Министерство образования Республики Беларусь
Учреждение образования «Витебский государственный университет имени П.М. Машерова»
Кафедра прикладного и системного программирования

В.В. Новый

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические рекомендации по выполнению лабораторных работ

Витебск
ВГУ имени П.М. Машерова
2023

УДК 004.056(076.5)
ББК 16.8я73
Н76

Печатается по решению научно-методического совета учреждения образования «Витебский государственный университет имени П.М. Машерова». Протокол № 6 от 10.03.2023.

Автор: старший преподаватель кафедры прикладного и системного программирования ВГУ имени П.М. Машерова **В.В. Новый**

Р е ц е н з е н т :
заведующий кафедрой математики
и информационных технологий УО «ВГТУ»,
кандидат физико-математических наук, доцент *Т.В. Никонова*

Новый, В.В.

Н76 Основы информационной безопасности : методические рекомендации по выполнению лабораторных работ / В.В. Новый. – Витебск : ВГУ имени П.М. Машерова, 2023. – 36 с.

В методических рекомендациях предлагается ряд лабораторных работ, сопровождающихся пояснениями и описанием хода выполнения, помогающих ознакомиться со многими направлениями в области информационной безопасности. Рассмотрены вопросы управления учетными данными пользователей, аутентификации, аудита событий, криптографической защиты данных и применения электронной цифровой подписи. По всем темам приведены краткие теоретические сведения и задания для самостоятельного выполнения.

Издание предназначается для студентов специальностей «Информационные системы и технологии (в здравоохранении)» и «Программное обеспечение информационных технологий» (дисциплина «Основы информационной безопасности»).

УДК 004.056(076.5)
ББК 16.8я73

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Обеспечение информационной безопасности является одним из важнейших направлений информационных технологий. Вопросы, связанные с безопасностью информации, одинаково важны и для домашних пользователей, и для крупных корпоративных клиентов. Данные методические рекомендации преследуют цель познакомить студентов с рядом основных направлений в сфере обеспечения информационной безопасности IT-технологий.

Методические рекомендации охватывают такие темы, как управление учетными записями пользователей (включая вопросы, связанные с инструментальными средствами работы с пользователями и группами, настройкой политик парольной аутентификации и групповыми политиками в целом, традиционно являющиеся частью политики безопасности большинства организации), аудит парольной аутентификации (включая некоторые виды атак на парольную аутентификацию, знание которых позволяет лучше понимать необходимость и способы противодействия таким атакам), аудит событий безопасности операционной системы, применение основных видов криптографического программного обеспечения для защиты данных пользователя и знакомство с принципами работы и областями применения электронной цифровой подписи. Приведенные темы дополняют знания, полученные в курсах «Операционные системы» и «Компьютерные сети», и могут служить отправной точкой для более глубокого изучения соответствующей тематики.

Лабораторные работы в первую очередь ориентированы на операционные системы семейства Microsoft Windows как наиболее распространенные клиентские рабочие места в настоящее время и могут выполняться на всех актуальных версиях операционных систем этого семейства.

Материал методических рекомендации соответствует темам рабочих программ дисциплины «Основы информационной безопасности» специальностей «Информационные системы и технологии (в здравоохранении)» и «Программное обеспечение информационных технологий», а также отдельным темам дисциплины «Основы информационной безопасности» специальности «Компьютерная безопасность (радиофизические методы и программно-технические средства)».

ЛАБОРАТОРНАЯ РАБОТА № 1
АУТЕНТИФИКАЦИЯ И ПОЛИТИКА ПАРОЛЕЙ В WINDOWS

Цель работы: рассмотреть ряд технических мер повышения защищенности операционных систем, связанных с идентификацией и аутентификацией пользователей; сформировать умения управления соответствующими механизмами операционных систем.

1.1 Теоретические сведения

Идентификация – это присвоение пользователям идентификаторов (уникальных имен или числовых значений) по которым система «узнает» пользователей и «отличает» друг от друга.

Аутентификация – это установление подлинности пользователя (предъявленного пользователем идентификатора), т.е. проверка, является ли пользователь тем, за кого себя выдает.

Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от несанкционированного доступа любой информационной системы.

Обычно выделяется три группы методов аутентификации:

- Аутентификация, основанная на том, что известно пользователю. В англоязычной литературе эти способы называют (“I know” – «я знаю»). К этой группе относится, например, парольная аутентификация.
- Аутентификация, основанная на том, что есть у пользователя. В англоязычной литературе эти способы называют (“I have” – «у меня есть»). К этой группе относится, например, аутентификация по электронному ключу или карте.
- Аутентификация, основанная на собственных уникальных признаках пользователя. В англоязычной литературе эти способы называют (“I am” – «я есть»). К этой группе относятся биометрические методы аутентификации, например, по отпечаткам пальцев.

Часто используются комбинированные схемы аутентификации, объединяющие методы из разных групп. Такие варианты называются **многофакторной аутентификацией**.

Наиболее распространенным методом аутентификации в настоящее время является аутентификация на основе пароля. У пользователя имеется секретная информация, известная только ему и системе – идентификатор и пароль.

В зависимости от реализации, пароль может быть многоразовым или одноразовым. Операционные системы обычно используют аутентификацию на основе многоразовых паролей. Совокупность идентификатора, пароля и, возможно, дополнительной информации, служащей для описания пользователя составляют **учетную запись пользователя**.

В случае если злоумышленник получил пароль пользователя информационной системы, то он может войти в систему под его учетной записью (маскарад) и, например, получить доступ к конфиденциальным данным. Поэтому безопасности паролей уделяется особое внимание.

Согласно стандарта ISO 17799, рекомендуется, чтобы пользователи системы подписывали документ о сохранении конфиденциальности паролей. Однако злоумышленники могут использовать другие методы – подбор пароля по словарю или получение пароля полным перебором (brute force), перехват при передаче по сети и другие.

Основными **рекомендациями по администрированию парольной аутентификации** для снижения подобных рисков являются следующие:

1. Задание минимальной длины используемых в системе паролей. Это усложняет атаку путем перебора паролей. В настоящее время рекомендуется использовать не менее 12 символов.
2. Установка требования применять в пароле разные группы символов – большие и маленькие буквы, цифры, специальные символы. Это позволяет еще больше усложнить подбор пароля (вместо перебора 26 вариантов для каждого символа пароля злоумышленнику будет требоваться перебрать 50 и более вариантов).
3. Периодическое выполнение администраторами безопасности аудита паролей – проверки качества используемых пользователями системы паролей путем имитации атак, таких как подбор паролей «по словарю» (следующая лабораторная работа).
4. Установка максимального и минимального сроков жизни паролей, использование механизма принудительной смены старых паролей при помощи политик безопасности системы.
5. Ограничение числа неудачных попыток ввода пароля (блокирование учетной записи после заданного числа неудачных попыток войти в систему на определенное время или до разблокирования администратором).
6. Ведение журнала истории паролей, чтобы пользователи, после принудительной смены пароля, не могли вновь выбрать себе старый, возможно скомпрометированный пароль.

Современные версии операционных систем Windows позволяют выполнять настройки, автоматически контролирующие выполнение большинства из этих требований. Домен Windows позволяет распространить эти требования на все компьютеры домена и тем самым повысить защищенность всей сети предприятия.

Однако при внедрении новых механизмов защиты могут появиться и нежелательные последствия. Неподготовленным пользователям потребуется объяснить, что с точки зрения операционной системы Windows надежный пароль должен содержать 3 из 4 групп символов (большие буквы, малые буквы, цифры, служебные знаки). Аналогично, необходимо подгото-

вить пользователей к применению блокировки учетных записей после нескольких неудачных попыток ввода пароля, а сами правила блокировки должны быть хорошо продуманы. Например, если высока вероятность того, что пользователь заблокирует свою учетную запись в период отсутствия администратора, лучше установить не постоянную блокировку, а на какой-то срок (15 минут, полчаса, час).

Это приводит к тому, что должна быть разработана политика управления паролями, сопровождающие ее документы, и лишь потом проведено внедрение.

Пользователи и группы пользователей. Для управления группами пользователей и более детального управления учетными записями пользователей в ОС Windows можно воспользоваться оснасткой «**Локальные пользователи и группы**» консоли управления (**mmc**). Для запуска консоли управления необходимо выполнить: «**Пуск -> Панель управления -> Администрирование -> Управление компьютером**». В появившемся окне необходимо выбрать «**Локальные пользователи и группы**». Доступ к этой оснастке также можно получить, набрав в диалоге «Выполнить» lusrmgr.msc.

Чтобы добавить учетную запись нового пользователя, щелкните правой кнопкой мыши на папке Пользователи и выберите из выпадающего меню команду «**Новый пользователь...**» В открывшемся окне введите данные для создания новой учетной записи. Чтобы удалить учетную запись пользователя, щелкните правой кнопкой мыши на названии учетной записи в правом окне программы и выберите из выпадающего меню «Удалить».

Для каждого пользователя можно отключить срок действия пароля, запретить смену пароля пользователем, отключить учетную запись, а также назначить путь к профилю и сценарий входа в систему.

Для того, чтобы добавить учетную запись пользователя в ту или иную группу, щелкните правой кнопкой мыши на названии группы и из выпадающего меню выберите «**Добавить в группу**». В появившемся окне нажмите кнопку «**Добавить...**», в открывшемся диалоге – введите или выберите имя пользователя.

