОС Windows и Linux. Все выявленные угрозы (список параметров подачи тревоги имеет тонкие настройки), записываются в лог-файл. Snort работает по принципу анализа пакетов транспортного уровня, поэтому для его использования, требуется перевод сетевой карты в специальный мониторный режим. Разработчики учитывали проблему потребления системных ресурсов системами класса IDS, поэтому Snort нетребовательна к железу и работает в фоновом режиме.

Поступив в SNORT, пакет последовательно проходит через декодеры, препроцессоры и только потом уже попадает в детектор, который начинает применять правила. Задача декодеров сводится к тому, чтоб из протоколов канального уровня (Ethernet, 802.11, Token Ring...) «вытащить» данные сетевого и транспортного уровня (IP, TCP, UDP) (Рис.88).

Snort использует 'правила' (указанные в файлах 'правила'), чтобы знать какой трафик пропустить а какой задержать. Инструмент гибок, позволяя вам записывать новые правила и соблюдать их . Программа также имеет ' механизм обнаружения ', который использует модульную сменную архитектуру, посредством чего определенные дополнения к программе могут быть добавлены или удалены из ' механизма обнаружения'.

Snort может работать в трех режимах:

1. Как пакетный снифер, подобно tcpdump;
2. Как регистратор пакета;

Если для завершения очистки требуется перезагрузка компьютера, появится следующее уведомление (рис.29.). Нажмите его для запуска Защитника Windows.

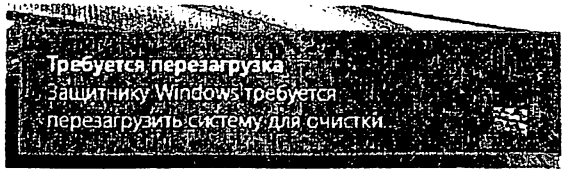


Рис.29. Уведомление о перезагрузке компьютера.

Нажмите большую кнопку "Перезагрузить сейчас" в окне Защитника Windows. Ваш компьютер будет перезагружен и защитник Windows удалит оставшиеся следы вредоносной программы.

Обновление антивирусной программы. Откройте "Все параметры". Выберите "Обновления и безопасность" => "Безопасность Windows" => "Защита от вирусов и угроз"(рис.30.). Нажмите на "Обновление защиты от вирусов и угроз" в открывшимся окне нажмите на кнопку "Проверить наличие обновлений"(рис.31.).

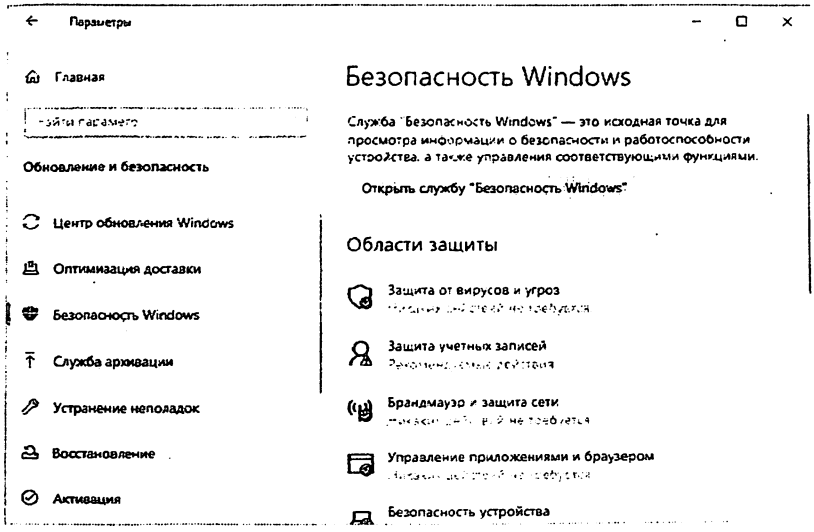


Рис. 30. Опция "Защита от вирусов и угроз"

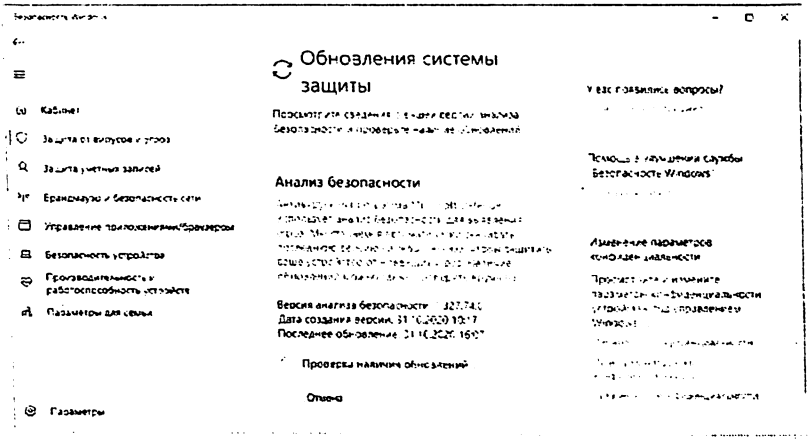


Рис.31. Обновление антивирусной программы

2. Установка и настройка антивирусной программы

Для установки антивируса было выбрано Антивирус Касперского. Для этого скачиваем с официального сайта 30-дневную пробную версию антивируса(рис.32.).

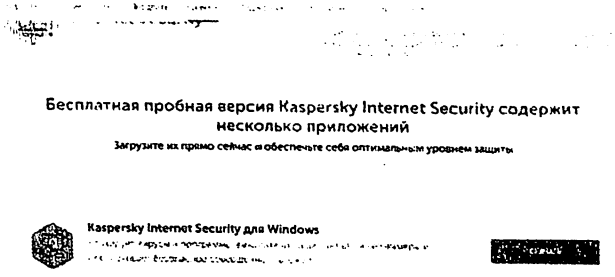


Рис.32. Скачивание файла с официального сайта.

После скачивания запускаем программу. Все, что вам нужно сделать, это нажать на загруженный файл (рис.33). Мы можем прочитать предупреждение. Щелкните «Продолжить».

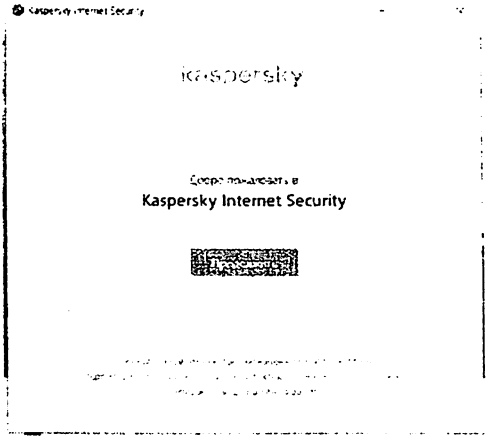


Рис.33. Установка программы.

Нужно ознакомится с условиями лицензионного соглашения (рис.34.) и положением о Kaspersky Security Network, затем нажать кнопку «принять» (рис.35.).

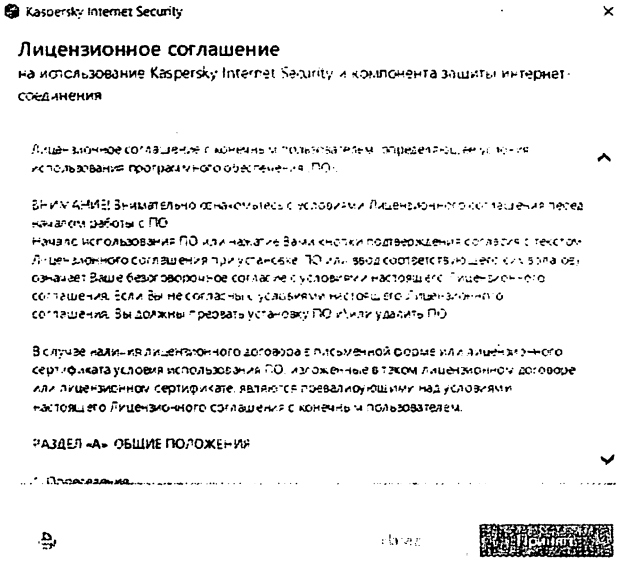


Рис.34. Лицензионное соглашение

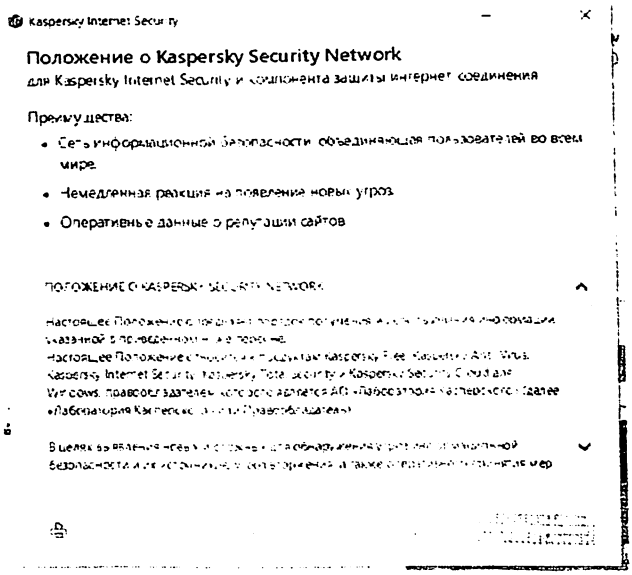


Рис.35. Положение о Kaspersky Security Network

После этого переходим к установке. Это займёт несколько минут (рис.36.).

Рис.36. Процесс установки.

После установки откроется окно с рекомендуемыми настройками (рис.37.). Нажимаем на «Применить». На этом установка завершена (рис.38.).

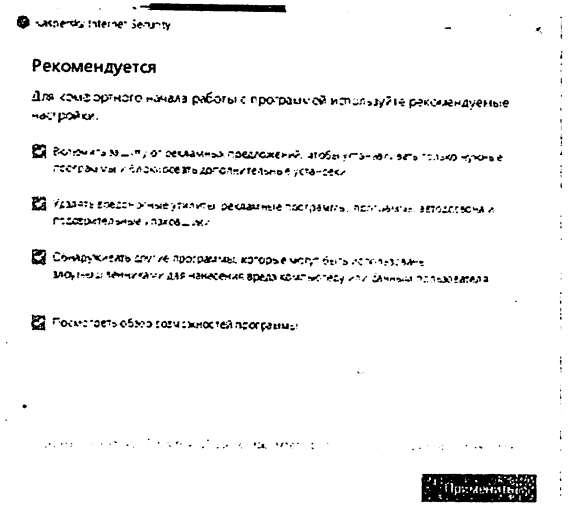


Рис.37. Рекомендуемые настройки

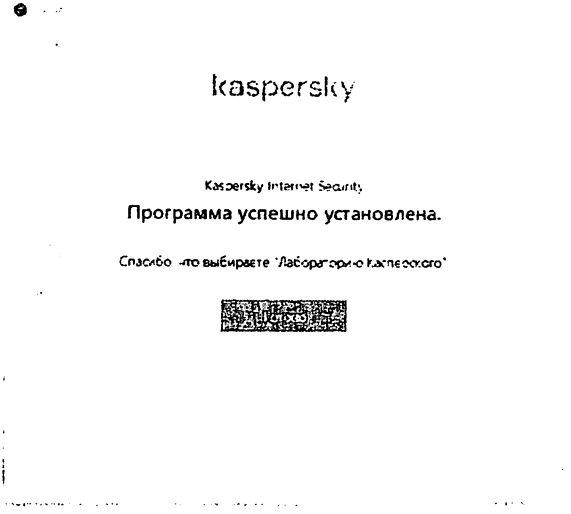


Рис. 38. Окно завершение установки.

После установки программы идёт запуск программы. При первом запуске программа дает нам различные рекомендации, информацию о программе. Нужно ознакомится с дополнительными возможностями и каждый раз нажать «далее» (рис.39.).

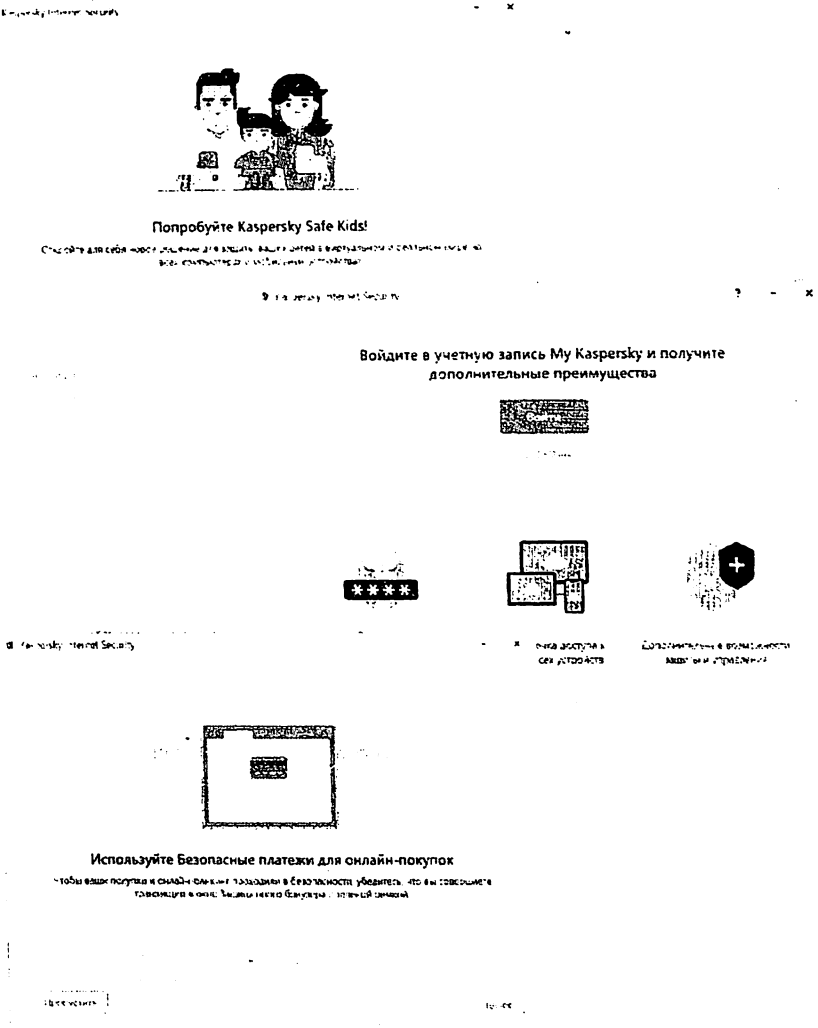


Рис.39. Дополнительные возможности программы

После ознакомления с дополнительными возможностями требуются обновить базу сигнатур. Для этого нажмите кнопку «Обновление баз». Нажимаем на кнопку «Обновить». Затем дожидаемся загрузки новой базы данных (рис.40.).

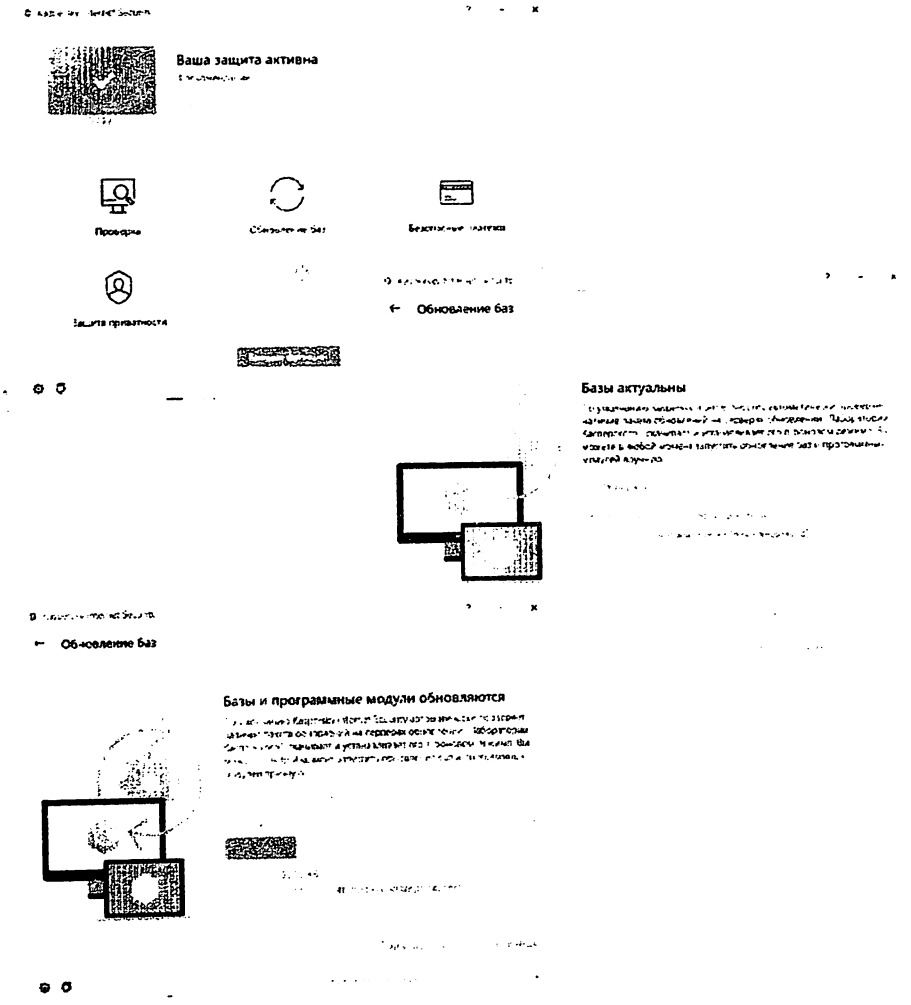


Рис.40. Обновление баз сигнатур.

Сканирование жесткого диска. Чтобы проверить жёсткий диск компьютера, откройте главное меню. Затем нажмите «Проверка» (рис.41.).

Рис.41. Главное меню программы

Ниже приведены типы сканирования памяти. Мы можем выбрать наиболее подходящий вариант. В нашем случае показан «Быстрая проверка» (рис.42.).

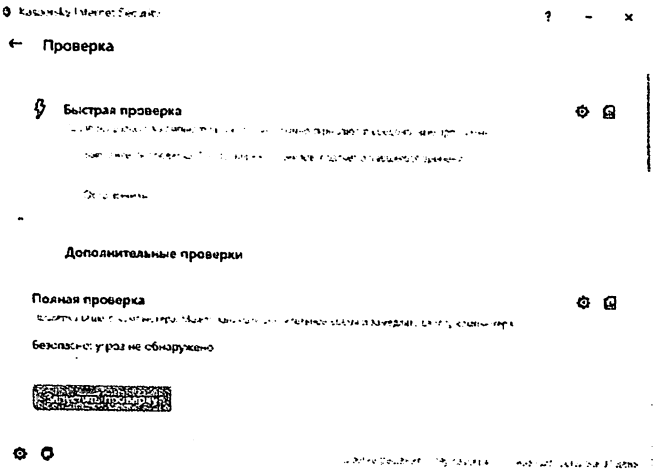


Рис.42. Быстрая проверка

По окончании проверки мы будем уведомлены. При обнаружении вредоносного ПО нужно нажать «Лечить с перезагрузкой компьютера». После завершения операции компьютер перезагрузится (рис.43.)

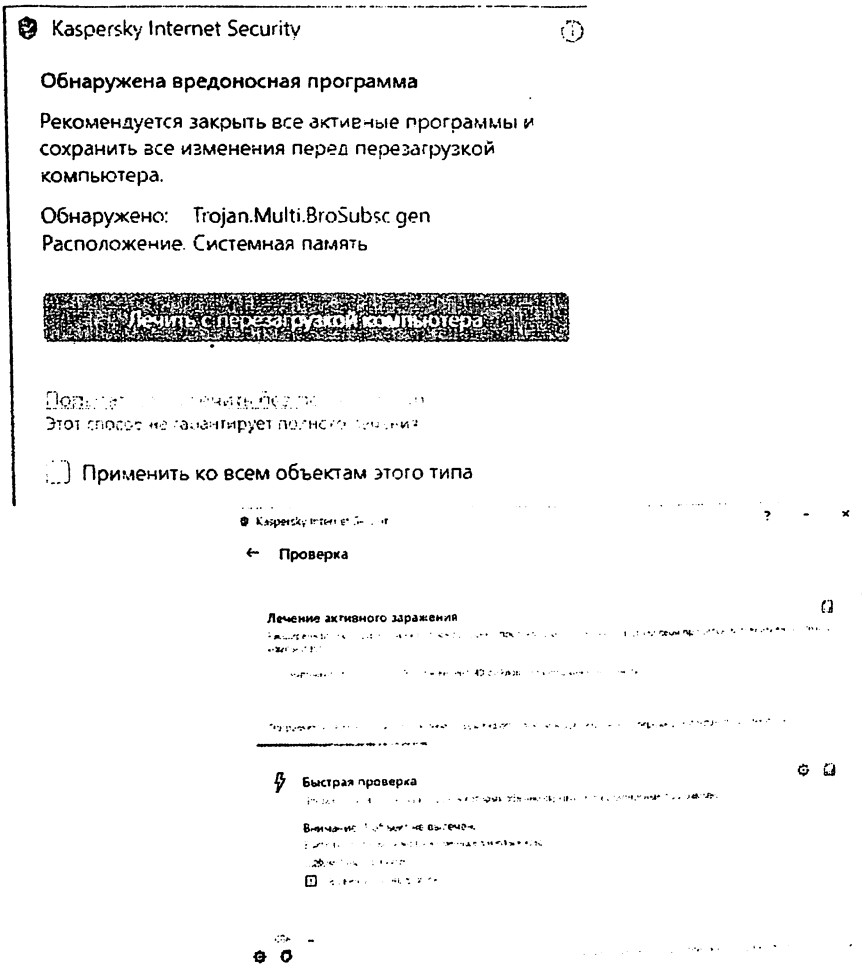


Рис. 43. Лечение активного заражения.

В дополнительных настройках имеется Мастер восстановления после заражения, он выполняет поиск повреждений в операционной системе (рис.44-45). Причиной появления таких повреждений может быть активность вредоносных программ, системные сбои, а также применение неправильно работающих оптимизаторов операционной системы.

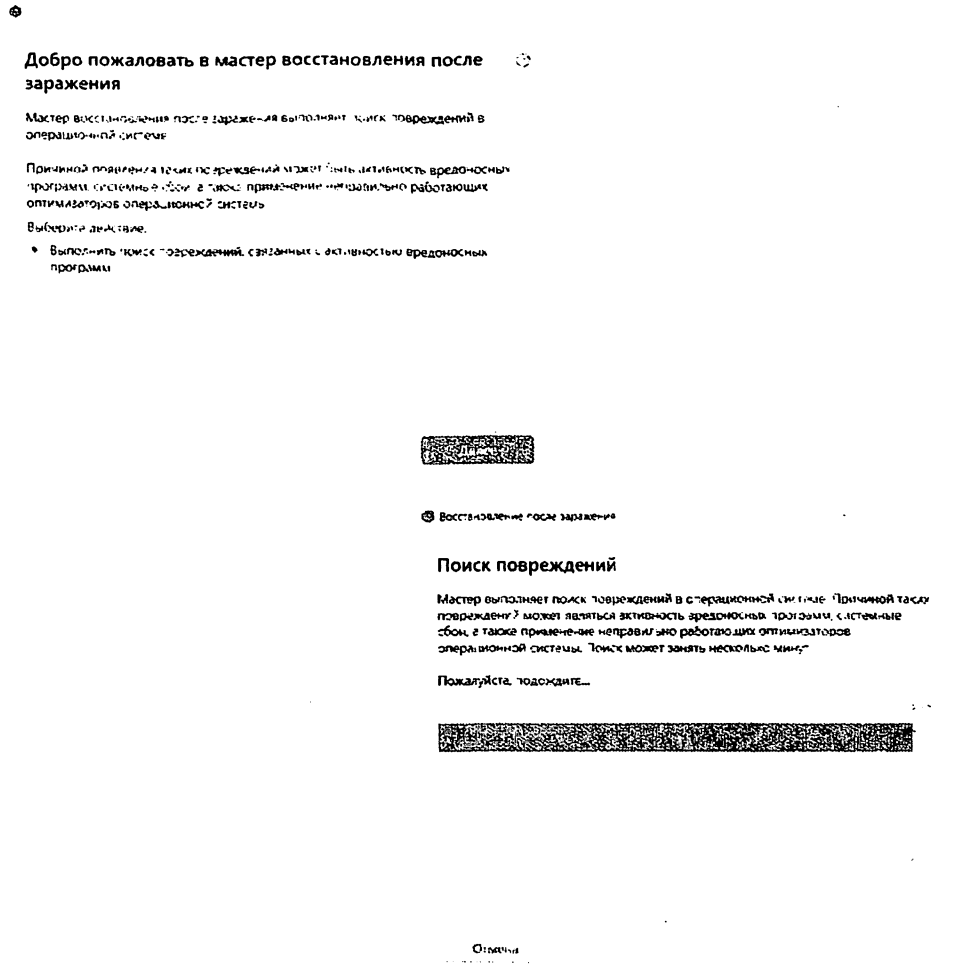


Рис.44. Мастер восстановления после заражения

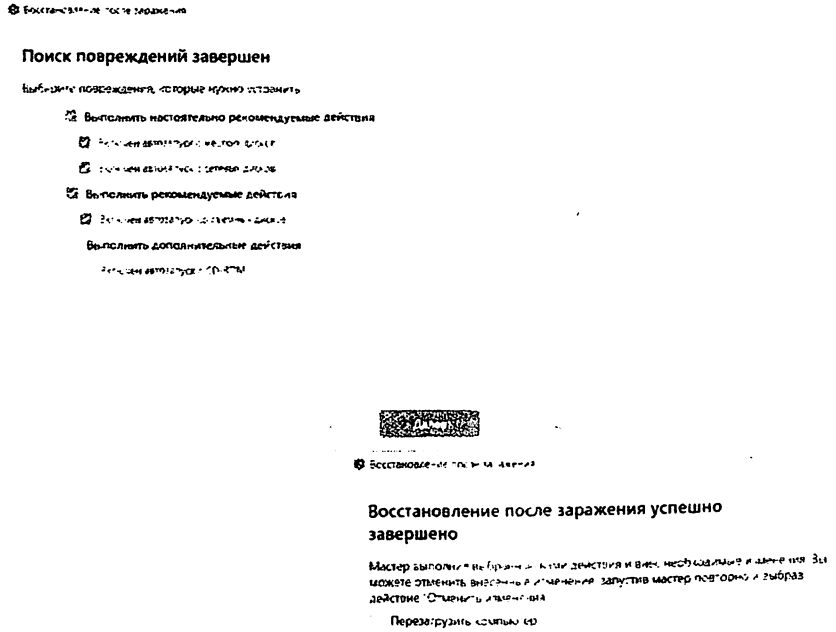
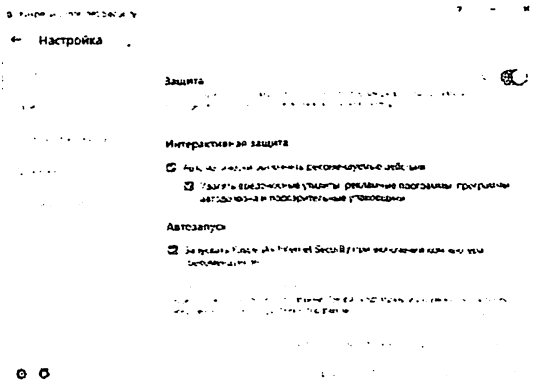


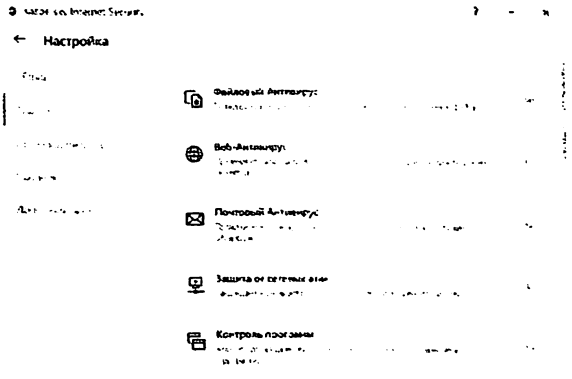
Рис.45. Восстановление после заражения

Настройка основных параметров.

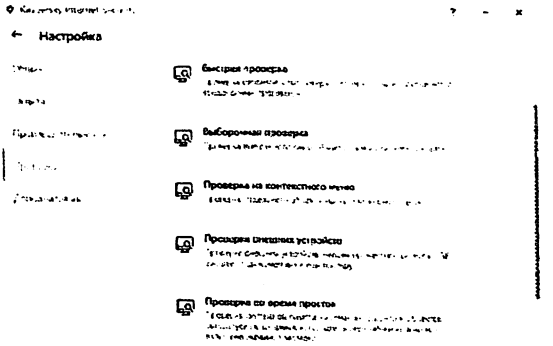
Чтобы ознакомится с дополнительными настройками, выберите значок «Настройки» внизу главной страницы. Через них можно настроить наш антивирус, временно отключить настройки, установить пароль для доступа к ней, установить различные ограничения (рис.46 (а,б,в,г,д).


Настройка
Защита
Интерактивная защита
Автозапуск

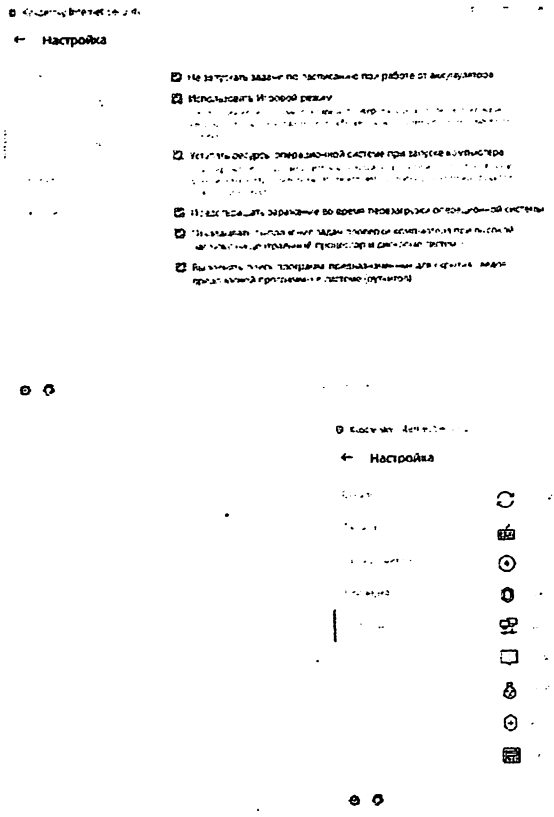
а)


Настройка
Файловый Антивирус
Веб-Антивирус
Почтовый Антивирус
Защита от сетевых атак
Контроль программ

б)


Настройка
Быстрая проверка
Выборочная проверка
Проверка из контекстного меню
Проверка внешних устройств
Проверка со время простоя

в)



г)

д)

Рис.46. Основные настройки антивируса

Задание:

1. Установка антивирусной программы.
2. Настройка основных параметров.
3. Сканирование жесткого диска.
4. Обновление антивирусной программы.

Контрольные вопросы:

1. Назовите основные виды вирусов и виды поиска вирусов.
2. Назовите основные виды антивирусных программ.
3. Перечислите основные настройки антивирусных программ.
4. Частота обновления антивирусных программ

Лабораторная работа №3
Защита от атак по локальным и глобальным сетям.

Цель работы:

Освоение навыков по установке и настройке межсетевого экрана для защиты данных от атак по локальным и глобальным сетям.

Порядок выполнения работы:

1. Установка и настройка параметров межсетевого экрана.
2. Создание разграничения доступа к сети.
3. Выполнение разрешенных и запрещенных действий в соответствии с настройками.

1. Установка и настройка параметров межсетевого экрана.

Сначала нужно посмотреть состояние межсетевого экрана из командной строки. Для этого нужно нажать комбинацию клавиш win + R. Затем ввести команду cmd и нажать Enter.

Перед нами откроется следующее окно. Вводим в него следующий код: "C:\Windows\System32> netshadvfirwall выключить состояние всех профилей" и нажимаем Enter (Рис.47.).

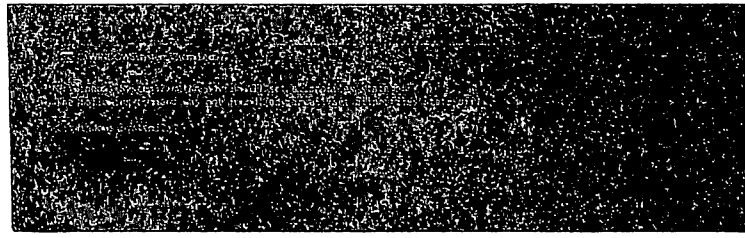


Рис.№47. Набор кода в CLI

Если мы заменим «состояние выключено» в конце кода на «состояние включено», мы активируем межсетевой экран (Рис.48.).

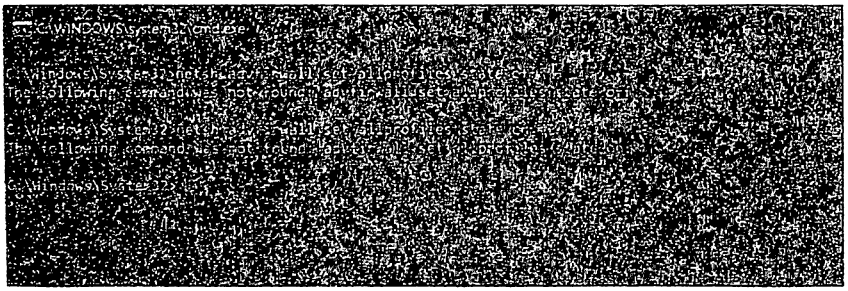


Рис.№48. Активирование межсетевого экрана

Чтобы открыть брандмауэр очень просто. Для этого нажмите кнопку «Пуск», введите в строке поиска «firewall» и нажмите клавишу. После этого откроется следующее окно(рис.49.).

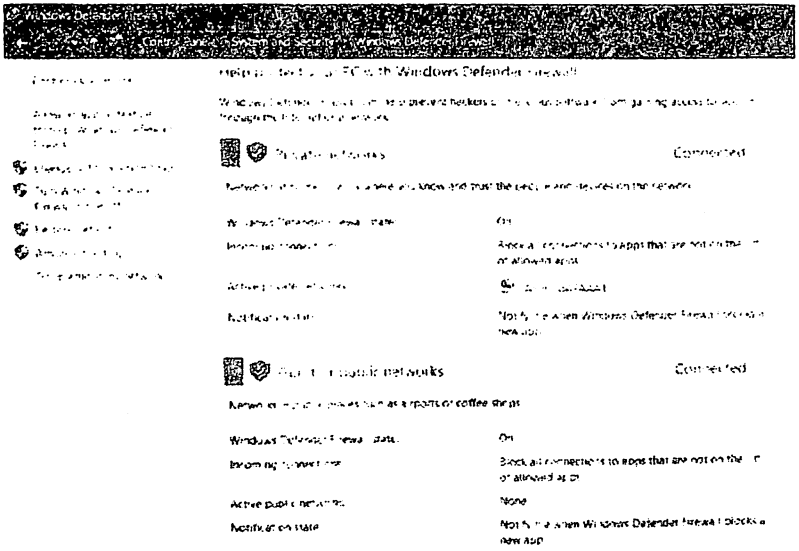


Рис.49. Главное окно Windows Defender Firewall

Здесь можно настроить основные настройки, а также для настройки дополнительных функций нужно перейти в раздел «Дополнительные функции» (рис.50).