Работа с учетными записями также может осуществляться с помощью системной утилиты net user:

```
NET USER [имя_пользователя [пароль | *] [параметры]] [/DOMAIN]
имя_пользователя {пароль | *} /ADD [параметры] [/DOMAIN]
имя_пользователя [/DELETE] [/DOMAIN]
```

Эта команда создает и изменяет учетные записи пользователей на компьютере. Если используется без параметров, то выводит список учетных записей пользователей для данного компьютера. Выводимая информация об учетных записях пользователей хранится в базе данных учетных записей операционной системы SAM.

имя_пользователя – задает имя пользователя, которое необходимо добавить, удалить, изменить или вывести на экран. Длина имени пользователя не должна превосходить 20 знаков.

пароль - назначает или изменяет пароль для учетной записи пользователя. Пароль должен отвечать установленным требованиям на длину – быть не короче, чем значение, установленное параметром /MINPWLEN в команде NET ACCOUNTS, и в то же время не длиннее 14 знаков.

* – вызывает открытие специальной строки ввода пароля. Пароль не выводится на экран во время его ввода в этой строке.

/ADD – добавляет учетную запись пользователя в базу данных учетных записей.

/DELETE – удаляет учетную запись пользователя из базы данных учетных записей.

Допустимыми являются следующие параметры:

1. /ACTIVE: {YES | NO} – активизирует учетную запись или делает ее не активной. Если учетная запись не активна, пользователь не может получить доступ к серверу. По умолчанию используется значение YES (т.е. учетная запись активна).

2. /COMMENT:"текст" – добавляет описательный комментарий об учетной записи (длиной не более 48 знаков). Текст должен быть заключен в кавычки.

3. /COUNTRYCODE:nnn – использует кодовую страницу нужного языка для вывода справки и сообщений об ошибках. Значение 0 означает выбор кодовой страницы по умолчанию.

4. /EXPIRES:{дата | NEVER} – устанавливает дату истечения срока действия ученой записи. Если используется значение NEVER, то время действия учетной записи не имеет ограничений срока действия. Дата истечения срока действия задается в формате дд/мм/гг или мм/дд/гг, в зависимости от того, какая кодовая страница используется. Месяц может быть указан цифрами, названием месяца или его трехбуквенным сокращением. В качестве разделителя полей должен использоваться знак косой черты (/).

5. /FULLNAME:"имя" – указывает настоящее имя пользователя (а не кодовое имя, заданное параметром имя_пользователя). Настоящее имя следует заключить в кавычки.

6./HOMEDIR:путь – указывает путь к домашнему каталогу пользователя. Этот каталог должен существовать.

7. /PASSWORDCHG:{YES | NO} – определяет, может ли пользователь изменять свой пароль. По умолчанию используется значение YES (т.е. изменение пароля разрешено).

8. /PASSWORDREQ:{YES | NO} – определяет, является ли указание пароля обязательным. По умолчанию используется значение YES (т.е. пароль обязателен).

9./PROFILEPATH[:путь] – устанавливает путь к профилю пользователя.

10. /SCRIPTPATH:путь – устанавливает расположение пользовательского сценария для входа в систему.

11. /TIMES:{промежуток | ALL} – устанавливает промежуток времени, во время которого пользователю разрешен вход в систему. Этот параметр задается в следующем формате:

день[-день][,день[-день]],время[-время][,время[-время]]

Время указывается с точностью до одного часа. Дни являются днями недели и могут указываться как в полном, так и в сокращенном виде. Время можно указывать в 12- и 24-часовом формате. Если используется 12-часовой формат, то можно использовать am, pm, a.m. или p.m. Значение ALL указывает, что пользователь может войти в систему в любое время, а пустое значение указывает, что пользователь не может войти в систему никогда. Разделителем полей указания дней недели и времени является запятая, разделителем при использовании нескольких частей является точка с запятой.

12. /USERCOMMENT:"текст" – позволяет администратору добавлять или изменять текст комментария к учетной записи.

Кроме учетных записей, создаваемых администратором системы, после установки системы в ней присутствуют встроенные учетные записи, например:

- Администратор (Administrator, учётная запись отключена по умолчанию из соображений безопасности);
- Гость (Guest);
- WDAGUtilityAccount – (Windows Defender Guard Utility Account) системная учетная запись, которая используется технологией Application Guard Защитника Windows;

  и т.д.

Существует утилита, позволяющая получить информацию о пользователях, вошедших в систему – PsLoggedOn (из состава PsTools, доступна на сайте Microsoft в разделе Sysinternals):

psloggedon.exe [-l] [-d domain] [-x] [\\computername] или psloggedon.exe [username]

Здесь,

-l - показать только локальных пользователей.

-d - показать только пользователей домена domain.

-x - не показывать время входа в систему.

Идентификаторы безопасности. В ОС Windows вводится общее понятие «участник безопасности», как некоторый специальный объект. К участникам безопасности относятся пользователи, группы пользователей, компьютеры и службы идентификации объектов в системе. Каждому участнику безопасности присваивается идентификатор безопасности SID (Security IDentifier). SID имеет следующую структуру: S-R-X-Y-Y-…-Y-RID. S – это символ означающий, что SID выписывается в строковом виде

(на самом деле это некоторая структура языка Си), R – версия SID (на сегодняшний день существует только одна первая версия), X – идентификатор учетных данных, принимающий значение от 0 до 5, и определяющий уровень службы, выдавшей SID, Y-Y-…-Y – идентификатор домена, RID – относительный идентификатор пользователя. SID пользователя или группы может быть получен с помощью следующих утилит:

1. whoami /user /SID – выводит SID текущего пользователя,
2. psgetsid <имя> - возвращает SID по имени,
3. psgetsid <SID> - возвращает имя по SID,

Команда whoami доступна начиная с версии Windows Vista/Windows Server 2003 в составе операционной системы. Утилита psgetsid является частью бесплатного пакета pstools, который можно скачать с сайта Microsoft (*https://learn.microsoft.com/en-us/sysinternals/downloads/pstools*). Помните, что скачанную и распакованную утилиту нужно разместить в доступном каталоге.

1.2 Задания и комментарии к их выполнению

Задание 0. Подготовка к работе. Для выполнения лабораторной работы Вам потребуется операционная система семейства Microsoft Windows с доступом уровня администратора. При отсутствии данного уровня доступа рекомендуется использовать виртуальную машину с необходимой версией Windows (желательно использовать профессиональную или корпоративную версии, так как в домашних версиях Windows, как правило, ряд инструментов администрирования недоступен). Войдите в систему с правами администратора.

Задание 1. С помощью оснастки lusrmgr.msc выполните следующие действия:

1) Создайте группу StoakleyForest;
2) Создайте учетные записи CristopherRobin и WinnieThePooh в группе StoakleyForest;
3) Для учетной записи WinnieThePooh явным образом пропишите путь к профилю (папку для профиля выберите самостоятельно).

Задание 2. Напишите пакетный файл start.bat (start.cmd) выполняющий следующие действия:

1) Создание учетной записи Tigger с обязательной установкой всех параметров командой net user;
2) Вывод списка всех учетных записей, зарегистрированных в системе.

Задание 3. Используя утилиты, напишите пакетный файл next.bat, записывающий следующую информацию в файл user.txt:

1) SID текущего пользователя (администратора)
2) SID пользователя CristopherRobin
3) SID группы StoakleyForest
4) Имя участника безопасности с SID: S -1-1-0.

Теперь рассмотрим какие настройки необходимо сделать, чтобы пароли пользователей компьютера были достаточно надежны. Выше были рассмотрены рекомендации по администрированию парольной системы. Потребовать их выполнения можно с помощью политики безопасности. Настройка выполняется через **Панель управления Windows**.

Откройте **Панель управления | Администрирование | Локальная политика безопасности**. Также к этой оснастке можно получить доступ через выполнение команды gpedit.msc в диалоге Выполнить. Выберите в списке **Политика учетных записей** и затем **Политика паролей**. Экран консоли управления будет выглядеть так, как представлено на рисунке 1.1 ниже:

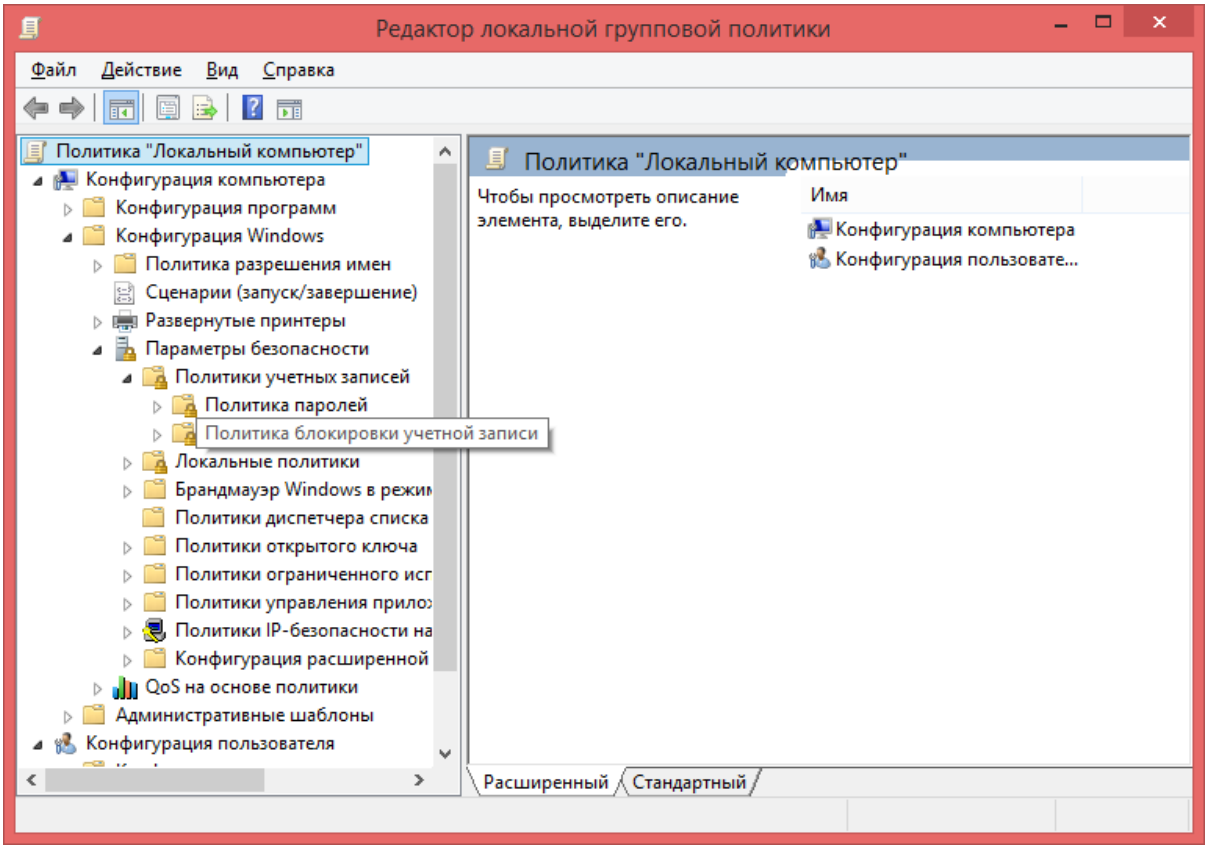

Рисунок 1.1 – Окно редактора групповой политики в оснастке gpedit.msc

Надо понимать, что не все требования политики паролей автоматически подействуют в отношении всех учетных записей. Например, если в свойствах учетной записи стоит "Срок действия пароля не ограничен", установленное политикой требование максимального срока действия пароля будет игнорироваться. Для обычной пользовательской учетной записи, эту настройку лучше не устанавливать. Но в некоторых случаях она рекомендуется. Например, если в учебной лаборатории нужна "групповая" учетная запись, параметры которой известны всем студентам, лучше поставить для

нее "Срок действия пароля не ограничен" и "Запретить смену пароля пользователем".

Свойства учетной записи можно посмотреть в **Панель управления | Администрирование | Управление компьютером**, затем выберите **Локальные пользователи и группы**, после **Пользователи** (или запустите эту же оснастку через диалог «Выполнить» командой lusrmgr.msc).

Задание 4. Опишите действующую на Вашем компьютере политику паролей. Измените ее в соответствии с рассмотренными выше рекомендациями по администрированию парольной системы.

1.3 Задания для самостоятельной работы

Задание 1. Рассмотрите политики блокировки учетной записи. Настройте политики для защиты от подбора пароля злоумышленником.

ЛАБОРАТОРНАЯ РАБОТА № 2
АУДИТ ПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ

Цель работы: рассмотреть основные угрозы безопасности, связанные с идентификацией и аутентификацией пользователей; получить навыки использования инструментария для выполнения аудита паролей в ОС Windows.

2.1 Теоретические сведения

Операционные системы семейства Windows NT хранят пароли в зашифрованном виде, называемом хэшами паролей (hash (англ.) - смесь, мешанина). Функция хэширования – это односторонняя функция. Соответственно, пароли не могут быть получены непосредственно из хэшей.

Для получения паролей в таком случае используется вычисление хэшей по возможным паролям и сравнении их с имеющимися хэшами паролей. При этом злоумышленники могут использовать различные методы – подбор пароля по словарю, полный перебор (brute force), восстановление через «радужные таблицы» и др.

При этом, использование политик управления парольной аутентификацией в Windows и следование рекомендациям, перечисленным в предыдущей лабораторной работе полностью проблему не решает.

В случае, если пользователи не соблюдают принятую политику парольной аутентификации это увеличивает проблему в разы. Для проверки соблюдения пользователями принятой политики в отношении паролей используется **аудит паролей**. Аудит паролей включает в себя проверку возможных путей получения информации об учетных записях пользователей,

а также сложность паролей, которые используют пользователи системы. Результатом аудита паролей является их представление в явном виде с учетом регистра.

Для выполнения аудита паролей в настоящее время существует большое количество инструментов – как платных, так и бесплатно распространяемых. К первой группе можно отнести, например, SAMInside (в настоящее время устарел), Passcape Windows Password Recovery и др.

Ко второй группе можно отнести, к примеру, приложение OphCrack (https://ophcrack.sourceforge.io/), выполняющее аудит паролей на основе метода "грубой силы" (для паролей до 14 символов) или с использованием rainbow tables, L0phtCrack Password Auditor (для старой версии доступен 15-дневный пробный период, в настоящее время утилита распространяется на бесплатной основе, её исходный код выложен авторами на github), а также ряд он-лайн сервисов, например, https://crackstation.net/.

2.2 Задания и комментарии к их выполнению

Задание 1. На примере настроенной в прошлой лабораторной работе виртуальной машины выполните аудит паролей используя:

а) подбор пароля методом "грубой силы" ("bruteforce");

б) перебор по словарю (L0pthCrack, SAMInside или OphCrack).

Задание 2. Извлеките NTLM-хэш паролей (fgdump, mimicatz) и выполните аудит паролей пользователей с использованием техники "rainbow tables" (с помощью таблиц OphCrarck или он-лайн инструментов типа crackstation.net).

2.3 Задания для самостоятельной работы

При наличии физического доступа к вычислительной системе у злоумышленника появляется возможность не подбирать пароль к этой системе, а выполнить его сброс. Подобная же задача может решаться техническим и обслуживающим персоналом, в случае если пользователь забыл учетные данные для входа в систему.

Задание 1. Используя NT Offline Password and Registry Editor (или его аналоги) выполните сброс пароля для административного аккаунта тестовой машины.

ЛАБОРАТОРНАЯ РАБОТА № 3
АУДИТ СОБЫТИЙ БЕЗОПАСНОСТИ И ЖУРНАЛЫ В ОС WINDOWS

Цель работы: рассмотреть особенности выполнения аудита событий в современных операционных системах семейства Windows, получить представление об инструментарии выполнения аудита; сформировать умения по использованию аудита событий для выявления угроз безопасности операционной системе.

3.1 Теоретические сведения

Аудит событий безопасности Windows - это технические средства и мероприятия, направленные на регистрацию и систематический регулярный анализ событий, влияющих на информационную безопасность организации.

Технически, аудит безопасности в Windows реализуется через настройку **политик аудита** и настройку **аудита объектов**. Политика аудита определяет какие события и для каких объектов будут генерироваться в журнал событий «Безопасность». Регулярный анализ данных журнала безопасности относится к организационным мерам, для поддержки которых может применяться различное программное обеспечение. В самом простом случае можно обходиться приложением «Просмотр событий» (Event viewer, eventvwr.msc).

Для автоматизации задач анализа событий безопасности могут применяться более продвинутые программы и **системы управления событиями безопасности** (SIEM), обеспечивающие постоянный контроль журналов безопасности, обнаружение новых событий, их классификацию, оповещение специалистов при обнаружении критических событий.

Журнал безопасности ведется на каждом компьютере и регистрирует события, происходящие на данном компьютере. Благодаря системе аудита, администратор может узнать, кто, каким образом и когда пользовался (или пытался пользоваться, но получил отказ в доступе) интересующими его ресурсами. Настройка аудита позволяет выбрать типы событий, подлежащих регистрации, и определить, какие именно параметры будут регистрироваться. Наиболее общими типами событий для аудита безопасности являются:

- доступ к файлам и папкам;
- управление учетными записями пользователей и групп;
- вход пользователей в систему и выход из нее.

Фиксируются следующие параметры, касающиеся действий, совершаемых пользователями:

- выполненное действие;
- имя пользователя, выполнившего действие;
- дата и время выполнения.

Аудит приводит к дополнительной нагрузке на систему, поэтому следует регистрировать лишь события, действительно представляющие интерес.

Перед выполнением аудита необходимо выбрать политику аудита. Политика аудита указывает типы событий, которые будут регистрироваться в журнале безопасности. После установки Windows все категории аудита выключены. Включая аудит различных категорий событий, можно создавать политику аудита, удовлетворяющую необходимым требованиям.

Настройка политик аудита доступна в оснастке **Групповая политика (gpedit.msc)**.

Существуют следующие категории аудита:

- Аудит событий входа в систему. Отслеживает события, связанные с входом пользователя в систему и выходом из неё;
- Аудит управления учетными записями. Отслеживает все события, связанные с управлением учетными записями. Записи аудита появляются при создании, изменении или удалении учетных записей пользователя или группы;
- Аудит доступа к службе каталогов. Отслеживает события доступа к каталогу Active Directory. Записи аудита создаются каждый раз при доступе пользователей или компьютеров к каталогу;
- Аудит входа в систему. Отслеживает события входа в систему или выхода из нее, а также удаленные сетевые подключения;
- Аудит доступа к объектам. Отслеживает использование системных ресурсов файлами, каталогами, общими ресурсами, и объектами Active Directory;
- Аудит изменения политики. Отслеживает изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений;
- Аудит использования привилегий. Отслеживает каждую попытку применения пользователем предоставленного ему права или привилегии.