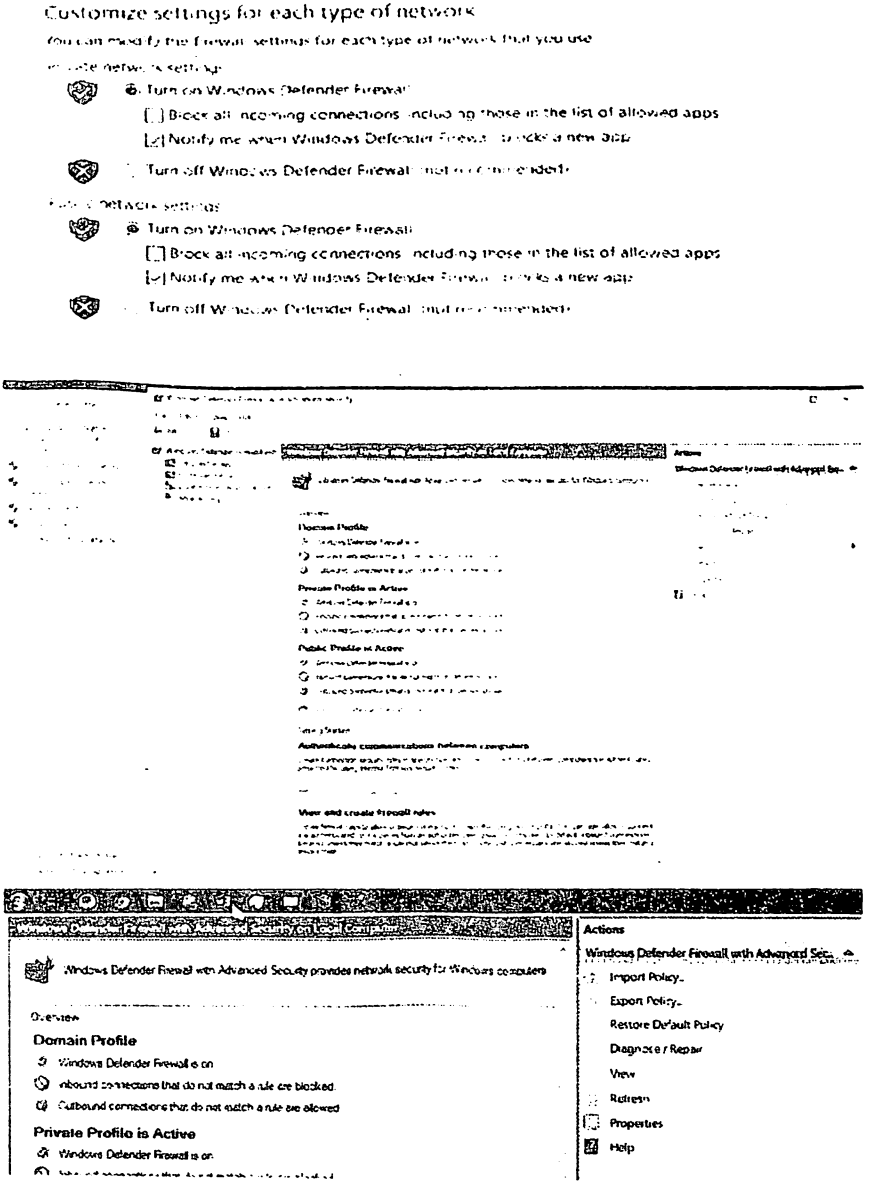


Рис.50. Основные и дополнительные настройки межсетевого экрана

2. Создание разграничения доступа к сети.

Следующие разделы доступны для установки ограничений для межсетевых экранов. В рисунке 51 показано как мы на исходящие подключения включаем: «Разрешить».

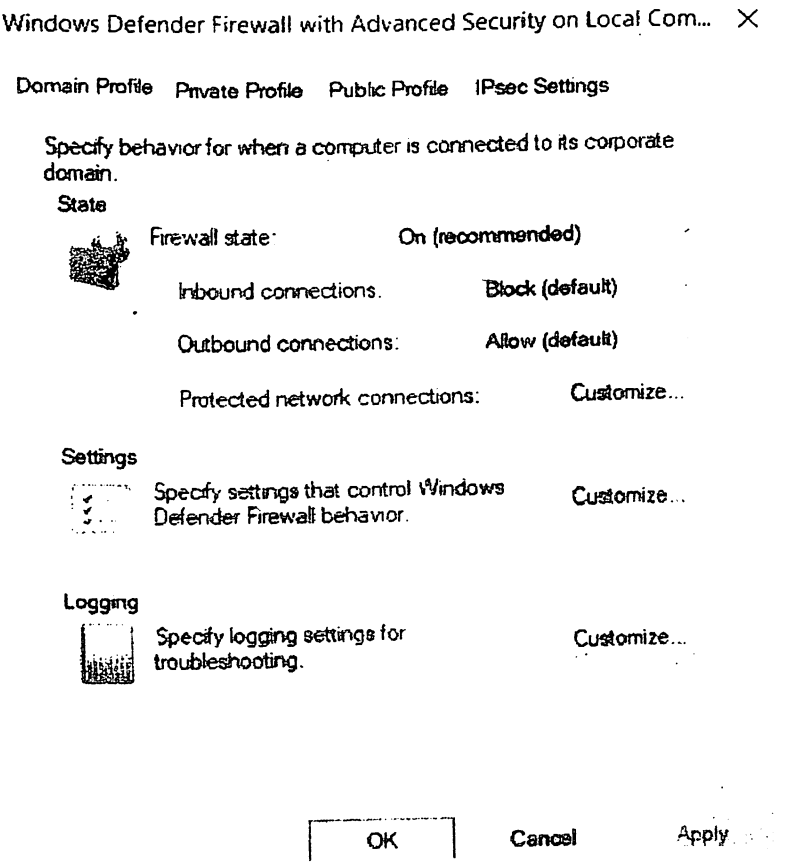


Рис.№51. Настройки по умолчанию

Теперь давайте изменим эту функцию на «Блокировать». Включение блокировки относится к профилю домена, частному профилю и общедоступному профилю (рис52).

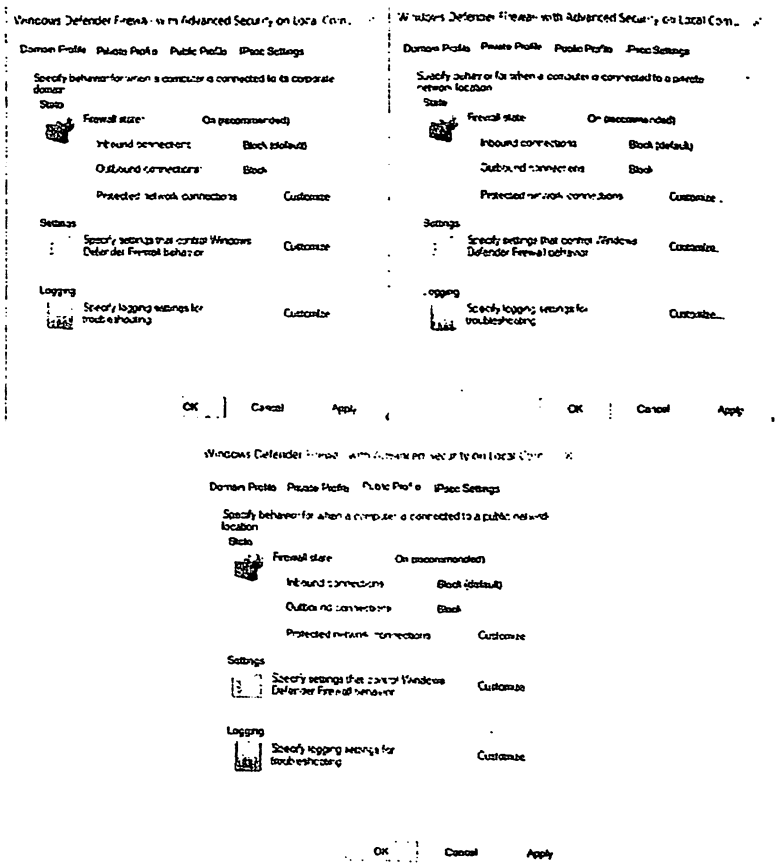


Рис.52. Состояние блокировки межсетевого экрана

3. Выполнение разрешенных и запрещенных действий в соответствии с настройками.

Межсетевой экран служит для повышения защищенности компьютера путем фильтрации входящего или исходящего трафика. С помощью него можно ограничить доступ в интернет всем кроме конкретных программ или разрешить соединяться с компьютером на котором он установлен только из внешней сети или только из внутренней сети, только по определенному порту, с определенных ip-адресов и т.д.

Межсетевой экран представляет собой набор правил. Правило это описание разрешения или запрета соединения. Могут быть входящими и исходящими, регулирующими соответственно доступ к этому компьютеру или с этого компьютера в сеть.

Например, если хотите чтобы Ваш сайт был доступен из внешней сети необходимо настроить правило Firewall.

Для этого нажимаем Win+R и вводим в командную строку firewall.cpl. После выбираем в левом столбце "Дополнительные параметры" (рис.53).

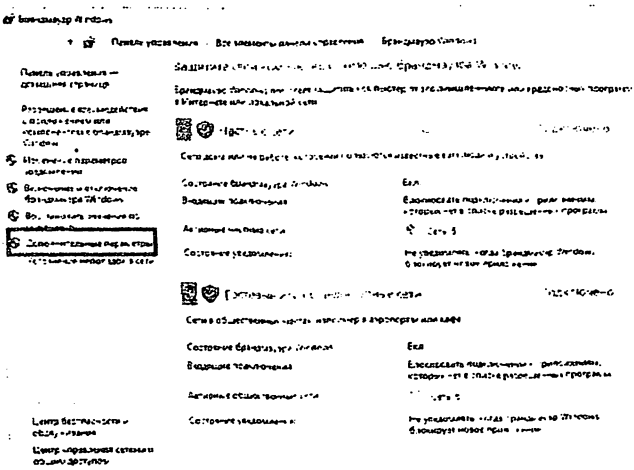


Рис. 53. Дополнительные параметры межсетевого экрана

В открывшемся окне повышенной безопасности нужно перейти в раздел "Правила для входящих подключений", после чего нажать "Создать правило" (Рис.54).

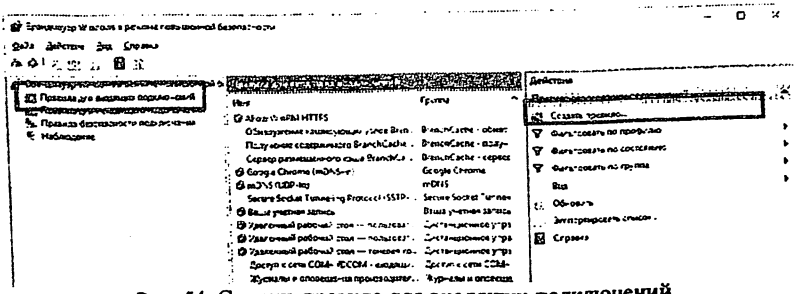


Рис. 54. Создать правило для входящих подключений.

Создадим правило для порта 80 (Рис.55.), также можно создать правило для конкретной программы или использовать стандартное правило для стандартных служб Windows. Можно также создать полностью настраиваемое правило.

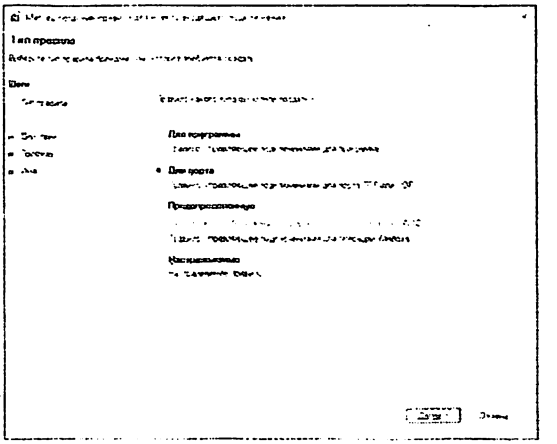


Рис. 55. Создание правило для порта.

Выберем тип протокола для фильтрации трафика, это может быть либо tcp либо udp, порт может быть любой или вообще можно открыть-закрыть все порты (рис.56).

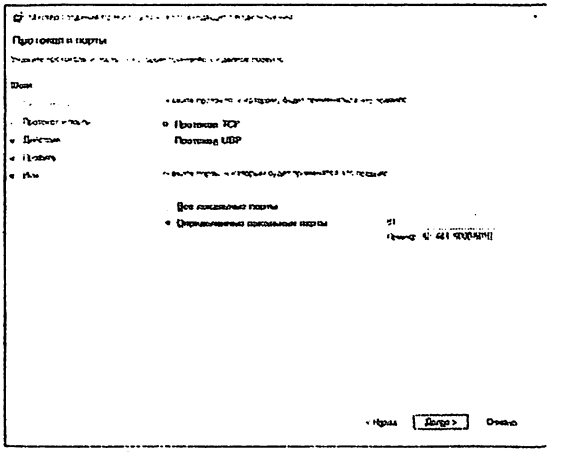


Рис. 56. Выбор типа протокола.

Далее определим что именно должно делать правило - разрешать или запрещать трафик по указанным нами на предыдущем шаге портам (рис.57).

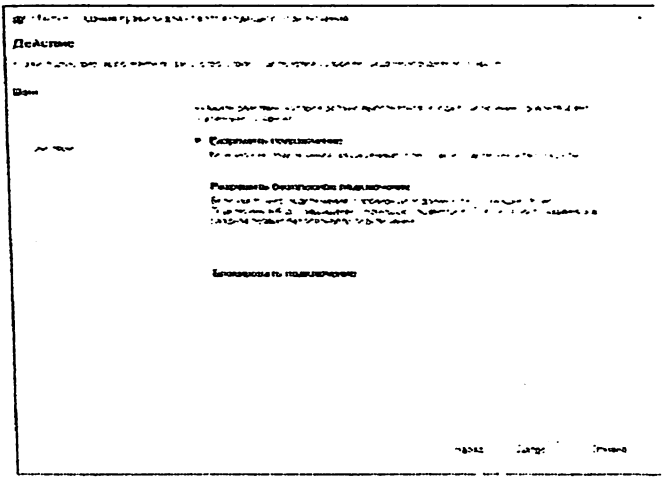


Рис. 57. Выбор действия, выполняемое при соответствии подключения условиям.

Укажем для какой сети должно применяться это правило. Доменной, частной или публичной (рис.58.).

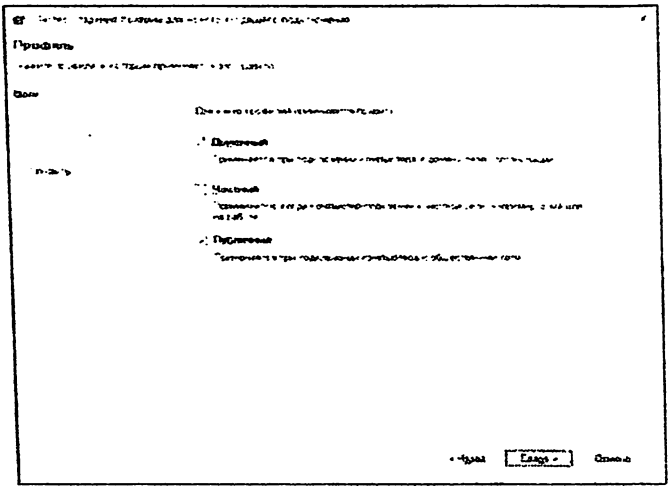


Рис. 58. Выбор профиля для применения правило.

На последнем шаге задайте имя правила. После этого можно соединяться по этому порту. Для проверки установленного лимита нужно

зайти в google chrome. Затем пройти по ссылке. Браузер не откроет введенный вами адрес и появится окно ниже. «Ваш доступ в Интернет заблокирован» означает, что право на использование Интернета заблокировано (рис.59).

Рис. 59. Интернет-соединение заблокировано.

Если отменить параметр блокировки, которое было установлено выше и обновить браузер, то можно увидеть, что браузер проходит по указанному адресу (рис.60-61).

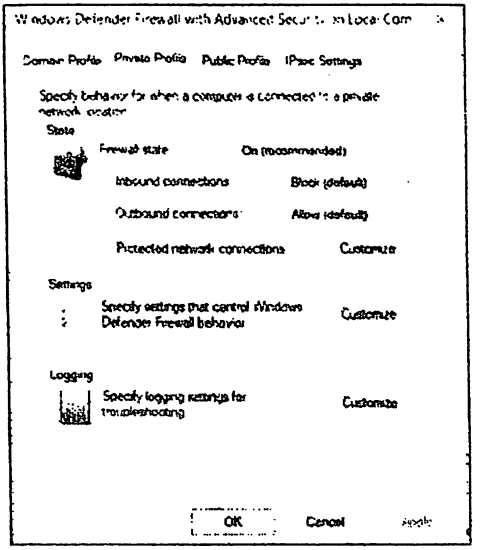


Рис. 60. Востановление параметров по умолчанию.

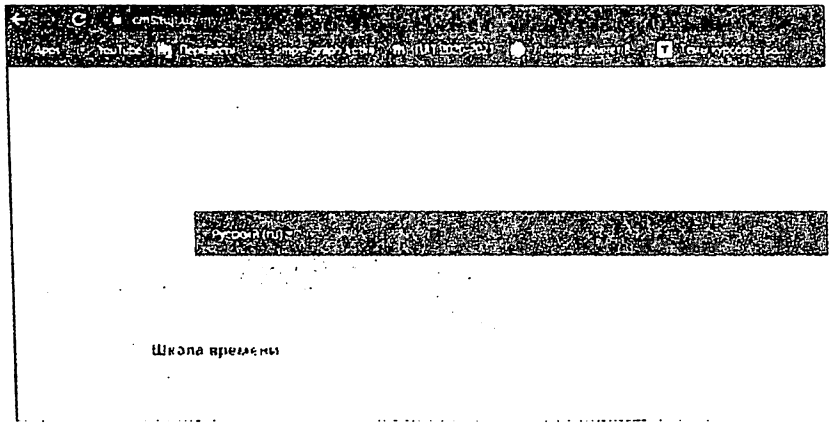


Рис. 61. Переход браузера по указанному адресу.

При создании ограничения или правило для программы, нужно перейти в раздел Outbound Rules (рис.62.).

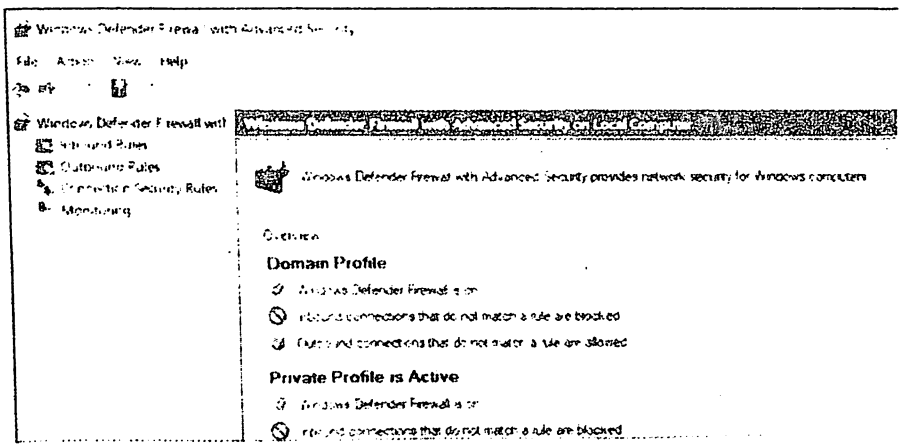


Рис. 62. Выбор раздела «Outbound Rules»

В строке «Действия» этого раздела нужно выбрать «Новые правила». Система запросить выбрать тип правило, которое нужно создать. Нужно выбрать раздел «Программа» и нажать кнопку «Далее» (рис.63).

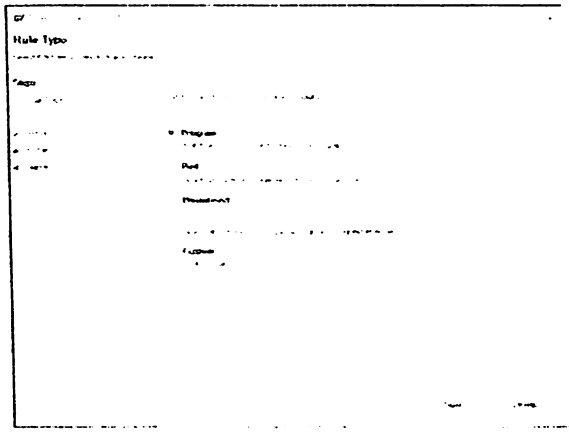


Рис. 63. Выбор типа создаваемого правило.

Откроется следующее окно. Через это окно можно создать правило для всех программ или для одной программы. Для этого выбираем «Этот путь к программе» и даем адрес exe-файла программы, в которой мы хотим создать правило. Для этого через кнопку обзор выбираем нужную программу (рис.64.).

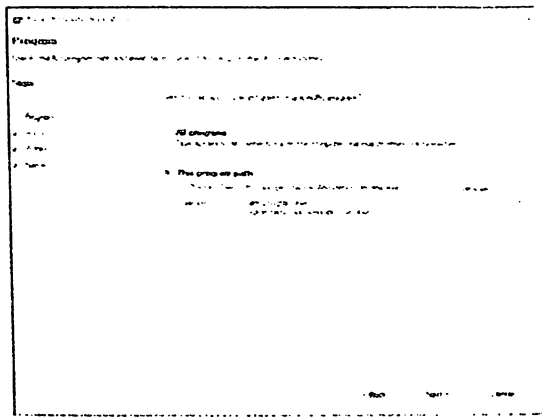


Рис. 64. Выбор нужной программы.

На следующем окне нужно выбрать действие, в нашем случае нужно выбрать «Заблокировать соединение» (рис.65). Затем выбираем профили относящиеся к создаваемого правило (рис.66).

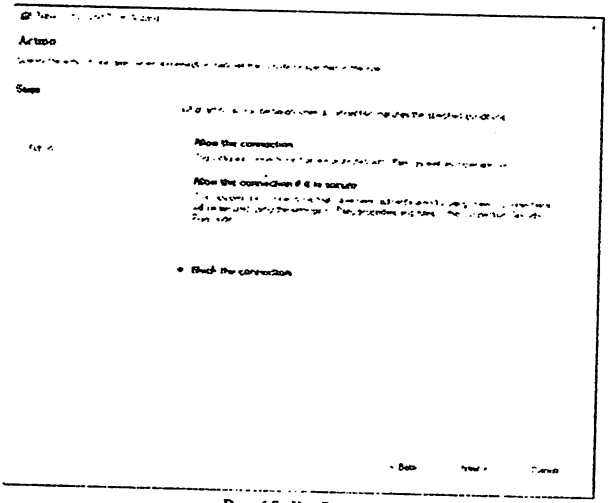


Рис.65. Выбор действия.

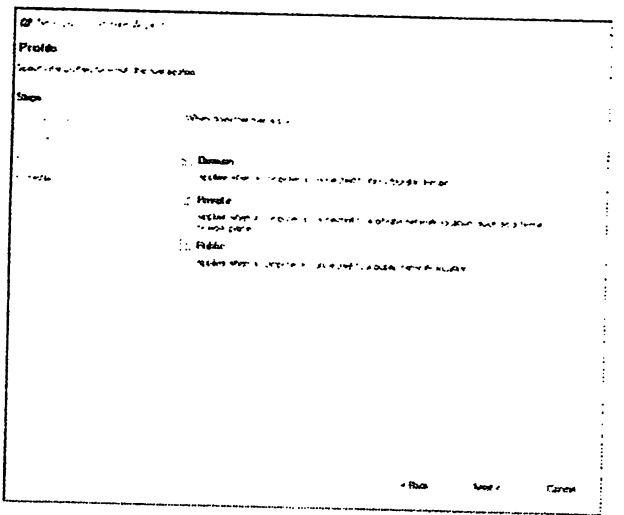


Рис.66. Выбор профиля.

Для окончания создаваемого правило нужно дать название к правилу и нажать на кнопку «Готово» (рис.67.).

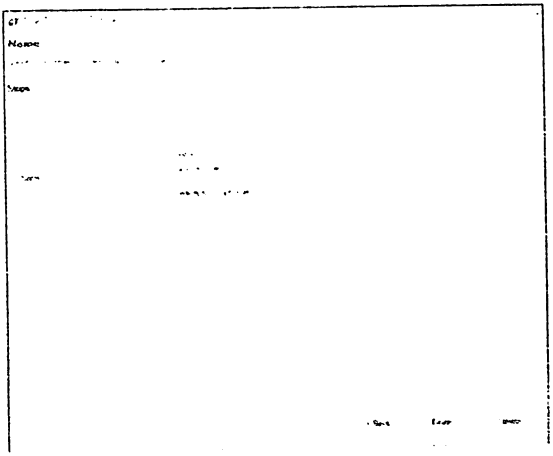


Рис. 67. Процесс названия правило.

Созданное правило будет в списке правил межсетевого экрана. Его можно скопировать, вырезать, удалить или редактировать в любое время (рис. 68.).

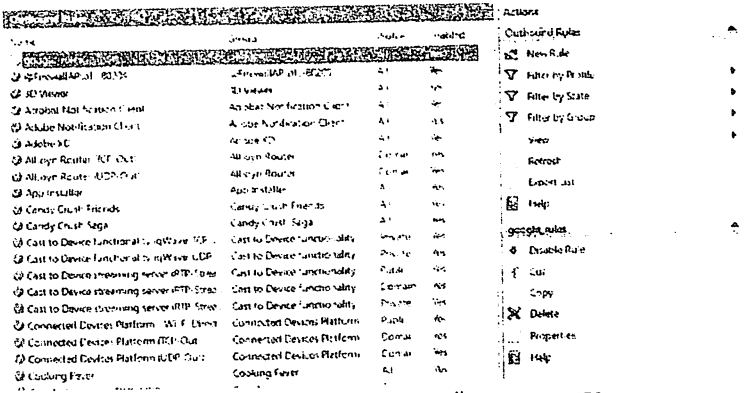


Рис. 68. Действия над созданной нами правило.

Чтобы удостовериться что созданное нами правило работает, открываем Google Chrome. Так как при создание мы блокировали работу этой программы, у нас появится окно с предупреждением о том что программа заблокирована межсетевым экраном (рис.69). Если удалить из

списка правил созданное правило, то программа по прежнему будет работать и откроет последнюю запрошенную страницу (рис.70).

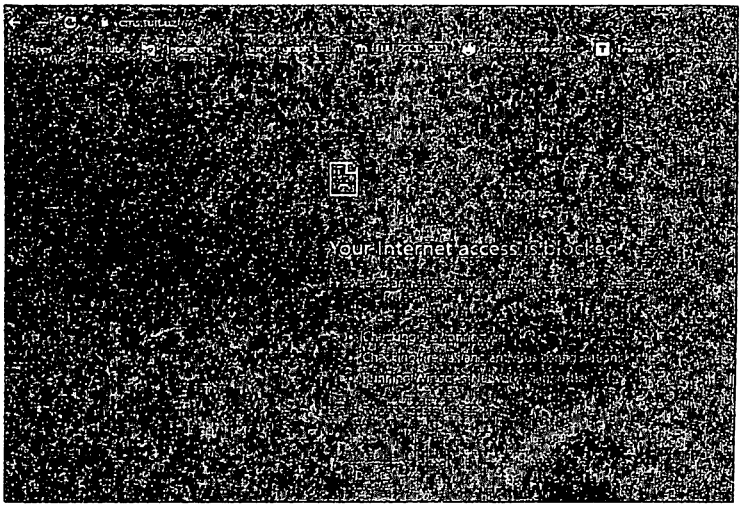


Рис. 69. Программа заблокирована межсетевым экраном.

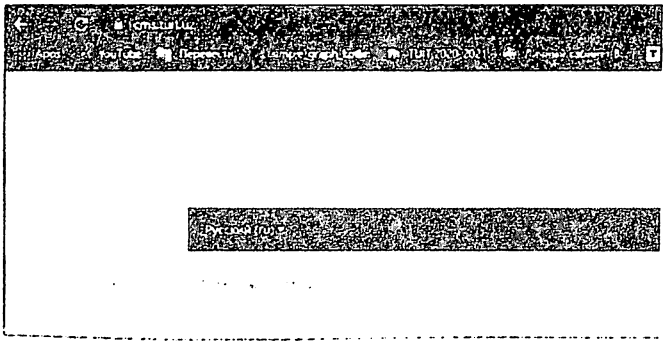


Рис. 70. Программа Google Chrome работает.

Задание:

1. Создать разграничение доступа к сети в межсетевом экране ОС Windows.
2. Выполнить разрешенных и запрещенных действий в соответствии с настройками.

3. Установить межсетевой экран «Outpost Firewall» и сравнить настройки с шататными средствами ОС Windows.
4. Сделать сравнительный анализ двух межсетевых экранов.

Контрольные вопросы:

1. Что такое межсетевой экран? Перечислите основные функции межсетевого экрана.
2. Выделите два основных типа межсетевых экранов.
3. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
4. Как создается правило для программ? Какие профили можно выбрать к созидаемой правиле?
5. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
6. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

Лабораторная работа №4

Использование клиентов электронной почты.

Цель работы:

Изучение специфики работы криптосистем с открытым ключом на примере программы «The Bat!»

Порядок выполнения работы:

1. Установка программы
2. Изучение дополнительных функций программы

The Bat! является коммерческим решением и доступен в двух версиях — Professional и Home, разнящихся количеством поддерживаемых функций. Профессиональная редакция продукта оснащена многоязычным интерфейсом, включает в себя возможность применять шифрование

информации, а также позволяет бесплатно использовать портативную защищенную версию программы — The Bat! Voyager. Мобильный вариант запускается с любого портативного накопителя (флешки, USB-диска и прочих) и может сослужить добрую службу разъездным сотрудникам в компаниях, часто работающим вне офиса и нуждающимся в защищенном удаленном доступе к корпоративным коммуникационным ресурсам.

1. Установка программы The Bat

Чтобы установить программу заходим в мастер установки программы The Bat, для продолжения установки нужно нажать кнопку «Next» (Рис.71).

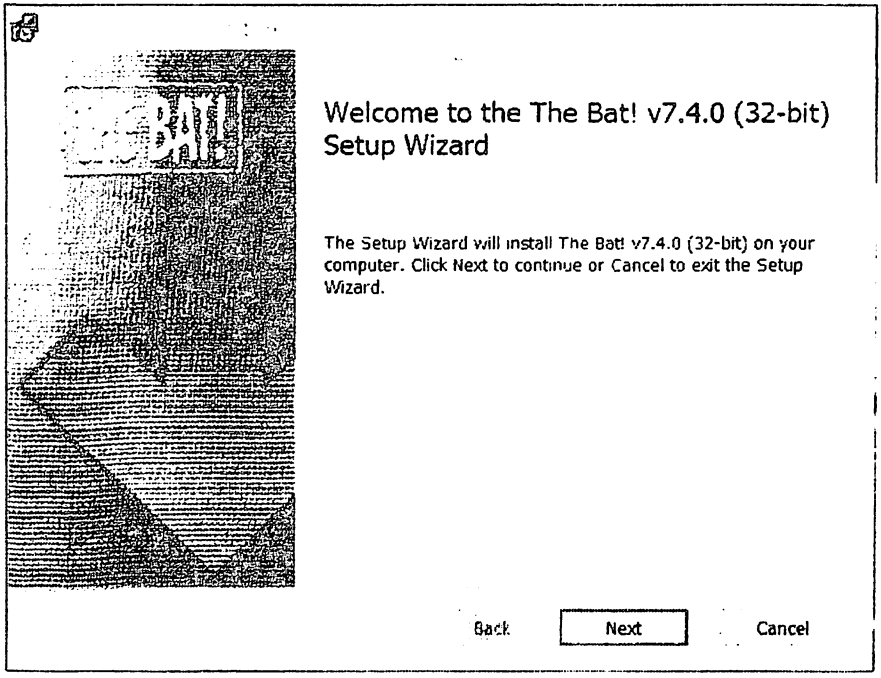


Рис.71. Мастер установки

Принимаем пользовательское соглашение, и переходим к следующему этапу (Рис.72).

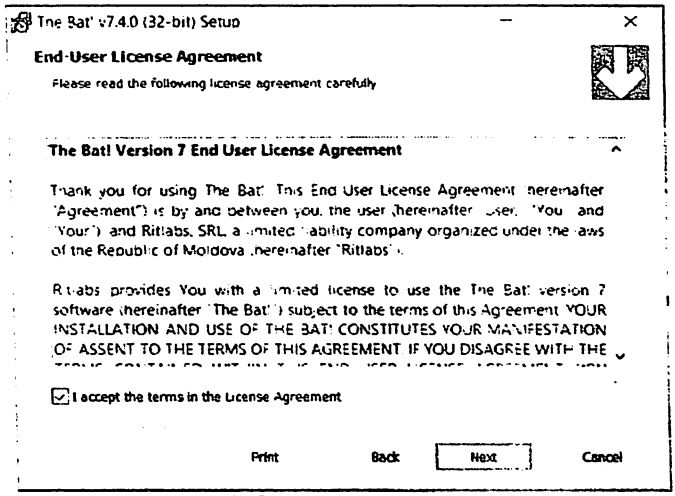


Рис. 72. Лицензионное соглашение

После этого мастер установки предлагает выбрать компоненты установки. Тут нужно ничего не менять и для продолжения нажать на кнопку «Next». Если же нужно устанавливать какой-либо определенный компонент надо снять галочку (Рис.73).

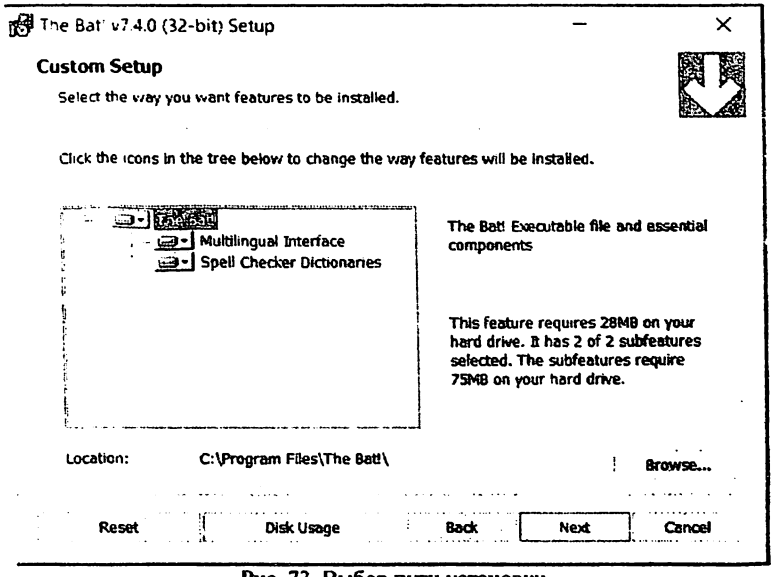


Рис. 73. Выбор пути установки

После прохождение этих этапов Мастер установки завершает сбор информации и готовится к процессу установки, для продолжения нажимаем кнопку «Next». Начинается процесс установки программы, который завершается появлением диалогового окна «Completed The Bat! Setup Wizard » и сообщением об успешной установке программы The Bat! Нажмите кнопку «Finish» для окончания установки (рис.74).