3.2 Задания и комментарии к их выполнению

Задание 0. Подготовка к работе. Для выполнения лабораторной работы Вам потребуется операционная система Microsoft Windows и учетные записи, созданные в ходе выполнения первой части лабораторной работы №1.

Задание 1. Войдите в систему административным пользователем. Через оснастку групповой политики включите аудит и настройте регистрацию попыток (успех и отказ) входа в систему для пользователей. Попытайтесь войти в систему с указанием неверного пароля от имени одного из пользователей. Отметьте, какие коды событий и какую информацию при этом добавляет в журнал система аудита.

Задание 2. Настройка аудита доступа к объектам файловой системы. От имени одного из пользователей системы создайте на диске каталог "Секретные данные" и поместите внутрь текстовый файл "Данные.txt". Средствами ОС запретите доступ к этому файлу тестовым пользователям. Включите аудит для созданного каталога и файла. Войдите в систему от имени тестового пользователя. Попытайтесь получить доступ к файлу с секретными данными. Отметьте в отчете, какая информация при этом была внесена в журнал безопасности.

Задание 3. Настройте параметры журнала безопасности в Вашей ОС (размер и поведение в случае переполнения записями о событиях). Очистите его от старых событий (с сохранением копии). Проанализируйте, какие записи были внесены при этом в журнал.

ЛАБОРАТОРНАЯ РАБОТА № 4
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ (WINDOWS)

Цель работы: рассмотреть основные механизмы защиты данных на основе криптографии, используемые в современных операционных системах семейства Windows, получить умения настройки и применения криптографической защиты данных в ОС Windows; закрепить навыки использования инструментов администрирования в ОС Windows.

4.1 Теоретические сведения

Кратко напомним материал лекционных занятий. Процесс шифрования может быть схематически представлен следующим образом (см. рисунок 4.1):

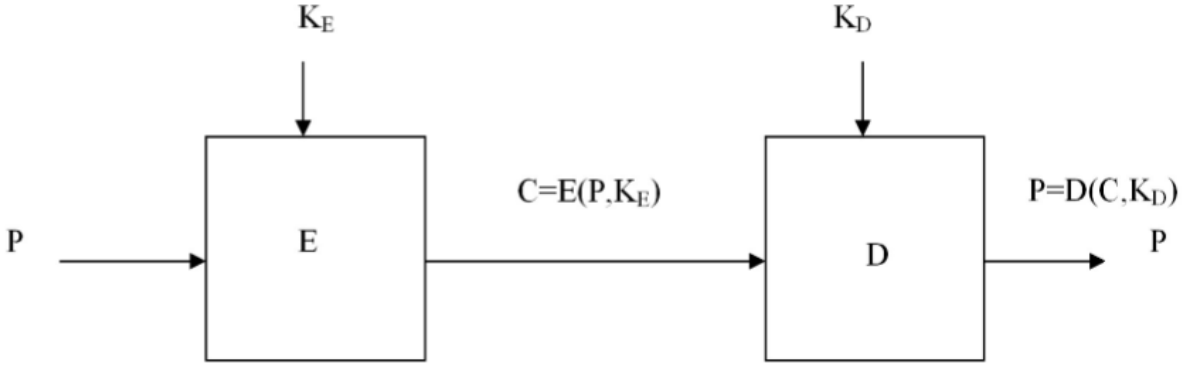

Рисунок 4.1 – Процессы шифрования и дешифрования

Здесь

P – открытый (не зашифрованный) текст;

K_E – ключ шифрования;

K_D – ключ дешифрования;

C – зашифрованный текст (криптограмма);
E – алгоритм шифрования;
D – алгоритм дешифрования.

По наличию и количеству ключей, криптографические алгоритмы могут быть разделены на:

- Бесключевые;
- Одноключевые (или симметричные);
- Двухключевые (ассиметричные или криптосистемы с открытым ключом).

В **симметричных криптосистемах** для процессов шифрования и дешифрования используется один и тот же ключ (или один из ключей легко вычисляется при наличии второго ключа). Для таких криптографических алгоритмов очевидно требование секретности ключа, а одной из важнейших проблем становится безопасная передача этого ключа другому лицу, которому требуется доступ к зашифрованным данным. Подобные криптосистемы лучше всего подходят для защиты хранимых данных пользователя, так как в этом случае передача ключа не требуется.

В **системах с открытым ключом** (СОК) используются два ключа – открытый (или публичный) и закрытый (или приватный), которые математически друг с другом связаны, но при этом по значению одного из ключей крайне сложно (или вообще невозможно) вычислить значение второго ключа. В таких системах данные шифруются открытым ключом, который делается доступным всем желающим, а дешифрование криптограммы осуществляется закрытым ключом, который известен только владельцу. Подобные криптосистемы лучше всего подходят для организации коммуникации и передачи данных за пределы локальной вычислительной системы.

Симметричное шифрование в свою очередь делится на два вида:

- **Блочное шифрование** (информация представляется в виде блоков некоторой фиксированной длины, которые поочередно шифруются);
- **Потоковое шифрование** (информация шифруется побитово или посимвольно, по мере поступления).

Потоковое шифрование чаще всего используется в коммуникационных каналах, в то время как блочное шифрование применяется чаще всего для хранимых данных.

В настоящее время большинство блочных шифров строится на основе двух основных методов: сети Фейстеля (Feistel Network) или подстановочно-перестановочных сетей (Substitution-Permutation network или сокращенно SP-network).

К наиболее известным представителям СОК можно отнести RSA (Rivest, Shamir, Adleman, 1977), Elgamal (1985), DSA (Digital Signature Algorithm, 1991, СОК предназначенная для электронной цифровой подписи),

McEliece (Роберт Мак-Элис, 1978), ГОСТ 34.10-2018 (ФСБ России, АО «ИнфоТеКС», 2018), ECDSA (Elliptic Curve Digital Signature Algorithm, 1991-1998).

К наиболее известным представителям симметричных криптосистем можно отнести предыдущий американский стандарт шифрования DES (IBM, 1977) и 3DES (Triple DES, 1978), американский стандарт шифрования AES (Advanced Encryption Standard, 1998, в основе лежит алгоритм Rijndael), Blowfish (Брюс Шнайер, 1993), Serpent (Росс Андерс, Эли Бихам, Ларс Кнудсен, 1998), Twofish (группа во главе с Брюсом Шнайером, 1998), ГОСТ 28147-89 «Магма» (8-е управление КГБ, 1978), RC4 (Rivest cipher 4, 1987), ГОСТ 34.12-2018 «Кузнечик» (Центр защиты информации и специальной связи ФСБ России, АО «ИнфоТеКС», 2015), СТБ 34.101.31-2007 «BelT» (учреждение БГУ «Научно-исследовательский институт прикладных проблем математики и информатики», 2001).

С точки зрения защиты хранимых в локальной вычислительной системе данных пользователя можно выделить следующие подходы:

- Полное шифрование диска (FDE, Full Disk Encryption), предусматривает процесс шифрования всех данных на жестком диске, включая загрузчик операционной системы, операционную систему; доступ к данным предоставляется только после успешного прохождения аутентификации в FDE-приложении;
- Шифрование на уровне отдельных элементов файловой системы, таких как файлы и каталоги (FE, File Encryption), доступ к данным предоставляется только после успешного прохождения аутентификации на уровне приложения, драйвера или операционной системы;
- Шифрование на уровне виртуального диска и тома (VDE, Virtual Disk Encryption), предусматривает процесс шифрования файла, называемого *контейнер* или *крипто-контейнер*, который может содержать внутри себя множество файлов или каталогов; доступ к данным внутри контейнера предоставляется только после успешной аутентификации и подключения контейнера, который как правило монтируется как виртуальный диск.

Самым простым способом криптографической защиты данных в Windows является использование EFS (Encrypted File System). Это средство шифрования предназначено для защиты отдельных файлов и каталогов на диске с NTFS. Шифрование выполняется на уровне пользователя и добавляет еще один уровень безопасности файловой системы к механизмам контроля доступа. Ключ шифрования сохраняется в файловой системе, а не в TPM-модуле, что потенциально позволяет злоумышленнику извлечь его. Пользователь, обладающий нужным ключом, может работать с зашифрованными файлами, как если бы шифрование не использовалось («прозрачно»). Пользователь, не имеющий нужного ключа, не сможет получить доступ к информации, даже если этот пользователь имеет полный набор

полномочий NTFS. Он все равно получит сообщение об ошибке и не увидит содержимое файла. Предусмотрен агент восстановления, который может использоваться администратором в случае, если владелец не может предоставить ключ, необходимый расшифровки файлов или папок. Для доступа к зашифрованным при помощи EFS данным после переустановки операционной системы следует сохранить сертификат шифрования. Для этого может использоваться оснастка certmgr.msc или доступ к диалогу резервного копирования сертификата шифрования через значок уведомления в системном трее Windows при выполнении первой операции шифрования.