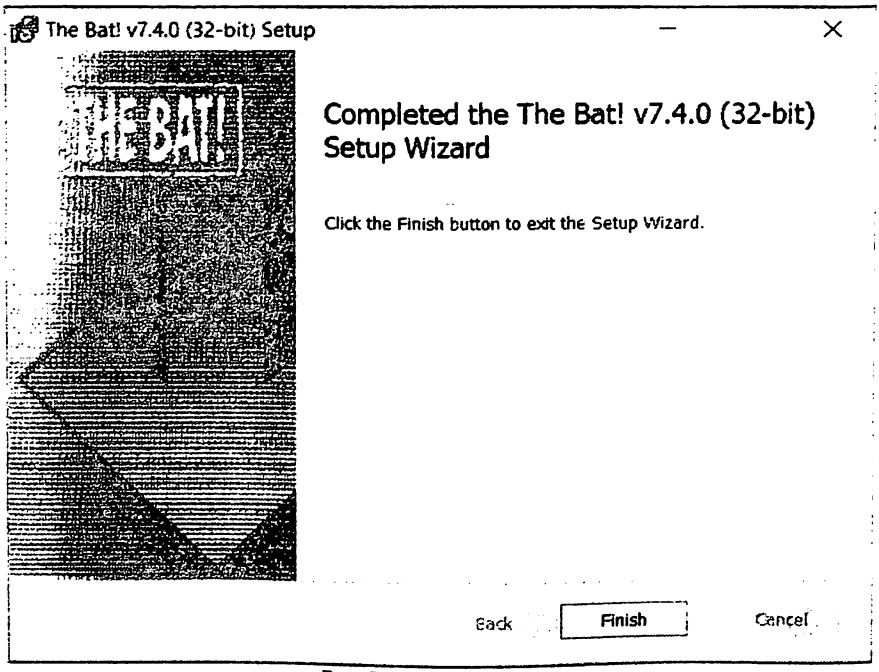


Рис. 74. Завершение установки

Чтобы никто кроме аутентифицированного пользователя не смог прочитать почту на компьютере нужно настроить параметры защиты данных при создании нового почтового ящика, то есть установить пароль. При настройке почты нужно ввести данные от заранее зарегистрированного почтового ящика и нажать кнопку «Далее» (рис.75.)

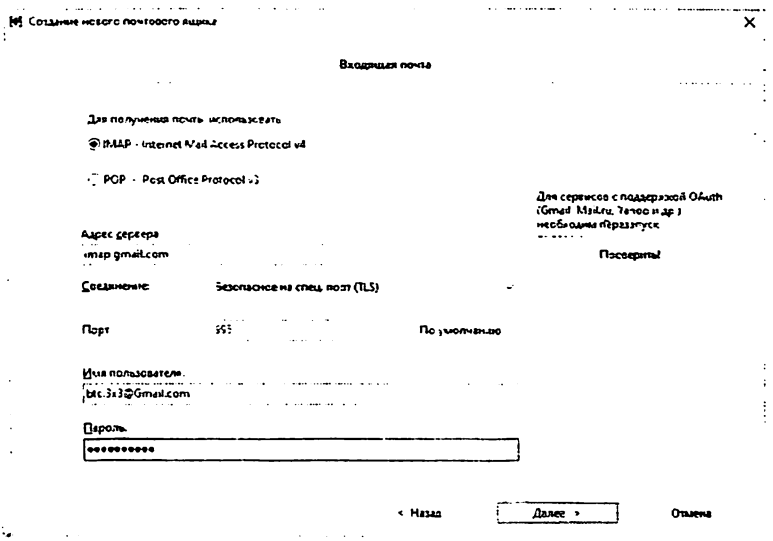


Рис. 75. Настройка Входящей почты

В окне «Исходящая почта» необходимо ввести данные от существующего почтового ящика, если не знаете то оставьте всё по умолчанию, а для продолжения нужно нажать «Далее» (рис.76).

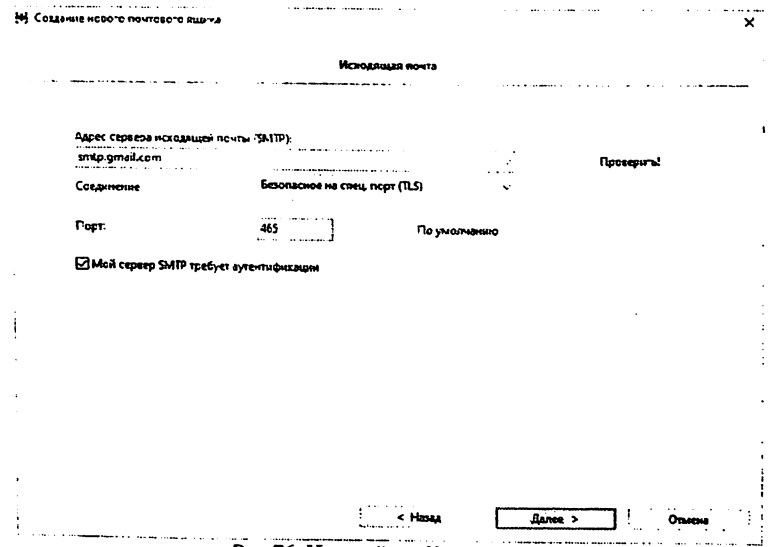


Рис.76. Настройка «Исходящей почты»

На последней стадии нужно ввести имя и электронный адрес почтового ящика и нажать кнопку «Готово» (Рис.77).

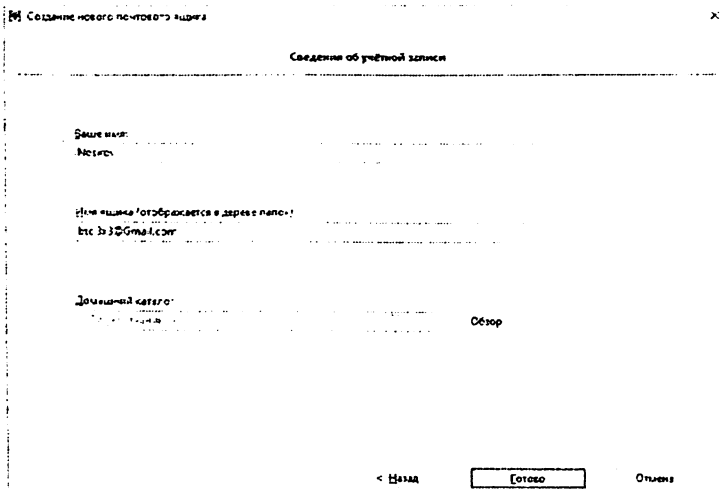


Рис.77. Завершение настройки

После нажатия кнопки готово, открывается главное окно программы, с подключенным почтовым ящиком, указанном при установке (Рис.78).

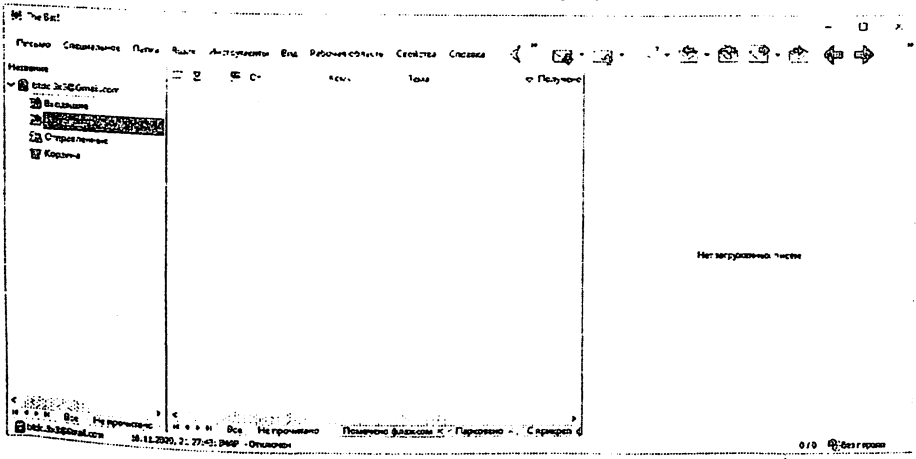


Рис.78. Главное окно программы

Для редактирования всех данных и настроек, нужно выделить почтовый адрес, затем нажать на меню «Ящик», далее «Свойства почтового ящика» (Рис.79).

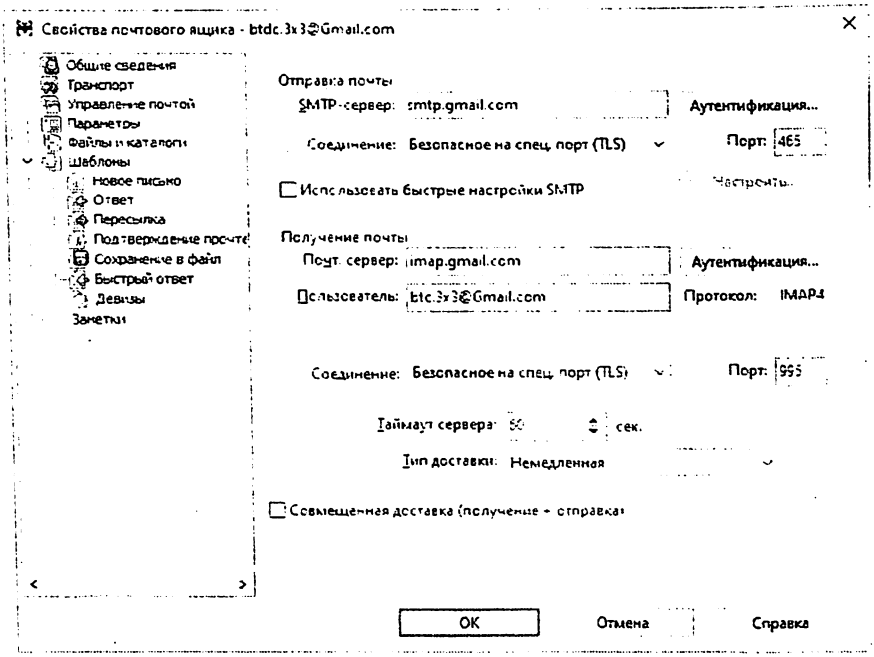


Рис.79. Свойство почтового ящика

2.Изучение дополнительных функций программы

Для связи с почтовыми серверами в The Bat! задействованы протоколы IMAP4, POP3 и SMTP с различными обеспечивающими безопасность связи методами аутентификации. Приложение поддерживает криптографические протоколы SSL и TLS различных версий, что позволяет клиенту взаимодействовать со всеми почтовыми сервисами, использующими шифрование сетевого трафика. Для большей защиты в The Bat! реализована поддержка аутентификации CRAM-MD5 с аппаратным USB-токеном, доступная в Professional-редакции почтового клиента и исключающая доступ

неавторизированных пользователей к учетной записи на почтовом сервере (Рис.80).

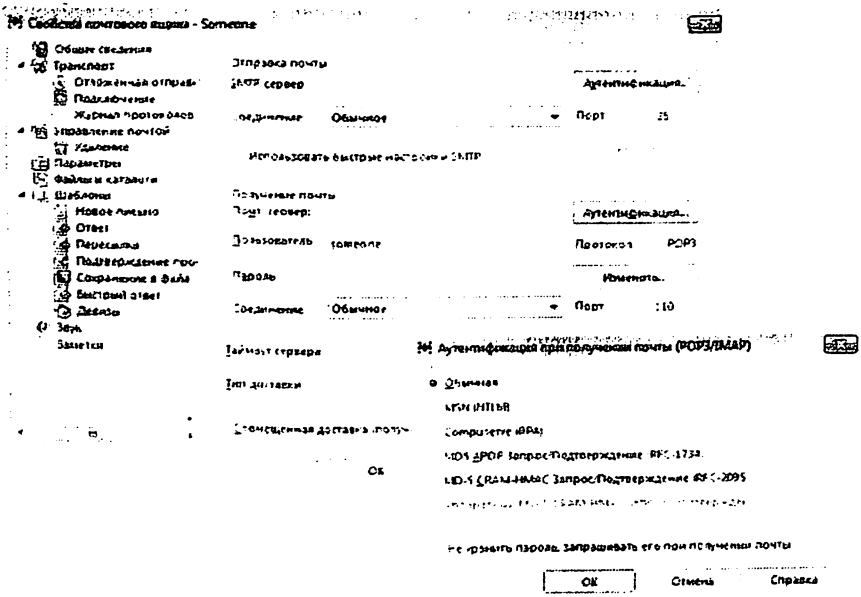


Рис.80. Поддержка протоколов аутентификации и шифрования при работе с почтовыми серверами

В The Bat! возможно не только использовать защищенные каналы связи, но и отправлять и принимать зашифрованные с помощью S/MIME, PGP и OpenPGP письма, а также подписывать их электронной подписью. В первом случае обеспечивается конфиденциальность email-переписки и безопасное хранение корреспонденции на почтовом сервере (в случае его взлома или перехвата писем злоумышленники не смогут прочесть сообщения), во втором — помимо идентификации отправителя гарантируется, что любая попытка изменить письмо на пути к получателю может быть легко выявлена. Соответствующий инструментарий расположен в окне редактирования писем в меню «Криптография и безопасность». Работу с ним можно осуществлять как в ручном режиме, так и в

автоматическом. Дополнительные сведения по данному вопросу представлены в прилагаемой к почтовому клиенту документации (Рис.81.).

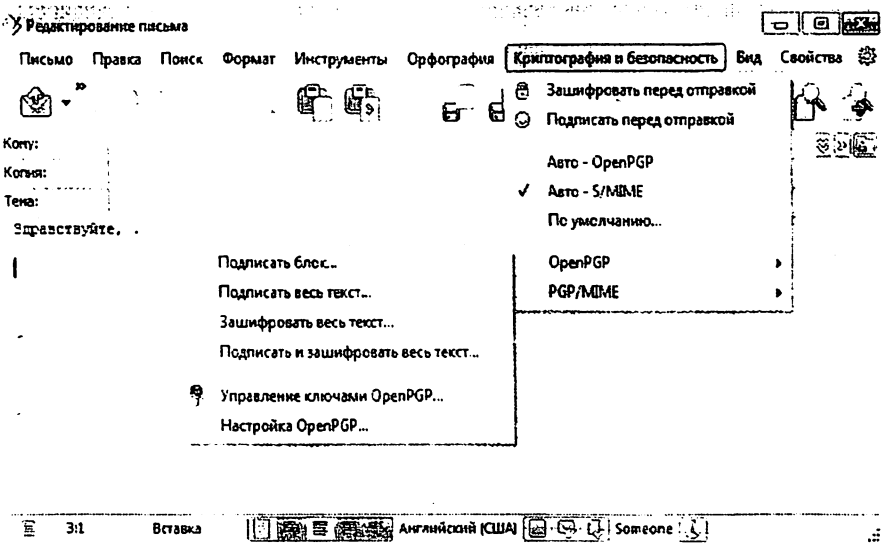


Рис.81. Использование криптографии при отправке почты.

Также в The Bat! имеется возможность защитить паролем почтовый ящик, что особенно полезно в многопользовательском окружении, когда почтовым клиентом пользуются несколько человек. Сделать это можно в меню «Ящик → Установить пароль». Важно понимать, что использование данной функции ограждает ящик от визуального просмотра, но не защищает саму почтовую базу, которую при желании можно прочитать любым текстовым редактором. Для исключения таких случаев в The Bat! Professional предусмотрено шифрование локальных файлов почтовых баз, адресных книг и файлов конфигурации в режиме реального времени. Включение механизма шифрования осуществляется после установки программы на стадии настройки. Защищать данные можно паролем либо USB-токенами Aladdin eToken и Rainbow iKey1000 (Рис.82.).

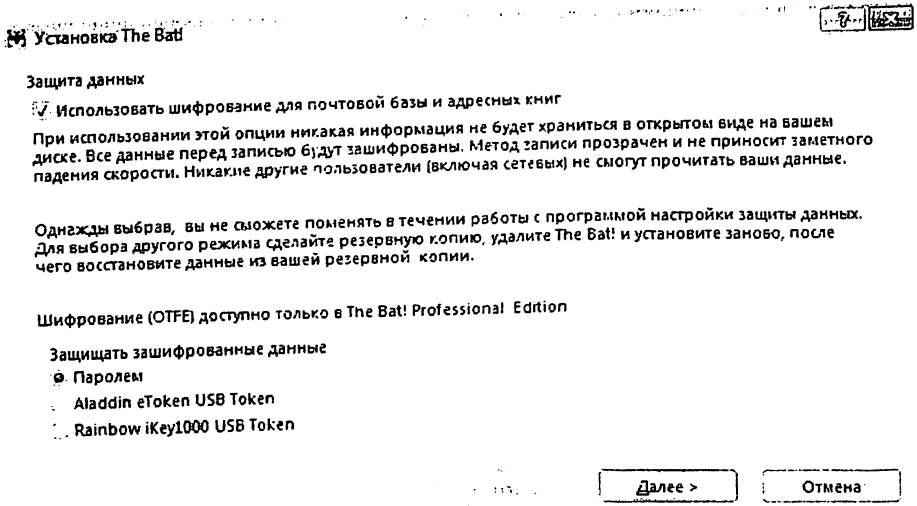


Рис.82. Использование шифрование для почтовой базы и адресных книг.

Обратной стороной защиты почтовых баз посредством шифрования становится сложность их восстановления в случае непредвиденного сбоя компьютера или утери ключа доступа к электронной переписке, которая является жизненно важным компонентом деловой активности любого человека. Во избежание потери писем и содержащейся в них информации в The Bat! предусмотрены средства резервного копирования и восстановления данных.

Все настройки программы и email-ящиков, адресные книги и почтовые папки могут быть сохранены в отдельном файле и затем восстановлены из резервной копии в случае нежелательного изменения информации или потери данных. Архив можно снабдить комментарием и защитить паролем (в этом случае содержимое резервной копии будет зашифровано). Кроме того, The Bat! позволяет создавать отдельные бекапы для каждого почтового ящика или папки, а также при помощи планировщика автоматизировать процесс резервного копирования (Рис 83.).