Чтобы зашифровать папку или файл с помощью графического интерфейса, необходимо на этом элементе нажать правую кнопку мыши и выбрать его свойства. В открывшемся окне на вкладке Общие нажмите кнопку Другие и выберите пункт «Шифровать содержимое для защиты данных». Следует помнить, что при шифровании папки шифруются только файлы в ней, список же файлов остается открытым. В графическом интерфейсе Windows ранних версии зашифрованные файлы подсвечиваются зеленым цветом, в Windows новых версии на значки таких файлов добавляется оверлейный значок в виде замка.

Шифрование и дешифрование файлов можно также производить, используя системную утилиту cipher:

```
CIPHER /[параметр команды] [имя файла]
```

Основными параметрами команды являются следующие:

/? – отображает встроенную справку утилиты;

/C – отображает сведения о зашифрованном файле;

/E – указывает, что файлы и папки следует зашифровать;

/D – указывает, что файлы и папки следует расшифровать;

/S:dir – указывает, что выбранную операцию (шифрование или дешифрование следует выполнить также для всех вложенных файлов и папок);

/B – прерывает выполнение команды в случае ошибки. По умолчанию CIPHER продолжает выполнение даже при обнаружении ошибок.

/H – отображает файлы с атрибутами «скрытый» и «системный». По умолчанию такие файлы пропускаются.

Запуск утилиты без параметров вводит список файлов текущей директории, с указанием зашифрованы они или нет.

Гораздо больший уровень защиты данных предоставляет технология BitLocker, относящаяся к типу полного шифрования диска. Этот механизм позволяет шифровать диски целиком, включая системный диск Windows (!!). Кроме того, BitLocker поддерживает более надежное хранение ключей шифрования с использованием аппаратного обеспечение – доверенного платформенного модуля (TPM).

Кроме использования BitLocker, можно воспользоваться внешними для Windows продуктами. После возможной компрометации TrueCrypt, в качестве таковых можно воспользоваться бесплатными программами с открытым исходным кодом VeraCrypt или GostCrypt. VeraCrypt предоставляет возможности полного шифрования диска и шифрования на уровне виртуального диска и тома (создание т.н. контейнера). При этом в отличие от BitLocker VeraCrypt не требует по умолчанию наличия модуля TPM.

4.2 Задания и комментарии к их выполнению

Задание 0. Подготовка к работе. Для выполнения лабораторной работы Вам потребуется операционная система семейства Microsoft Windows, установленная на носителе с файловой системой NTFS, а также приложение VeraCrypt (доступно по адресу https://www.veracrypt.fr/code/VeraCrypt/). Следует учитывать, что технология BitLocker доступна для профессиональной и корпоративной версии операционной системы, и не доступна на версиях, предназначенных для домашнего использования.

Задание 1. Войдите в систему от имени пользователя VinnieThePooh, созданного в ходе лабораторной работы №1. Создайте на диске с файловой системой NTFS файл honey.txt и с помощью графического интерфейса выполните его шифрование средствами EFS. Предоставьте доступ к этому файлу на уровне прав доступа NTFS для пользователя Tigger. Войдите в систему от пользователя Tigger и проверьте недоступность данных файла honey.txt. После этого вернитесь в учетную запись пользователя VinnieThePooh и используя утилиту cipher расшифруйте зашифрованный файл.

Замечание. Рассмотрите оба интерфейса к EFS – графический и команду cipher.

Задание 2. Сохраните сертификат и ключ шифрования EFS. Продемонстрируйте его восстановление для учетной записи пользователя после удаления сертификата.

Задание 3. Изучите на основе источников [9] и [10] из списка литературы как работает BitLocker. Выполните шифрование выбранного диска при помощи этой технологии (обратите внимание на различные способы доступа к BitLocker – графический интерфейс, команду manage-bde и командлеты PowerShell).

Замечание. Для проверки доступности модуля TPM можно воспользоваться оснасткой tpm.msc.

Задание 4. Расшифруйте зашифрованный ранее диск и отключите BitLocker. Повторите шифрование диска при помощи утилиты VeraCrypt.

4.3 Задания для самостоятельной работы

Задание 1. Рассмотрите создание зашифрованного файлового контейнера (криптоконтейнера) средствами VeraCrypt. Продемонстрируйте его монтирование, сохранение файлов в него и размонтирование.

ЛАБОРАТОРНАЯ РАБОТА № 5
ЭЦП (ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ)

Цель работы: рассмотреть основы использования технологии «электронной цифровой подписи», получить умения по проверке цифровой подписи, использовании цифровой подписи в электронной почте.

5.1 Теоретические сведения

Одним из направлений современной криптографии, основанном на ассиметричных криптосистемах, является электронная цифровая подпись. Электронная цифровая подпись (ЭЦП) может использоваться при подаче налоговых декларации, предоставлении отчетов в госорганы, работе с электронными счет-фактурами, при заверении сделок и так далее. Одна из традиционных сфер применения ЭЦП – аутентификация и проверка целостности документов, передаваемых по телекоммуникационным каналам. Использование телекоммуникации существенно ускоряет поиск подобных документов, снижает затраты на их хранение и обработку. Но при этом возникает проблема аутентификации автора электронного документа (установление его подлинности) и самого документа (удостоверение отсутствия изменений в полученном документе). В настоящее время под использование ЭЦП подведена законодательная база. В нашей стране использование ЭЦП регулируется Законом Республики Беларусь от 28.12.2009 г. «Об электронном документе и электронной цифровой подписи».

Целью аутентификации электронных документов является их защита от возможных действий злоумышленника, таких как:

- **Активный перехват** – нарушитель, подключившийся к сети, перехватывает файлы и изменяет их;
- **Маскарад** – злоумышленник посылает Бобу сообщения от имени Алисы;
- **Ренегатство** – Алиса заявляет, что не посылала сообщений Бобу, хотя на самом деле посылала;
- **Подмена** – Боб изменяет или формирует новый документ и заявляет, что получил его от Алиса;
- **Повтор** – злоумышленник повторяет ранее переданный документ, который Алиса посылала Бобу.

Такие действия могут наносить существенный ущерб банковским и коммерческим структурам, госпредприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные информационные системы.

Функционально ЭЦП аналогична обычной рукописной подписи и обладает её основными достоинствами:

- Удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

– Не дает этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
– Гарантирует целостность подписанного текста.

ЭЦП представляет собой относительно небольшое количество дополнительной цифровой информации, добавляемой к документу или передаваемой вместе с подписываемым текстом и в настоящее время чаще всего основана на применении криптосистем с открытым ключом (СОК) и хэш-функции.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: закрытый и открытый. Закрытый ключ хранится абонентом в тайне и используется для формирования ЭЦП – «подписи документов». Открытый ключ известен ВСЕМ остальным пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа.

Рассмотрим этот процесс подробнее (см. рисунок 5.1):

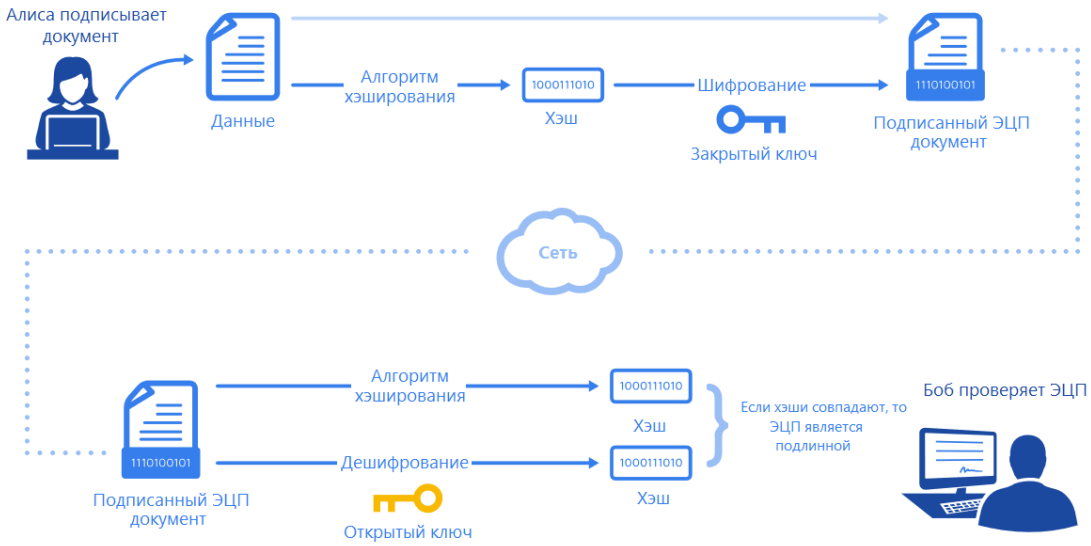

Рисунок 5.1 – Схема работы электронной цифровой подписи

Формирование ЭЦП. Алиса – отправитель сообщения – получает пару ключей: открытый и закрытый ключ. Открытый ключ делается доступным остальным абонентам сети для проверки подписи. Для формирования цифровой подписи Алиса вначале вычисляет значение хэш-функции m=h(M) подписываемого текста M.

Далее Алиса шифрует полученный дайджест m своим секретным ключом. Полученное значение и представляет собой электронную цифровую подпись сообщения M. Сообщение M вместе с цифровой подписью отправляется получателю. Обратите внимание, что вместо шифрования самого сообщения, которое может иметь достаточно большой объем, шифруется его

хэш. При этом сохраняется возможность чтения самого сообщения без необходимости дополнительного дешифрования. Таким образом процессы шифрования и подписи разделяются.

Проверка ЭЦП. Боб – получатель сообщения – расшифровывает принятый дайджест m открытым ключом Алисы. Кроме этого, Боб сам вычисляет с помощью хэш-функции h(M) дайджест m’ принятого сообщения M и сравнивает его с расшифрованным. Если эти два дайджеста m и m’ совпадают, то цифровая подпись является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения.

В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путём добавления в него одной или более электронных подписей.

Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) структура ЭЦП обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления ЭЦП, что обеспечивает и ее целостность. Обычно подпись содержит следующую информацию:

- Дату и время подписи;
- Алгоритм, использованный при формировании ЭЦП;
- Срок окончания действия ключа данной подписи;
- Информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
- Идентификатор подписавшего (имя открытого ключа);
- Собственно, цифровую подпись (зашифрованный хэш).

В настоящее время существует большое количество алгоритмов ЭЦП: RSA-PSS, DSA (Digital Signature Algorithm); ECDSA (Elliptic Curve Digital Signature Algorithm); ГОСТ Р 34.10-94 (первый российский стандарт цифровой подписи); ГОСТ Р 34.10-2001 и другие.

Аналогично асимметричным криптосистемам, необходимо обеспечить невозможность подмены открытого ключа, используемого для проверки ЭЦП. Подобную защиту от подмены можно реализовать с помощью соответствующих цифровых сертификатов в рамках инфраструктуры открытых ключей PKI (Public Key Infrastructure).

Чтобы пользователь мог доверять процессу аутентификации, он должен получать открытый ключ другого пользователя из надежного источника, которому он доверяет. Таким источником, согласно стандарту X.509, является центр сертификации CA (Certification Authority), который также называют УЦ – удостоверяющим центром (в Республике Беларусь таковым является РУП «Национальный центр электронных услуг» (НЦЭУ), в состав которого входит республиканский удостоверяющий центр Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (РУЦ ГосСУОК)).

Центр сертификации CA является доверенной третьей стороной, которая обеспечивает аутентификацию открытых ключей, содержащихся в

сертификатах. CA имеет собственную пару ключей (открытый/секретный), где секретный ключ CA используется для подписи сертификатов, а открытый ключ CA публикуется и применяется пользователями для проверки подлинности открытого ключа, содержащегося в сертификате.

Механизм ЭЦП используется во многих сферах IT. В частности, он применяется для подписей различного рода документов, например, MS Word, Adobe PDF и других. С его помощью подписываются программы и драйвера. Он используется для подписи пакетов в репозиториях различных дистрибутивов Linux. Этот же механизм используется в электронной почте и многих других технологиях.

На данный момент ЭЦП дает право подписывать электронные документы и обращения, подаваемые в МНС, таможенные органы, ФСЗН, Белгосстрах, Белстат и т.д. Также стоит отметить, что корпоративные системы (например, «Клиент-банк») могут применять ключи ЭЦП, выданные собственными удостоверяющими центрами. Однако такие ключи ЭЦП будут признаваться только в рамках этих систем.

5.2 Задания и комментарии к их выполнению

Задание 0. Подготовка к работе. Для выполнения лабораторной работы Вам потребуется операционная система семейства Microsoft Windows, шестнадцатеричный редактор (hex-редактор; например, Frhed, HxD, Binary EYE, Free Hex Editor Neo и т.д.), почтовый клиент Mozilla Thunderbird. Задание 3 также может быть выполнено в операционной системе семейства Linux.

Задание 1. Исследование основных свойств ЭЦП. Рассмотрим свойства ЭЦП на примере технологии Microsoft Authenticode, предназначенной для подписи исполнимых файлов и драйверов в операционной системе Microsoft Windows.

Найдите на своём компьютере какую-либо программу, подписанную ЭЦП разработчика. Через окно свойств «Цифровые подписи» изучите цифровую подпись приложения и сопровождающую её информацию. Определите:

- алгоритм хэширования;
- алгоритм цифровой подписи (алгоритм шифрования);
- сведения о подписавшем.

Для доступа к необходимой информации зайдите в свойства исполнимого файла (не ярлыка!) и переключитесь на вкладку «Цифровые подписи» как показано на рисунке ниже (см. рисунок 5.2).

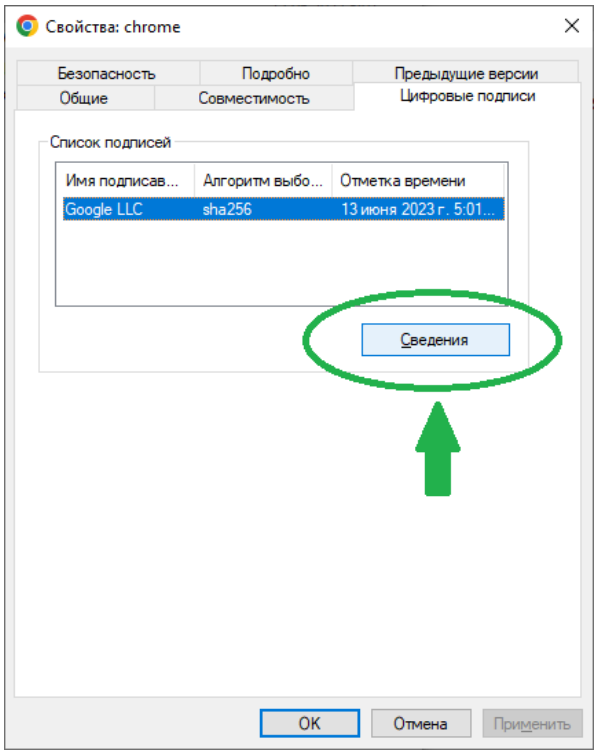

Рисунок 5.2 – Доступ к информации о цифровой подписи исполнимого файла

Указание. При сложностях с поиском подписанной программы (можно использовать любой современный браузер, например, Google Chrome) можно использовать MRT.exe из каталога %SystemRoot%\System32 или исполнимый файл Total Commander последних версий.

Контроль целостности исполняемого файла. Модифицируйте найденную ранее программу: при помощи шестнадцатеричного редактора измените хотя бы один бит кода программы. Перед выполнением этого шага рекомендуется сделать резервную копию модифицируемого файла. После внесения изменений проверьте цифровую подпись повторно. Является ли она валидной? Сделайте выводы о возможности модификации подписанного документа.

Примечание: помните, что исполнимые файлы имеют свою собственную структуру. В начале файла находится его заголовок, необходимый для загрузки файла (PE-header – информация об этом доступна по адресу: https://learn.microsoft.com/en-us/windows/win32/debug/pe-format или https://ru.wikipedia.org/wiki/Portable_Executable), а сама цифровая подпись размещается (обычно) в конце файла в виде отдельной секции. Поэтому вносить изменения стоит не в самом начале и не в самом конце файла (хотя и это тоже на нём отразится).

В качестве еще одного применения цифровой подписи рассмотрим настройку ЭЦП для сообщений электронной почты.

Задание 2. Подпись сообщений электронной почты. Настройте цифровую подпись для почтового клиента Mozilla Thunderbird. Продемонстрируйте подпись и отправку подписанного сообщения одним пользователем, получение сообщения, и проверку подписи другим пользователем.

Примечание: для тестирования удобно использовать две различных копии почтовой программы для двух учетных записей (например, можно использовать портативные версии Mozilla Thunderbird, предоставляемые PortableApps https://portableapps.com/apps/internet/thunderbird_portable (ниже на странице доступна русскоязычная версия)).

Примечание: шифрование и электронная цифровая подпись - это различные возможности почтовой программы; для целей этой работы шифрование не требуется.

Примечание: начиная с версии 78 средства цифровой подписи и шифрования встроены в клиент Thunderbird, использование плагина Enigmail не требуется, однако, большинство руководств в Интернет написаны для ранней версии. Будьте внимательны при чтении.

Ход выполнения. После установки (или распаковки) почтового клиента Mozilla Thunderbird, настраиваем на нём учетную запись, как было рассмотрено на занятиях по дисциплине «Компьютерные сети». В качестве примера возьмем две учетных записи: Alice и Bob. Алиса будет выступать в роли отправителя, а Боб – в роли получателя подписанного сообщения. Приведенные ниже иллюстрации справедливы для версии Mozilla Thunderbird 102.12.0, актуальной на момент написания пояснений.

В начале создадим ключевую пару (открытый и закрытый ключи для Алисы). Ключи могут быть созданы внешними инструментами (например, gpg) и импортированы в Mozilla Thunderbird, однако последние версии поддерживают создание ключей в самой программе. Заходим в пункт главного меню «Инструменты» («Tools») и выбираем пункт «Параметры учетной записи» («Account Settings»). В открывшемся окне выбираем пункт «Сквозное шифрование» («End-To-End Encryption») (как представлено на рисунке 5.3 ниже), так как функциональность добавления электронной цифровой подписи тесно связана с механизмами шифрования с открытым ключом. На данный момент у Алисы нет личного ключа для подписи сообщения. Для его создания можно нажать на кнопку «Добавить ключ…» («Add Key…») или на кнопку «Менеджер ключей OpenPGP» («OpenPGP Key Manager»). Также получить доступ к генерации ключевой пары можно было напрямую, из пункта главного меню «Инструменты» через пункт подменю «Менеджер ключей OpenPGP».