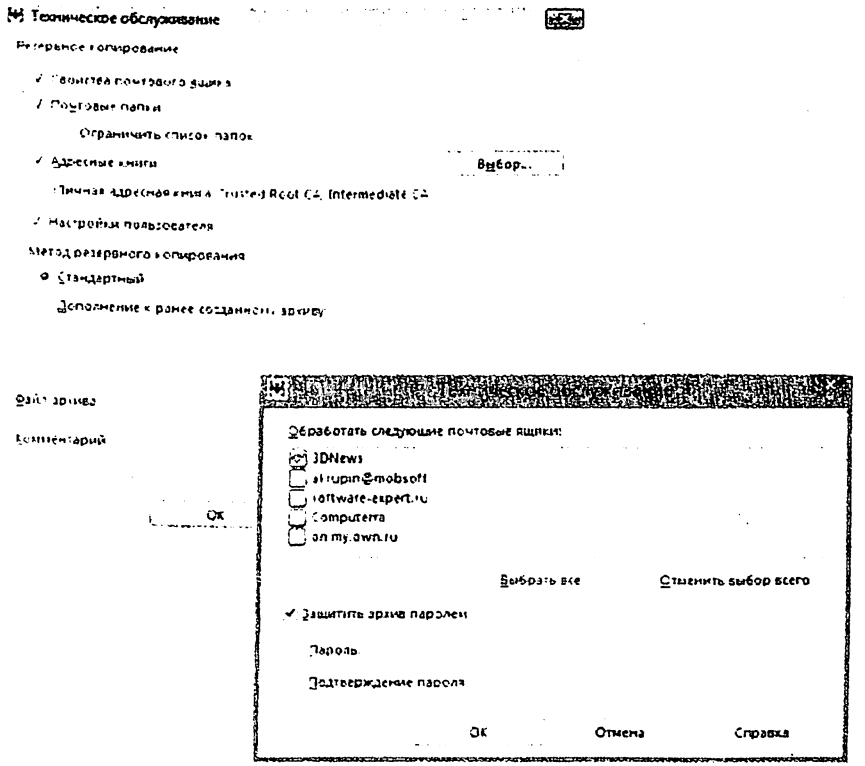


Рис. 83. Сервис резервного копирования и восстановления

Отдельного упоминания заслуживают реализованные в почтовом клиенте средства защиты от вирусных атак и вредоносного программного обеспечения. В отличие от многих других инструментов для работы с email-корреспонденцией, The Bat! никогда не открывает прикрепленные файлы автоматически, не исполняет скрипты и не подгружает картинки с удаленных серверов без разрешения пользователя. Встроенный в приложение URL-менеджер анализирует скачиваемые при просмотре HTML-писем изображения и, исходя из опасности хоста и выставленных пользователем правил, блокирует либо разрешает загрузку графического контента. Такая избирательность помогает бороться с вставляемыми в изображения вредоносными кодами и не позволяет третьим лицам отслеживать действия

пользователя. Важной особенностью является то, что The Bat! не скрывает тип присоединенных файлов. Если присоединенный файл имеет двойное расширение, например photo.jpg.exe, почтовый клиент акцентирует на этом внимание пользователя и выдаст дополнительное предупреждение. Инструмент для управления загрузкой изображений предоставляет пользователю возможность выборочной загрузки, блокировки и создания собственных правил (Рис.84.)

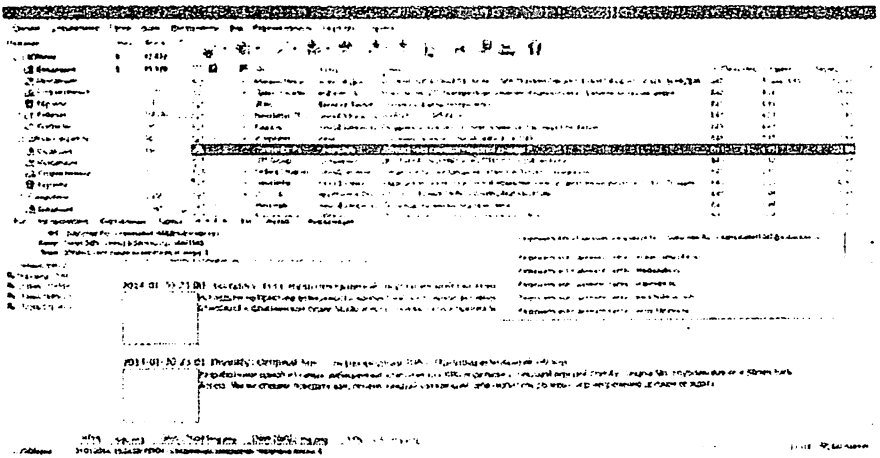


Рис.84. Инструмент управления загрузкой.

Помимо защиты пользователя от случайного открытия вредоносных прикрепленных файлов, The Bat! предлагает возможность использования модулей расширения (плагинов) для защиты от зловредного ПО и нежелательной корреспонденции. Посредством дополнительных компонентов можно наладить сканирование входящей почты для выявления вирусов и спама, настроить выборочную проверку вложенных в письма файлов, задать автоматическое удаление вредоносной и мусорной корреспонденции. Оставлять без внимания упомянутые модули расширения не стоит, поскольку в последнее время деятельность спамеров,

занимающихся массовыми рассылками нежелательных контентов, приобретает всё более криминальный характер. Даже опытным интернет-пользователям следует быть очень внимательными, чтобы не попасться на уловку мошенников.

Для выстраивания системной и глубоко эшелонированной обороны от злоумышленников и распространяемого при помощи почты вредоносного софта, в The Bat! предусмотрено немало других защитных решений. Программа предлагает использование собственного механизма просмотра HTML и собственный модуль просмотра изображений, что защищает от вирусов, направленных на использование брешей в операционной системе Windows (Рис. 85.). В дополнение к этому в программе задействует технологии Address space layout randomization (ASLR) и Data Execution Prevention (DEP), значительно усложняющие эксплуатацию нескольких типов уязвимостей. Кроме того, вся обработка данных производится исключительно в памяти программы, и поэтому они никогда не появляются на диске в незашифрованном виде.

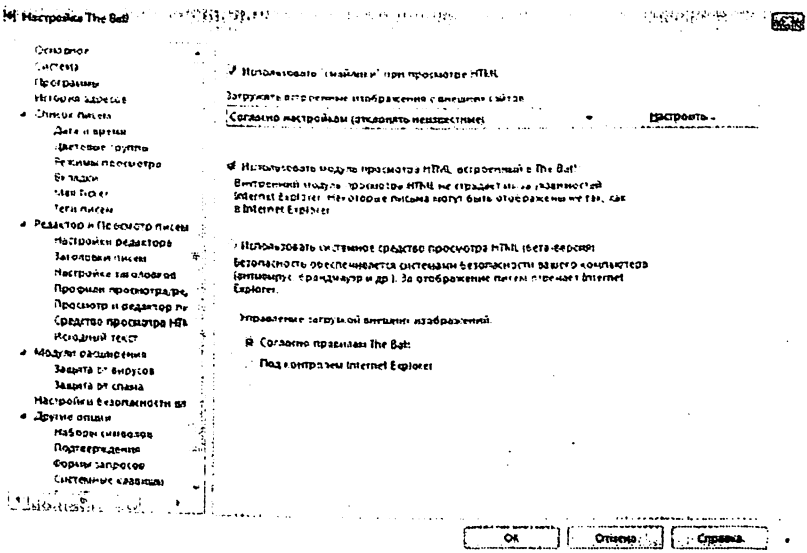


Рисунок 85. Настройка модуля просмотра HTML

Ещё одна сторона безопасности The Bat! — автономная адресная книга (Рис.86.), функционирующая независимо от Microsoft Outlook, Outlook Express и прочих почтовых клиентов, которые часто подвергаются атакам со стороны злоумышленников с целью кражи контактной информации. Используемый программой формат хранения данных совместим с vCard (VCF) и LDIF, что позволяет сохранять в адресной книге значительно больше сведений о человеке, чем просто его имя и электронный адрес. А именно: пол адресата, дату рождения, домашний адрес, место работы, шаблоны для писем к этому человеку и многое другое, включая его фотографию и используемые для безопасной переписки сертификаты. Контакты можно структурировать и объединять в группы, поддерживающие массовую рассылку писем с использованием шаблонов. Поддержка групп может широко использоваться в деловой среде для организации оперативного взаимодействия с другими отделами и подразделениями компании.

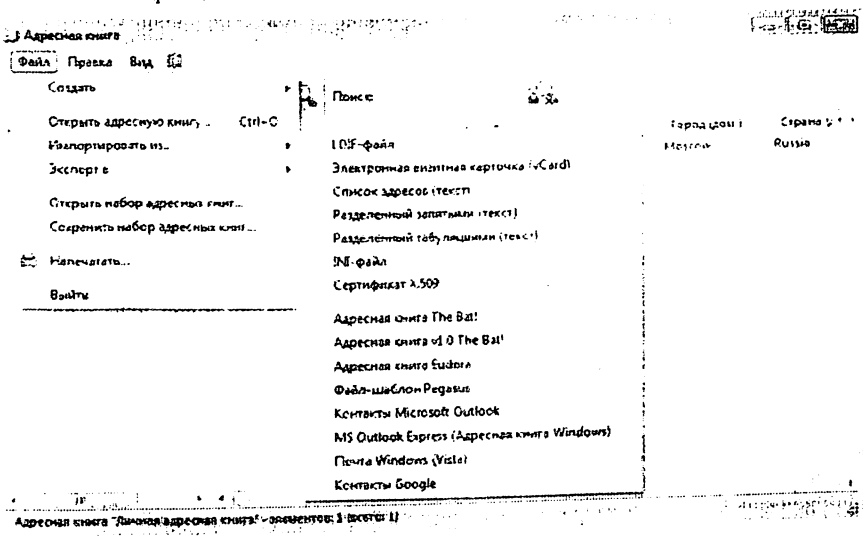


Рис.86. Адресная книга The Bat!

В числе прочих особенностей The Bat!, которые также могут быть востребованными среди рядовых и корпоративных пользователей, являются

вышеупомянутые средства фильтрации и сортировки писем. С их помощью можно не только автоматически распределять входящую, исходящую, прочитанную и обработанную корреспонденцию по соответствующим папкам, но и бороться со спамом посредством простейшей методики, предполагающей отделение писем родственников, друзей, знакомых, деловых партнеров и прочих присутствующих в адресной книге лиц от общего email-потока. Сортировщик писем позволяет автоматизировать обработку сообщений: настроить автоответ, запуск внешнего приложения, добавить адресатов в адресную книгу, экспортировать или архивировать сообщения, извлечь присоединенные файлы и многое другое вплоть до создания событий в планировщике и отправки писем на печать. Для автоматической обработки корреспонденции в The Bat! применяется встроенный сортировщик (Рис.87.)

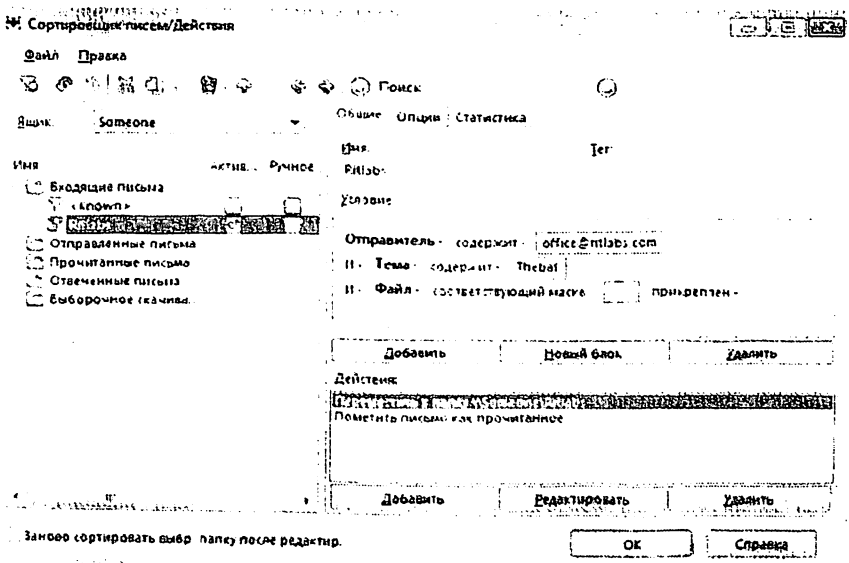


Рис. 87. Сортировщик писем.

Сильной стороной сортировщика писем The Bat! является наличие набора правил «Выборочное скачивание», позволяющих удалить письмо или оставить его на почтовом сервере, не дожидаясь загрузки. Используя

Нужно ввести значение 2 и убедится, что стоит шестнадцатеричная система исчисления, затем нажать ОК. Теперь служба Защитника Windows запустится автоматически.

Затем нужно повторить аналогичное действие для службы WdNisSvc (Служба инспектирования Защитника Windows).

Сохраните изменения и перезагрузите компьютер в обычном режиме, теперь Защитник Windows должен работать корректно.

Если Защитник Windows не может запуститься, сначала нужно запустить Rkill, а затем выполнять полное сканирование с помощью программы Malwarebytes Anti-Malware без перезагрузки компьютера.

Сканирование жесткого диска. Существует 3 метода сканирования файлов.

1. Быстрое сканирование
2. Полное сканирование
3. Выборочное сканирование

Для *«Быстрого сканирования»* откройте Windows Defender и нажмите кнопку Сканировать (рис. 27.).

Для *«сканирования всего компьютера (полное сканирование)»* откройте Windows Defender и щелкните стрелку рядом со Сканировать и выберите Полная проверка.

«Сканирование определенных мест (выборочное сканирование)». С помощью программы Windows Defender можно сканировать не весь компьютер, а только определенные места. Однако если Defender найдет шпионское или потенциально нежелательные программы, будет выполнено быстрое сканирование, чтобы удалить обнаруженные элементы в других местах (если требуется). Для это откройте Windows Defender и щелкните стрелку рядом со Сканировать и выберите Выборочное сканирование.

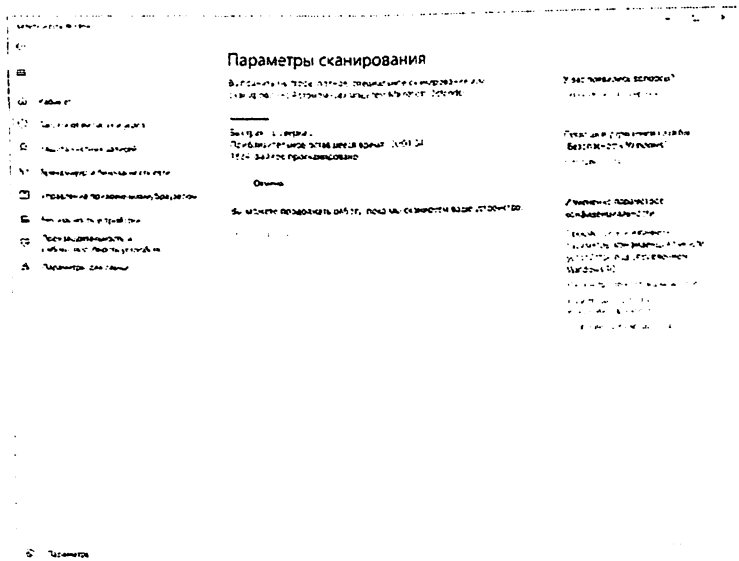


Рис.27. Параметры сканирования. Быстрое сканирование.

После этого выберите Сканирование выбранных дисков и папок и нажмите кнопку Выбрать. Задайте диски и папки для сканирования и нажмите кнопку ОК.

При обнаружении вредоносной программы, в верхней правой части экрана появляется сообщение (всплывающее уведомление) Вам не требуется что-либо предпринимать, т.к. Защитник Windows автоматически удаляет или отправляет в карантин найденные угрозы.

Всплывающее оповещение закрывается автоматически. Если другие сообщения не появляются, ваш компьютер был очищен успешно (рис.28.).

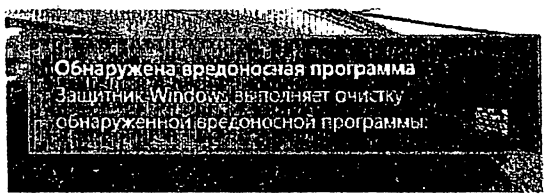


Рис.28. Всплывающее уведомление

3. Как развитая система обнаружения вторжения.

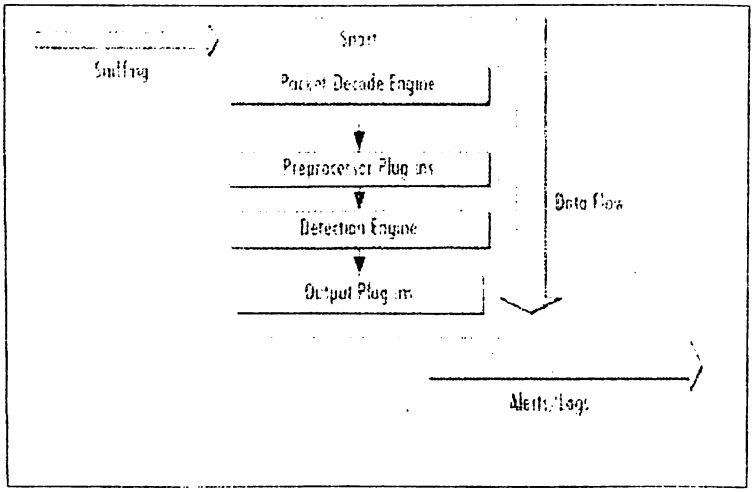


Рис.88. Принцип работы Snort

1. Установка программы

Основной сайт для Snort - http://www.snort.org. Snort распространяется согласно лицензии GNU GPL автором Мартином Рошом. После загрузки архива, нужно разархивировать его в каталог snort-1.7:

root @lord]# tar -zxvf snort-1.7.tar.gz

После загрузки libpcap, разархивируйте его подобным образом. Войдите в каталог libpacp, и выполните следующие шаги:

root @lord]# ./configure root @lord]# make

Теперь, нужно компилировать Snort. Для этого нужно войти в каталог, в котором находится Snort, и выполнить следующую команду:

root @lord]# ./configure --with-libpcap-includes=/path/to/libpcap/ { in my case it was :*

root@lord./configure--with-libpcap-includes=/home/dood/libpcap}
root @lord]# make root @lord]# make install

Snort теперь установлен на вашем компьютере. Теперь нужно создать директорию, в которой Snort будет хранить файлы регистрации:
root @lord]#mkdir /var/log/snort

И чтобы подтвердить где установлена программа нужно выполнить:
root @lord]# whereis snort

Архитектура Snort состоит из трех основных компонентов, которые могут быть описаны как:

1. *Дешифратор пакетов*: готовит перехваченные пакеты в форму типа данных, которые затем могут быть обработаны механизмом обнаружения. Дешифратор пакетов может регистрировать Ethernet, SLIP и PPP пакеты.
2. *Механизм Обнаружения*: анализирует и обрабатывает пакеты, поданные к нему "Дешифратором", основываясь на правилах Snort. Сменные модули могут быть включены в механизм обнаружения, чтобы увеличить функциональные возможности Snort.
3. *Logger/Alerter*: Регистратор позволяет вам регистрировать информацию, собранную дешифратором пакетов в удобочитаемом формате. По умолчанию файлы регистрации сохранены в каталоге :/var/log/Snort.
   Механизм предупреждения посылает предупреждения к syslog, файлу, Unix sockets или базе данных. По умолчанию, все предупреждения сохранены в файле: /var/log/Snort/alerts.