После выбора Менеджера ключей OpenPGP следует выбрать последний пункт главного меню окна «Создание» («Generate») | «Новая ключевая пара» («New Key Pair») (см. рисунок 5.4). Откроется диалоговое окно «До-

бавить персональный ключ OpenPGP для alice@cryptohaven.net» (вместо адреса электронной почты alice@cryptohaven.net будет подставлен адрес Вашей учетной записи).

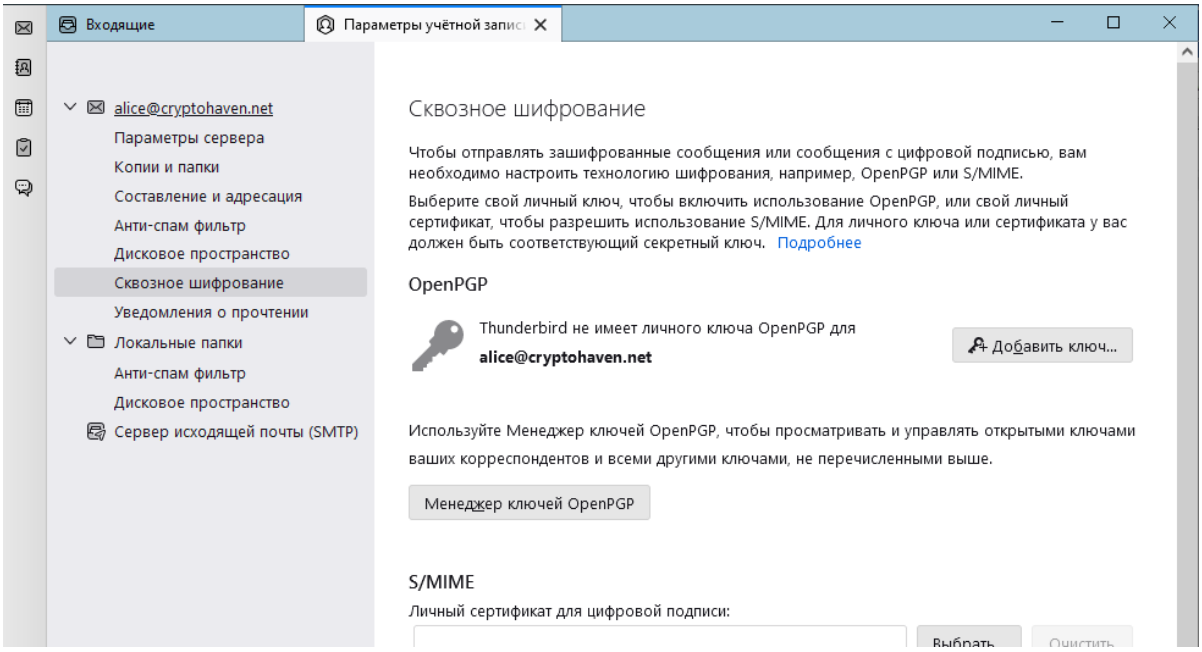

Рисунок 5.3 – Меню сквозного шифрования

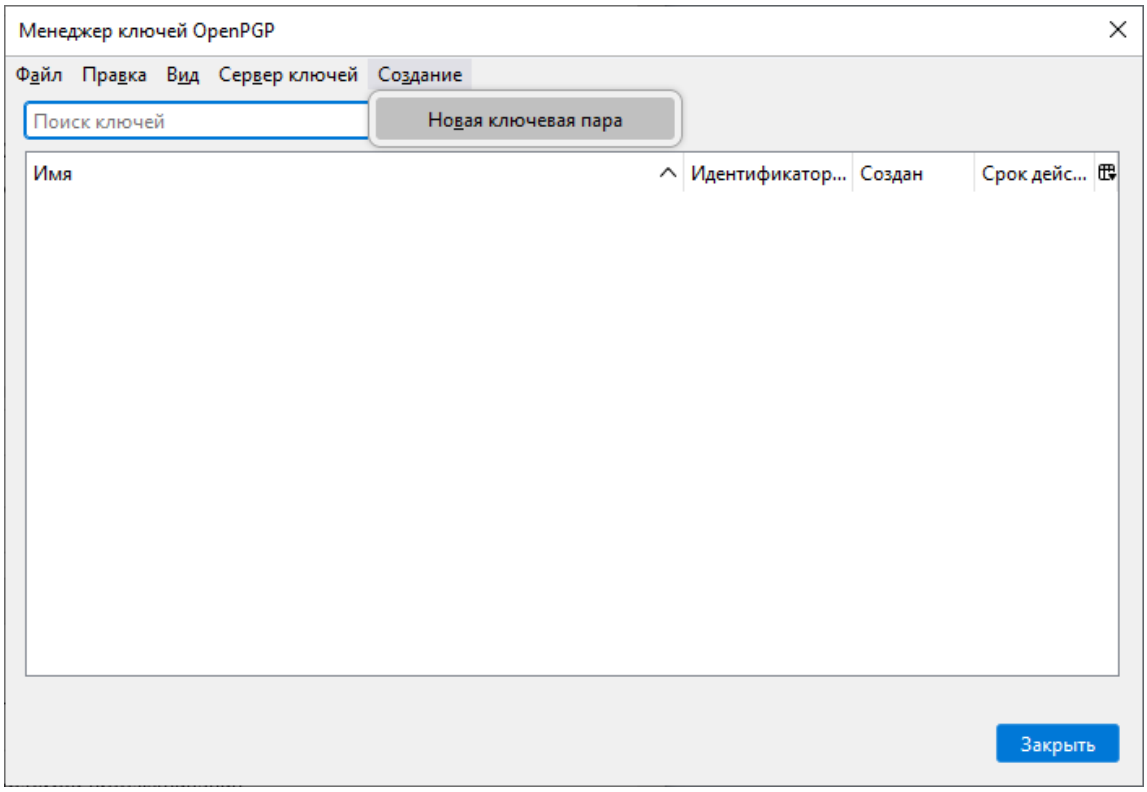

Рисунок 5.4 – Окно Менеджера ключей OpenPGP

В открывшемся окне можно настроить параметры генерации ключевой пары для учетной записи электронной почты:

– Если в программе настроено несколько учетных записей выбрать в выпадающем списке «Личность» нужную учетную запись;
– Задать срок действия ключа (для тестовых целей ограничим его 30 днями);
– Указать алгоритм шифрования, который будет использоваться для ключей (на приведенном ниже рисунке 5.5 выбрана криптографический алгоритм RSA);
– Указать длину ключа (на приведенном скриншоте – 3072 бита).

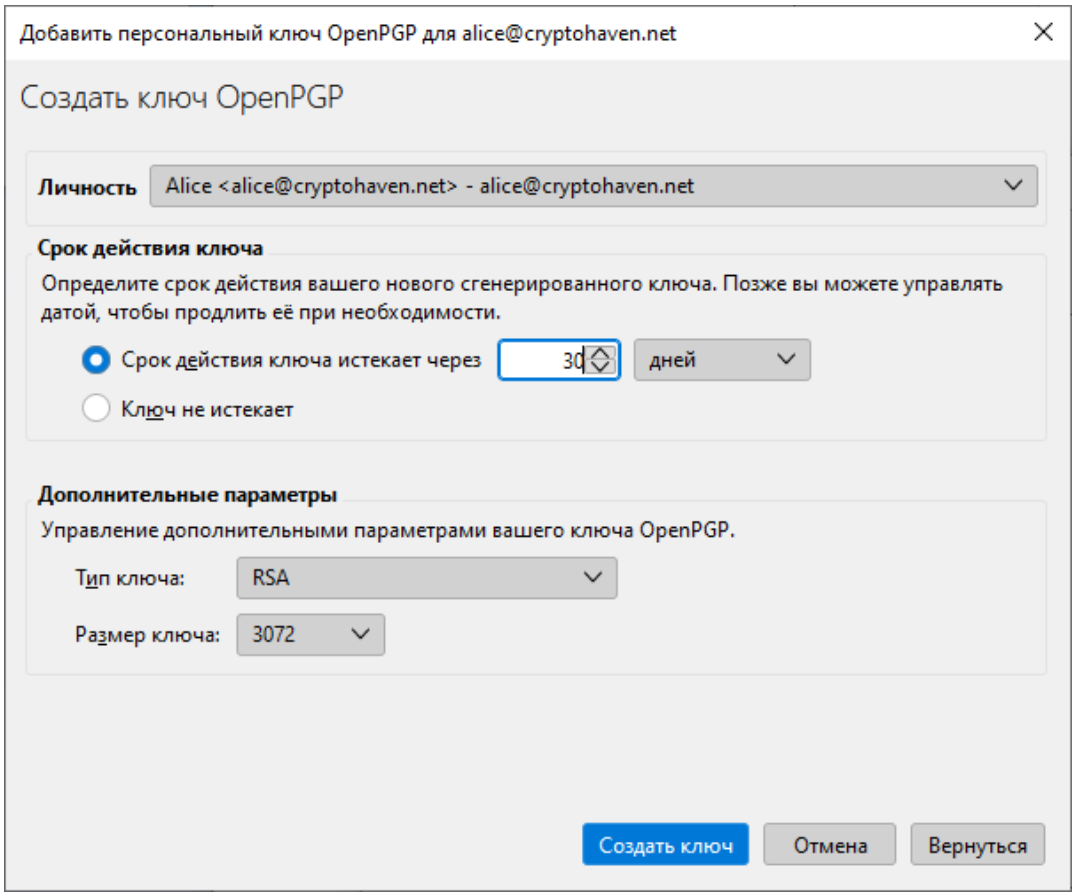

Рисунок 5.5 – Окно добавления ключевой пары OpenPGP

После генерации ключевой пары данные о публичном ключе появятся в окне Менеджера ключей OpenPGP. Более подробную информацию о ключевой паре можно просмотреть, если выполнить двойной клик на записи об этом ключе в окне. Закрываем окно Менеджера ключей OpenPGP. Теперь в разделе «Сквозное шифрование» появился новый личный ключ OpenPGP, который можно выбрать по его идентификатору для подписи сообщений (см. рисунок 5.6).