2. Изучение программы и его режимы

В этом разделе мы обсудим концепции и команды SNORT в подробностях. Начнем с простой команды, которая отображает все ключи программы:
root@lord snort -?

Команда выдаст следующее:

-> Snort! <*-*
Version 1.7
By Martin Roesch (roesch@clark.net, www.snort.org)
USAGE: snort [-options]
Options:
-A Set alert mode: fast, full, or none (alert file alerts only)
'unsock' enables UNIX socket logging (experimental).
-a Display ARP packets
-b Log packets in tcpdump format (much faster!)
-c Use Rules File
-C Print out payloads with character data only (no hex)
-d Dump the Application Layer
-D Run Snort in background (daemon) mode
-e Display the second layer header info
-F Read BPF filters from file
-g Run snort gid as 'gname' user or uid after initialization
-h Home network =
-i Listen on interface
-l Log to directory
-n Exit after receiving packets
-N Turn off logging (alerts still work)
-o Change the rule testing order to Pass|Alert|Log
-O Obfuscate the logged IP addresses
-p Disable promiscuous mode sniffing
-P set explicit snaplen [sp? -ed.] of packet (default: 1514)
-q Quiet. Don't show banner and status report
-r Read and process tcpdump file
-s Log alert messages to syslog

Как уже говорилось, SNORT выполняется в трех различных режимах:

1. *Режим пакетного снифера* : Когда Snort работает в этом режиме, он читает и дешифрует все сетевые пакеты и формирует дамп к stdout (ваш экран). Для перевода Snort в режим сниффера используйте ключ

–v: root @lord]# ./snort –v

Обратите внимание что, в этом режиме он показывает только заголовки пакетов. Для просмотра заголовка + содержания пакета выполните:

root @lord]# ./snort -X

2. *Режим регистрации пакетов* : Этот режим записывает пакеты на диск и декодирует их в ASCII формат.

root @lord]# Snort -l < directory to log packets to >

3. Режим обнаружения вторжения: Сигнальные данные регистрируются механизмом обнаружения (по умолчанию файл называемый " alert" в каталоге регистрации, но можно через syslog, Winpop сообщения и т.д.) Каталог регистрации по умолчанию *-/var/log/snort* , может быть изменен, используя ключ "-l". Теперь рассмотрим типичную команду Snort для анализа пакета:

root @lord]# snort -v -d -e -i eth0 -h 192.168.3.0/24

Здесь, мы рассматриваем подсеть класса С в пределах от 192.168.3.0-192.168.3.255 (маска подсети: 255.255.255.0). Сделаем подробный разбор вышеупомянутой команды, чтобы понять, что она означает:

'*-v* ': посылает подробный ответ на вашу консоль.

'*-d* ': формирует дамп декодированных данных прикладного уровня

'*-e* ': показывает декодированные Ethernet заголовки.

'*-i* ': определяет интерфейс, который будет проверен для анализа пакета.

'*-h* ': определяет сеть, которой нужно управлять.

В следующем примере мы заставим Snort генерировать предупреждения. Режимы предупреждения Snort состоят из трех основных групп (можно задавать свои):

a. Быстрый: записывает предупреждения в файл 'alert' в одну строку, так же как и в syslog.
b. Полный: записывает предупреждения в файл 'alert' с полным декодированным заголовком.
c. None: - не выдает предупреждения.Команда тогда изменится на следующую:

root @lord]# snort -v -d -e -i eth0 -h 192.168.3.0/24 -A fast

Чтобы посылать аварийные сообщения syslog, используйте ключ '*-s*' вместо этого.

Предупреждения появятся в */var/log/secure* или */var/log/messages* :

root @lord]# snort -v -d -e -i eth0 -h 192.168.3.0/24 -s

До сих пор все перехваченные и проанализированные пакеты показывались на вашем экране. Если вы хотите, чтобы Snort записывал их в ваш файл регистрации, вы должны использовать опцию "*-l*" и указать имя директории для записи логов (например */var/log/snort*):

root @lord]#snort -v -d -e -i eth0 -h 192.168.3.0/24 -A full -l /var/log/snort

Чтобы регистрировать пакеты в формате tcpdump и производить минимальные предупреждения, используйте ключ '*-b* ':

root @lord]#snort -b -i eth0 -A fast -h 192.168.3.0/24 -s -l /var/log/snort

В вышеупомянутых командах, Snort регистрирует все пакеты в вашем сегменте сети. Если вы хотите регистрировать только некоторые типы пакетов в зависимости от правил, используете ключ '*-c* '.

root @lord]# snort -b -i eth0 -A fast -h 192.168.5.0/24 -s -l /var/log/snort -c /snort-rule-file.

Задание:

1. Установите SNORT и настройте правила.
2. Со второй ВМ используйте ping, посмотрите, как реагирует SNORT.
3. Используйте различные методы сканирования nmap (используйте -sS, -sT, -sN, -sU, -sX, -sF и посмотрите, как реагирует SNORT;
4. Со второй виртуальной машины произведите сканирование и проверьте, как работает правило.

Контрольные вопросы:

1. Что такое IDS?
2. Что такое сетевая система обнаружения вторжений?
3. Чем отличаются пассивные и активные IDS?

4. Что такое SNORT?
5. Какие задачи выполняет SNORT?
6. Как работают правила SNORT?
7. Как писать правила для SNORT?
8. Зачем писать собственные правила SNORT?
9. Зачем загружать обновление правил SNORT?
10. Как в SNORT создавать логи?

Лабораторная работа №6

Шифрованная файловая система операционной системы.

Цель работы: формирование навыков по настройке штатных средств шифрования информации в операционных системах Microsoft Windows.

Порядок выполнения работы:

1. Шифрование папки и его содержимое с помощью EFS
2. Восстановление доступа к зашифрованным файлам, их открытие на другом компьютере или под другой учетной записью Windows
3. Шифрование диска с помощью Bitlocker

Работа выполняется на виртуальной машине с установленной операционной системой Windows, для запуска которой используется программа VMware Player.

Многие знают о такой встроенной возможности шифрования дисков и флешек в Windows 10, 8.1 и Windows 7 как Bitlocker, доступной в профессиональной и корпоративной редакциях ОС. Меньшему числу известно о другой функции шифрования файлов и папок — Шифрующей файловой системе EFS, которая также встроена в системе.

В этой лабораторной работе мы изучим о том, как именно работает шифрование EFS, каким образом оно позволяет ограничить доступ к важным

файлам и папкам, как восстановить доступ к данным при необходимости и в чем отличия от BitLocker.

EFS позволяет легко выполнить шифрование содержимого выбранных папок или отдельные файлы с помощью средств системы таким образом, что они будут доступны только для пользователя и на том компьютере, где выполнялось шифрование.

Другие пользователи на этом же или другом компьютере будут видеть файлы и их имена на накопителе, но не смогут получить доступ к ним (открыть их), даже если они имеют права администратора.

Этот способ менее безопасен чем шифрование Bitlocker, но если в вашем распоряжении лишь домашняя редакция Windows 10, 8.1 или Windows 7, а единственная задача — не дать пользователям других учетных записей просмотреть содержимое ваших файлов, вполне можно использовать и EFS: это будет удобно и быстро.

1.Шифрование папки и его содержимое с помощью EFS

Шаги для шифрования папки и его содержимого с помощью шифрующей файловой системы EFS в самом простом варианте будут следующими (доступно только для папок на NTFS дисках и флешках):

1. Откройте свойства нужной папки.
2. В разделе «Атрибуты» нажмите кнопку «Другие» (Рис.89).
3. В разделе «Атрибуты сжатия и шифрования» в следующем окне отметьте «Шифровать содержимое для защиты данных» и нажмите «Ок» (Рис.90).
4. Нажмите «Ок» в свойствах папки и примените изменения к вложенным файлам и папкам (Рис.91).
5. Сразу после этого появится системное уведомление, где вам предложат выполнить архивацию ключа шифрования. Нажмите по уведомлению (Рис.92).

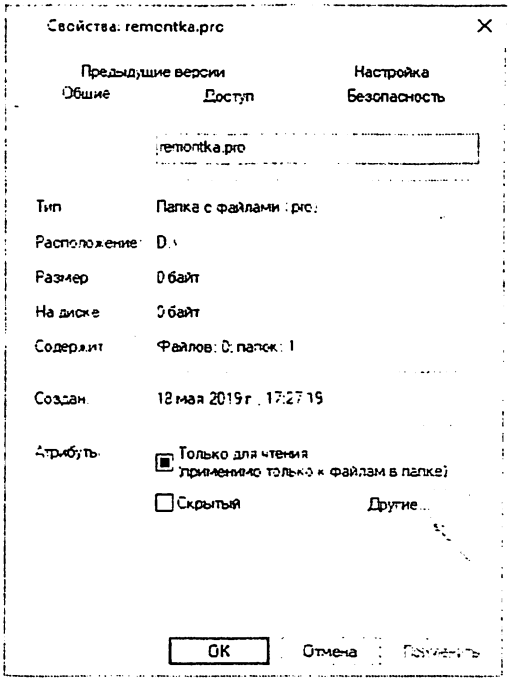


Рис.89. Свойства папки.

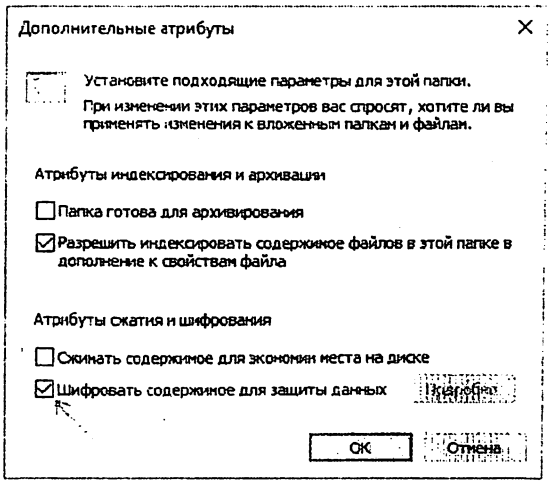


Рис.90. Атрибуты сжатия и шифрования

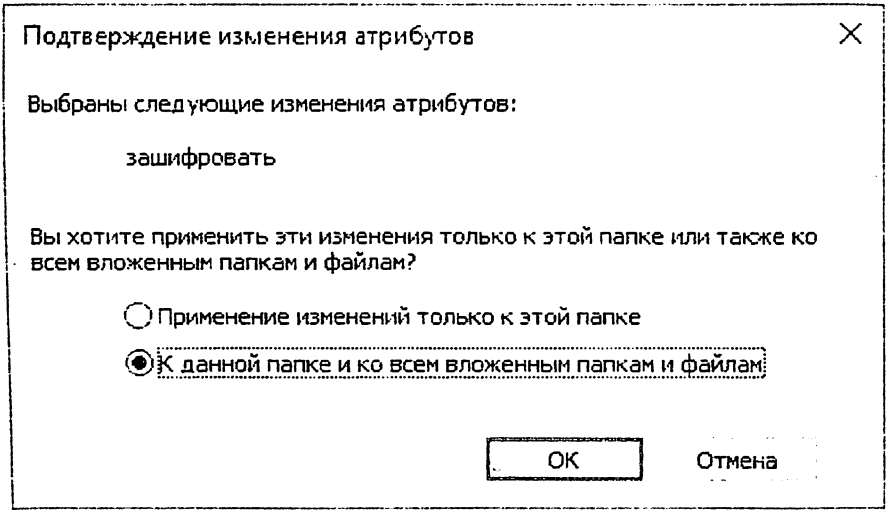


Рис.91. Подтверждение изменения атрибутов.

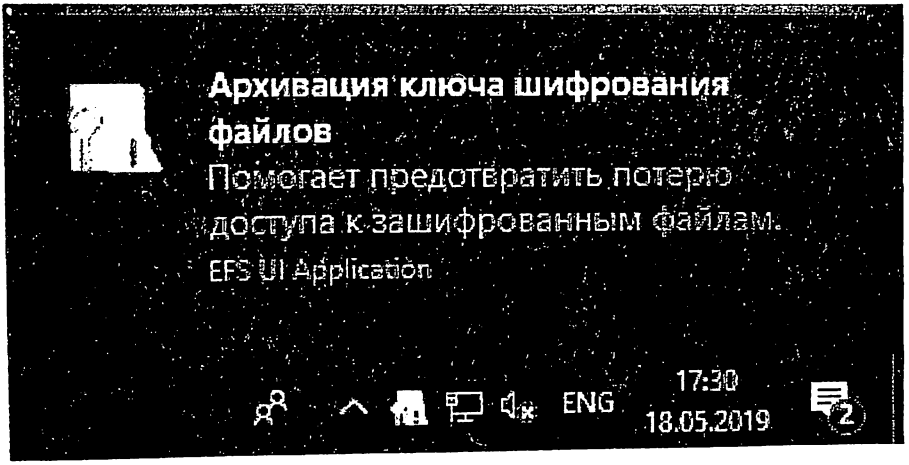


Рис.92. Уведомление об архивации ключа шифрования файлов.

6. Нажмите «Архивировать сейчас» (ключ может потребоваться для восстановления доступа к данным, если вы потеряли свою учетную запись или доступ к этому компьютеру)(Рис.93.).

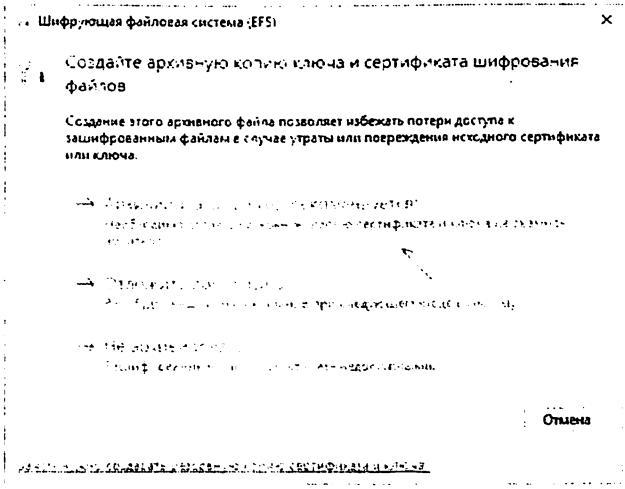


Рис.93. Создание архивного ключа и сертификата.

7. Запустится мастер экспорта сертификатов. Нажмите «Далее» и оставьте параметры по умолчанию. Снова нажмите «Далее». Задайте пароль для вашего сертификата, содержащего ключи шифрования (Рис.94).

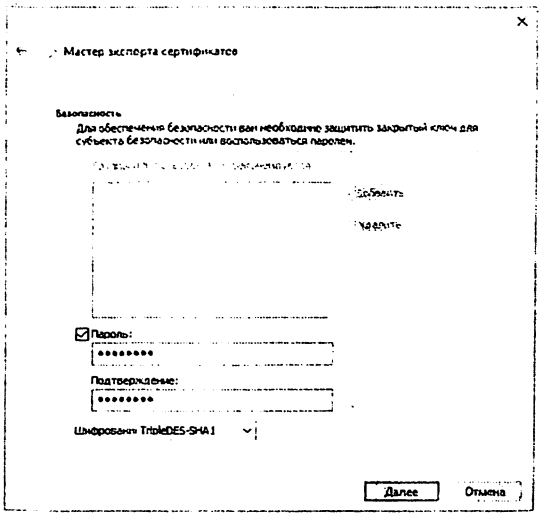


Рис.94. Мастер экспорта сертификатов.

8. Укажите место хранения файла и нажмите «Готово». Этот файл пригодится для восстановления доступа к файлам после сбоев ОС или при необходимости иметь возможность открывать зашифрованные EFS файлы на другом компьютере или под другим пользователем (о том, как это сделать — в следующем разделе инструкции) (Рис.95).

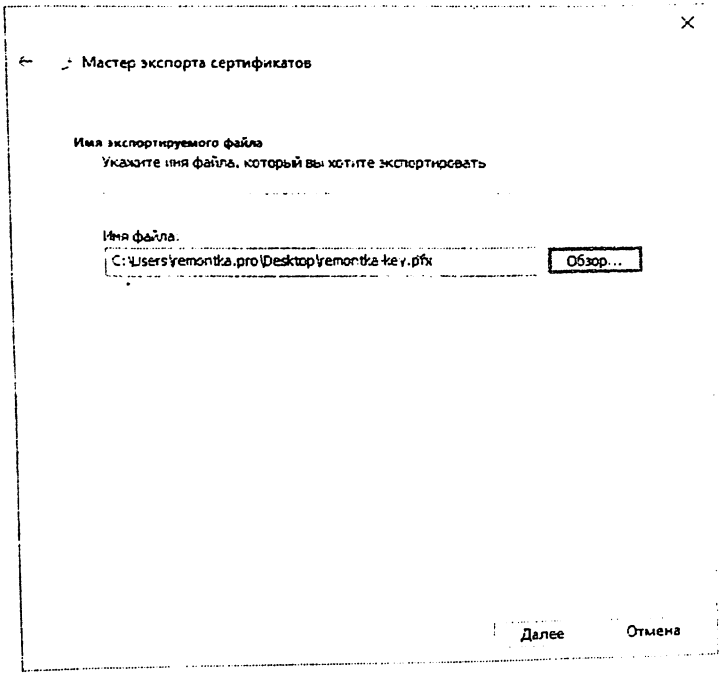


Рис.95. Процесс указания мест хранения для файлов.

На этом процесс завершен — сразу после выполнения процедуры, все файлы в указанной вами папке, как уже имеющиеся там, так и создаваемые вновь приобретут на иконке «замок», сообщающий о том, что файлы зашифрованы (Рис.96).

Они будут без проблем открываться в рамках этой учетной записи, но под другими учетными записями и на других компьютерах открыть их не получится, система будет сообщать об отсутствии доступа к файлам. При этом структура папок и файлов и их имена будут видны.

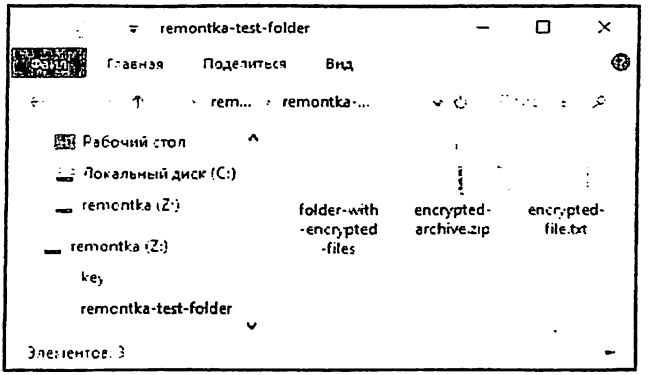


Рис.96. Вид зашифрованного файла.

При желании вы можете, наоборот, начать шифрование с создания и сохранения сертификатов (в том числе и на смарт-карте), а уже затем устанавливать отметку «Шифровать содержимое для защиты данных». Для этого, нажмите клавиши Win+R, введите *rekeywiz* и нажмите Enter (Рис.97).

После этого выполните все шаги, которые предложит вам мастер настройки сертификатов шифрования файлов шифрующей файловой системы EFS. Также, при необходимости, с помощью rekeywiz вы можете задать использование другого сертификата для другой папки.

2.Восстановление доступа к зашифрованным файлам, их открытие на другом компьютере или под другой учетной записью Windows

Если по той или иной причине (например, после переустановки Windows) вы потеряли возможность открыть файлы в зашифрованных EFS папках или вам потребовалась возможность открывать их на другом компьютере или под другим пользователем, сделать это легко:

1. На компьютере в той учетной записи, где нужно иметь доступ к зашифрованным файлам, откройте файл сертификата (Рис.98).

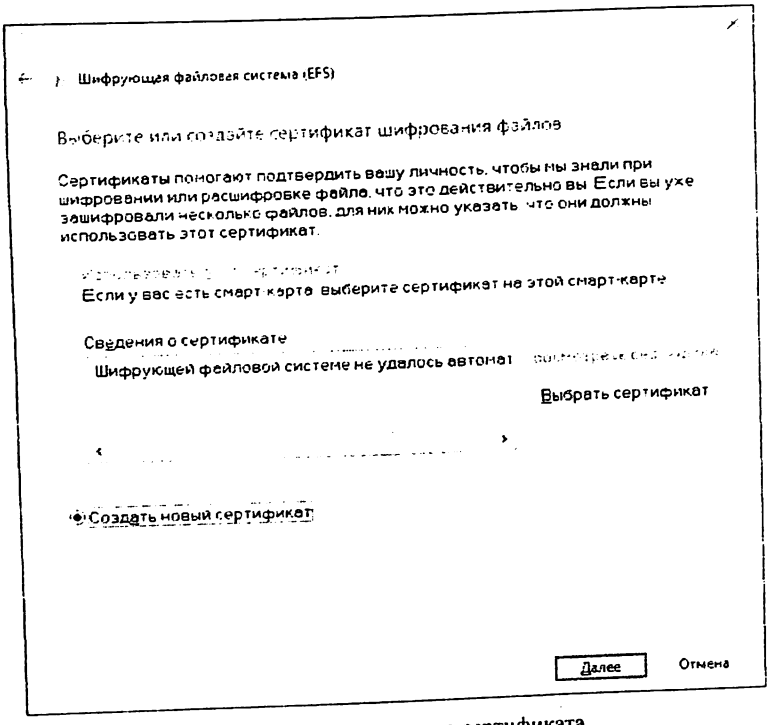


Рис. 97. Создание нового сертификата.

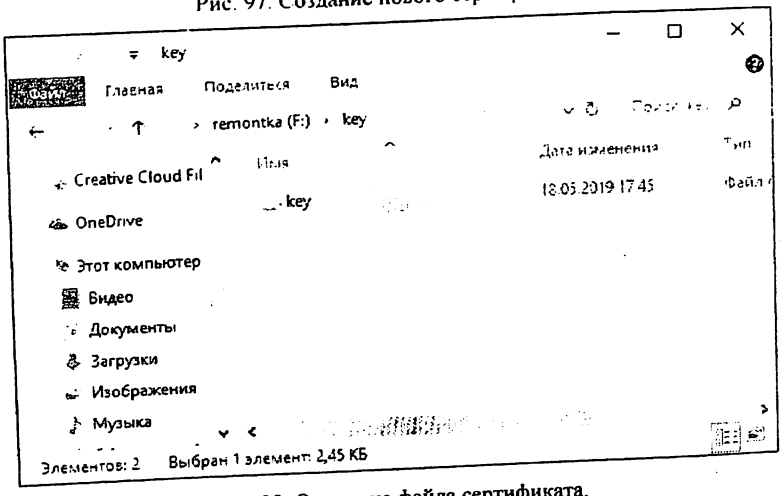


Рис. 98. Открытие файла сертификата.

2. Автоматически откроется мастер импорта сертификатов. Для базового сценария в нем достаточно использовать параметры по умолчанию (Рис.99).

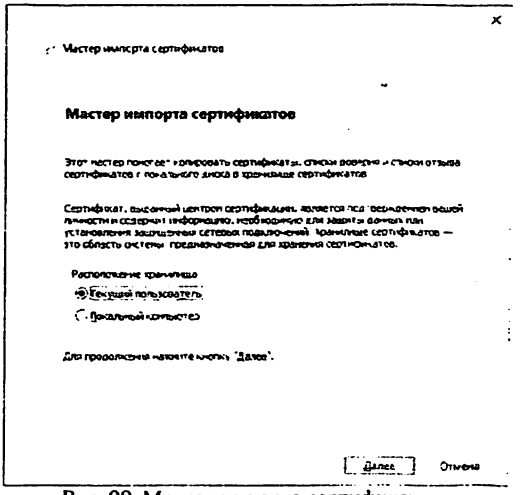


Рис. 99. Мастер импорта сертификатов.

3. Единственное, что потребуется — ввести пароль для сертификата (Рис.100).

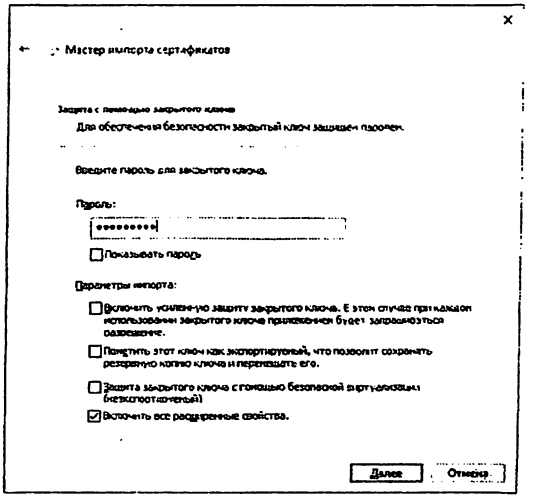


Рис. 100. Введение пароля для закрытого ключа.

4. После успешного импорта, о чем вы получите уведомление, ранее зашифрованные файлы будут открываться и на этом компьютере под текущим пользователем.

Если вам требуется удалить сертификаты шифрования EFS с компьютера, сделать это можно следующим образом: зайдите в Панель управления — Свойства браузера. На вкладке «Содержание» нажмите кнопку «Сертификаты». Удалите ненужные сертификаты: в их описании внизу окна в поле «Назначение сертификата» будет указано «Шифрующая файловая система (EFS)».

В том же разделе управления сертификатами в «Свойствах браузера» можно экспортировать файл сертификата для использования под другим пользователем или на другом компьютере.

3.Шифрование диска с помощью Bitlocker

Bitlocker шифрует целые диски (в том числе системные) или разделы дисков, в то время как EFS применяется к отдельным файлам и папкам. Впрочем, шифрование Bitlocker можно применить и к виртуальному диску (который на компьютере будет храниться как обычный файл).

Сертификаты шифрования EFS привязываются к конкретной учетной записи Windows и хранятся в системе (также ключ можно экспортировать в виде файла на флешке или записать на смарт-карту).

Ключи шифрования Bitlocker хранятся либо в аппаратном модуле TPM, либо могут быть сохранены на внешний накопитель. Открытый диск с Bitlocker одинаково доступен всем пользователям системы, более того, если не использовался TPM, такой диск можно легко открыть и на любом другом компьютере или ноутбуке, достаточно будет ввести пароль.

Шифрование для папок в случае использования EFS нужно включать вручную (файлы внутри будут в дальнейшем шифроваться автоматически).

При использовании Bitlocker всё, что попадает на зашифрованный диск шифруется на лету.

С точки зрения безопасности более эффективно использование Bitlocker. Однако, если требуется всего лишь не дать открыть ваши файлы другим пользователям Windows, а вы используете домашнюю редакцию ОС (где нет Bitlocker) — для этого подойдет и EFS.

Однако, при включении шифрования BitLocker для системного раздела жесткого диска, большинство пользователей сталкиваются с сообщением о том, что «Это устройство не может использовать доверенный платформенный модуль (TPM). Администратор должен задать параметр «Разрешить использование BitLocker без совместимого TPM» (Рис.101).

TPM — специальный криптографический аппаратный модуль, использующийся для задач шифрования. может быть интегрирован в материнскую плату или подключаться к ней.

Примечание: если ваш компьютер или ноутбук оснащен модулем TPM, а вы видите указанное сообщение, это может означать, что по какой-то причине TPM отключен в БИОС или не инициализирован в Windows (нажмите клавиши Win+R и введите tpm.msc для управления модулем).

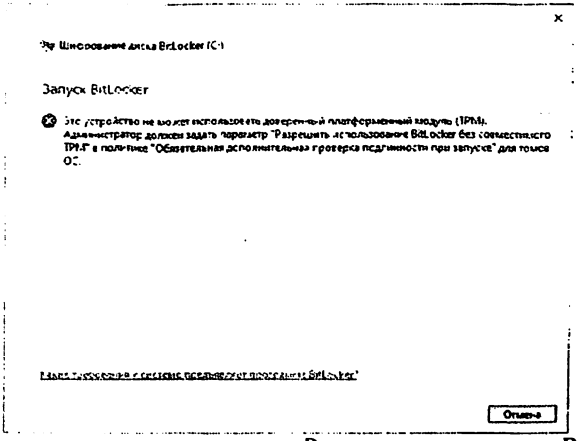


Рис.101. Процесс запроса задать параметр «Разрешить использование BitLocker без совместимого TPM»

В последней версии Windows 10 расположение политики, отвечающей за разрешение использования BitLocker для шифрования системного раздела диска без модуля TPM несколько изменилось.

Для включения шифрования BitlLocker без TPM в новой версии ОС проделайте следующие шаги:

1. Нажмите клавиши Win+R на клавиатуре, введите *gpedit.msc* и нажмите Enter.
2. Откроется редактор локальной групповой политики. Перейдите к разделу: Конфигурация компьютера — Административные шаблоны — Компоненты Windows — Шифрование диска BitLocker — Диски операционной системы.
3. В правой панели редактора локальной групповой политики найдите параметр «Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске» и дважды кликните по нему мышью (Рис.102). Обратите внимание, что в списке есть два параметра с таким именем, нам требуется тот, который без указания Windows Server.

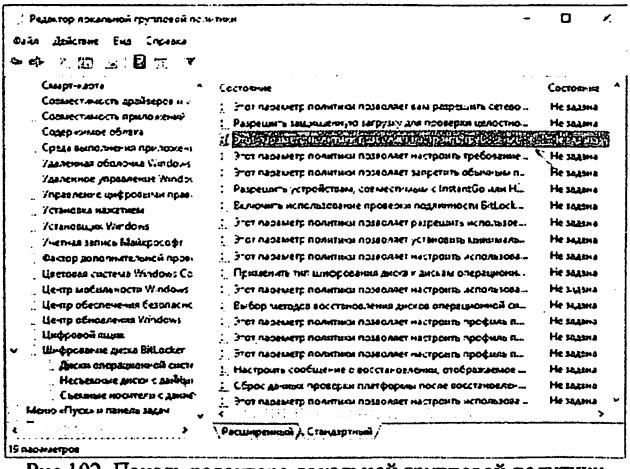


Рис.102. Панель редактора локальной групповой политики

4. В открывшемся окне выберите пункт «Включено» и убедитесь, что пункт «Разрешить использование BitLocker без совместимого TPM включен». Примените сделанные настройки (Рис.103).

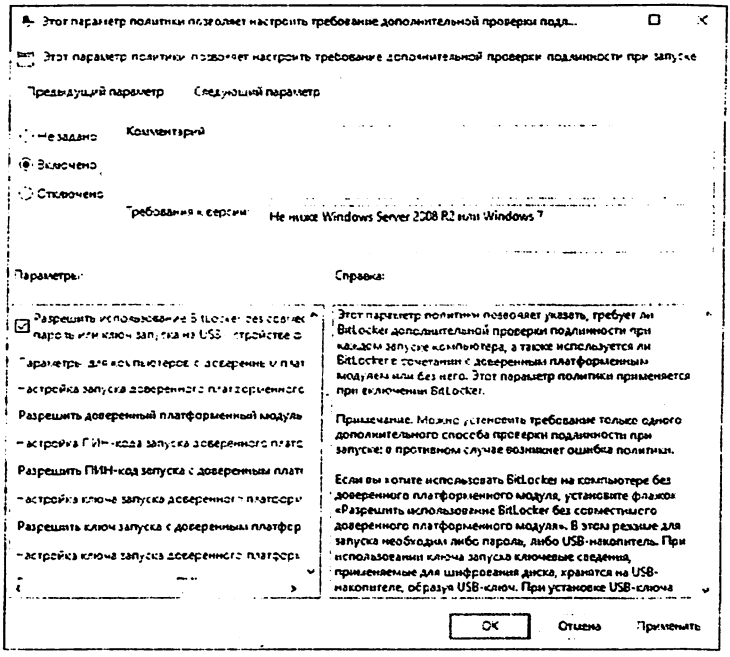


Рис.103. Включение параметра «Разрешить использование BitLocker без совместимого TPM»

На этом процесс завершен и теперь вы можете включить шифрование BitLocker для системного раздела диска Windows 10.

После этого вы можете использовать шифрование дисков без сообщений об ошибках: просто выберите системный диск в проводнике, кликните по нему правой кнопкой мыши и выберите пункт контекстного меню «Включить BitLocker», после чего следуйте указаниям мастера шифрования. Также этом можно сделать в «Панель управления» — «Шифрование диска BitLocker».

Вы сможете либо задать пароль для получения доступа к зашифрованному диску, либо создать USB-устройство (флешку), которая будет использоваться в качестве ключа (Рис.104).

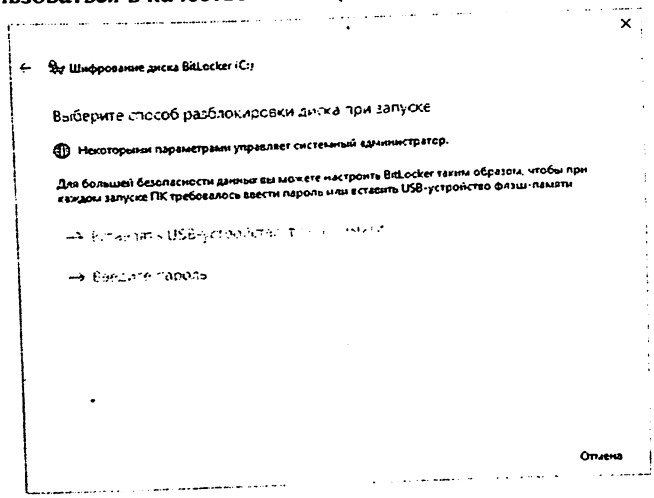


Рис.104. Выбор способа разблокировки диска при запуске.

В ходе шифрования диска в Windows 10 и 8 будет предложено сохранить данные для расшифровки в том числе в вашей учетной записи Майкрософт. Если она у вас должным образом настроена, код восстановления доступа к диску из учетной записи в случае возникновения проблем может оказаться единственным способом не потерять свои данные.

Задание:

1. Ознакомьтесь с ходом лабораторной работы;
2. По инструкцию выполните лабораторную работу и подготовьте отчет.
3. Подготовьтесь к контрольным вопросам.

Контрольные вопросы:

1. В каких выпусках операционных систем Windows присутствует шифрованная файловая система?
2. Для каких файловых систем применима шифрованная файловая система?

3. Для чего в шифрованной файловой системе используется симметричное шифрование? Асимметричное?
4. Как создать сертификат?
5. Чем отличается шифрование EFS от Bitlocker?

Содержание

ДЛЯ ЗАМЕТОК

Составители:

Муминова С.Ш. ассистент кафедры «Обеспечение информационной безопасности», ТУИТ

Агзамова М.Ш. ассистент кафедры «Обеспечение информационной безопасности», ТУИТ

Методические указания рассмотрены и одобрены на заседании кафедры "Обеспечение информационной безопасности"
(___ _____ 2021 г. Протокол № _____)

Методические указания рекомендованы к печати на заседании научно-методического совета факультета "Информационная безопасность"
(___ _____ 2021 г. Протокол № _____)

Методические указания утверждены на Научно-методическом совете Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий
(___ _____ 2021 г. Протокол № _____)

Формат 60x84 1/16. Печ.лист 6.
Заказ № 33. Тираж 50.
Отпечатано в «Редакционно издательском» отделе при ТУИТ.
Ташкент ул. Амир Темур, 108.