Ниже в этом же окне «Сквозное шифрование» можно настроить необходимое поведение почтового клиента:

– Флажок «Подписывать незашифрованные сообщения» задает добавление электронной цифровой подписи к каждому незашифрованному сообщению (зашифрованные подписываются автоматически);
– Флажок «Прикреплять мой открытый ключ при добавлении цифровой подписи OpenPGP» позволяет автоматически при подписи сообщения электронной почты добавить во вложения открытый ключ для верификации подписи (подробнее об этом ниже).

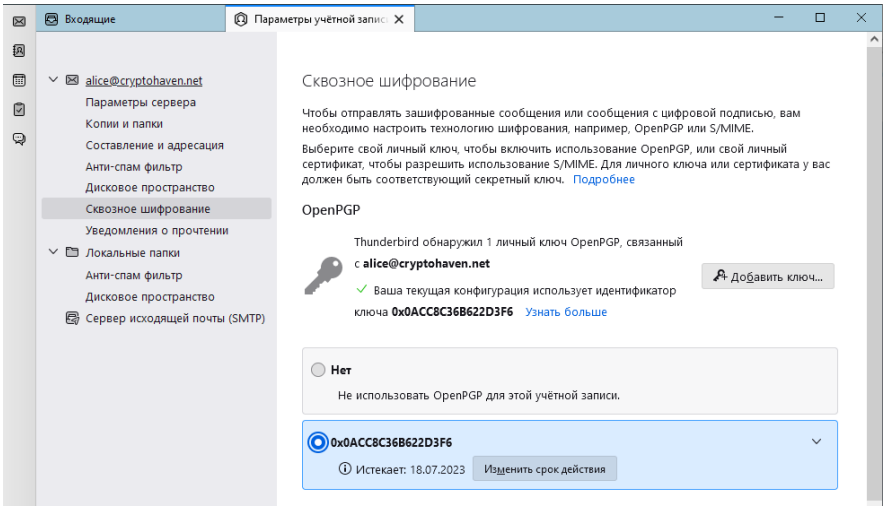

Рисунок 5.6 – Выбор личного ключа OpenPGP

Подготовим тестовое сообщение и подпишем его. Если Вы отключили автоматическую подпись незашифрованных сообщений, то сделать это можно через пункт «Безопасность» окна сообщения или через выпадающий список кнопки «OpenPGP» на панели инструментов окна (см. рисунок 5.7).

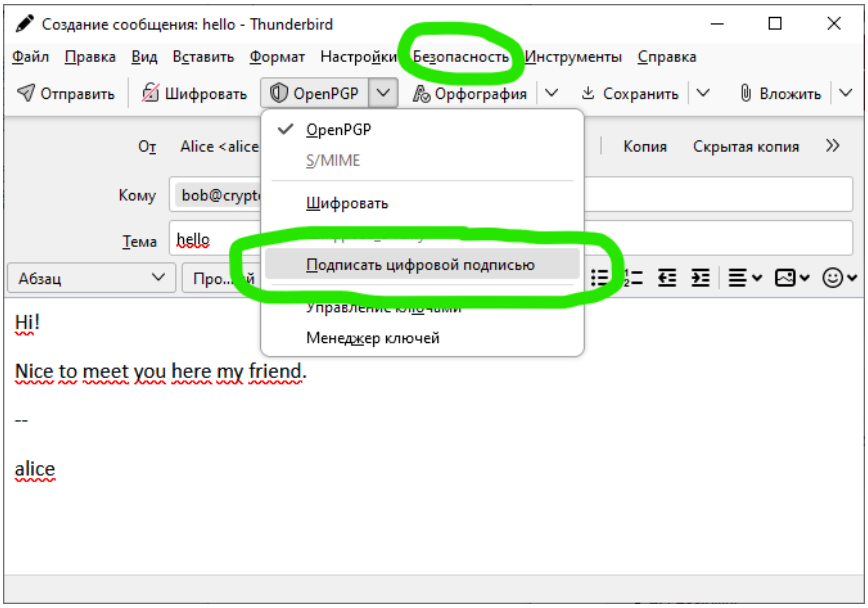

Рисунок 5.7 – Добавление подписи к сообщению

Для проверки электронной цифровой подписи у Боба должен быть открытый ключ Алисы. Один из способов выполнить это – добавить ключ к отправляемому сообщению (вопросы безопасности такого подхода рассматриваются ниже). Для этого в выпадающем списке «Вложить» на панели инструментов окна сообщения необходимо выбрать пункт «Мой открытый ключ OpenPGP» (см. рисунок 5.8).

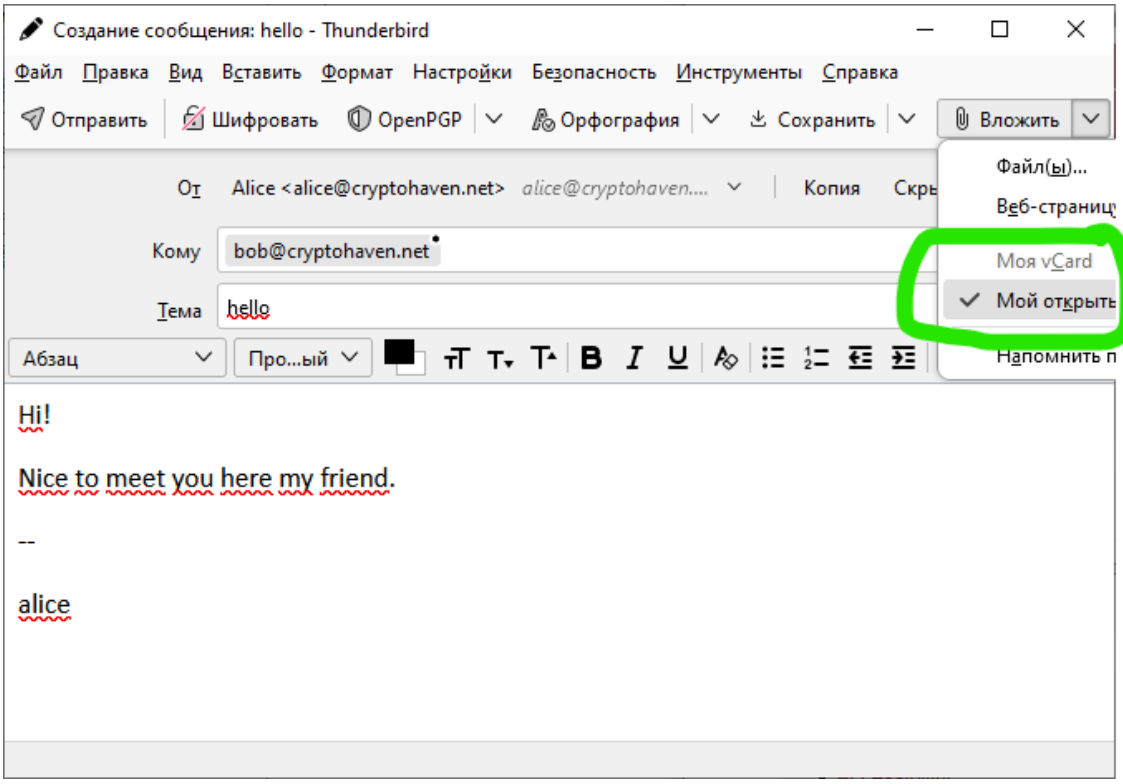

Рисунок 5.8 – Добавление открытого ключа отправителя к сообщению электронной почты

Теперь, после отправки тестового сообщения, рассмотрим действия получателя по проверке электронной цифровой подписи сообщения. Загружаем второй экземпляр почтового клиента, в котором настроена учетная запись Боба, и получаем пришедшие сообщения. Как можно видеть, сообщение от Алисы подписано (1) и содержит открытый ключ OpenPGP (2) (см. рисунок 5.9). Статус подписи сообщения электронной почты не определен – в хранилище ключевой информации почтового клиента Боба нет открытого ключа, соответствующего ключу подписи. Для решения этой проблемы Боб должен получить открытый ключ Алисы. Выполняем импорт ключа из вложения полученного электронного письма: делаем правый клик на вложении и выбираем опцию «Import OpenPGP Key».

После выполнения импорта ключа Алисы откроется диалоговое окно подтверждения, вид которого приведен на рисунке 5.10. Следует заметить,

что при передаче ключа в сообщении электронной почты этот ключ мог быть перехвачен злоумышленником, сообщение могло быть изменено и заново подписано поддельным ключом, сгенерированным злоумышленником. Для защиты от подобных атак используется инфраструктура PKI (Public Key Infrastructure) или децентрализованная модель Web of Trust. В самом простом случае, получатель сообщения, в нашем случае Боб, может проверить полученный от Алисы ключ по его отпечатку, связавшись с Алисой по какому-либо отличному от текущего каналу.

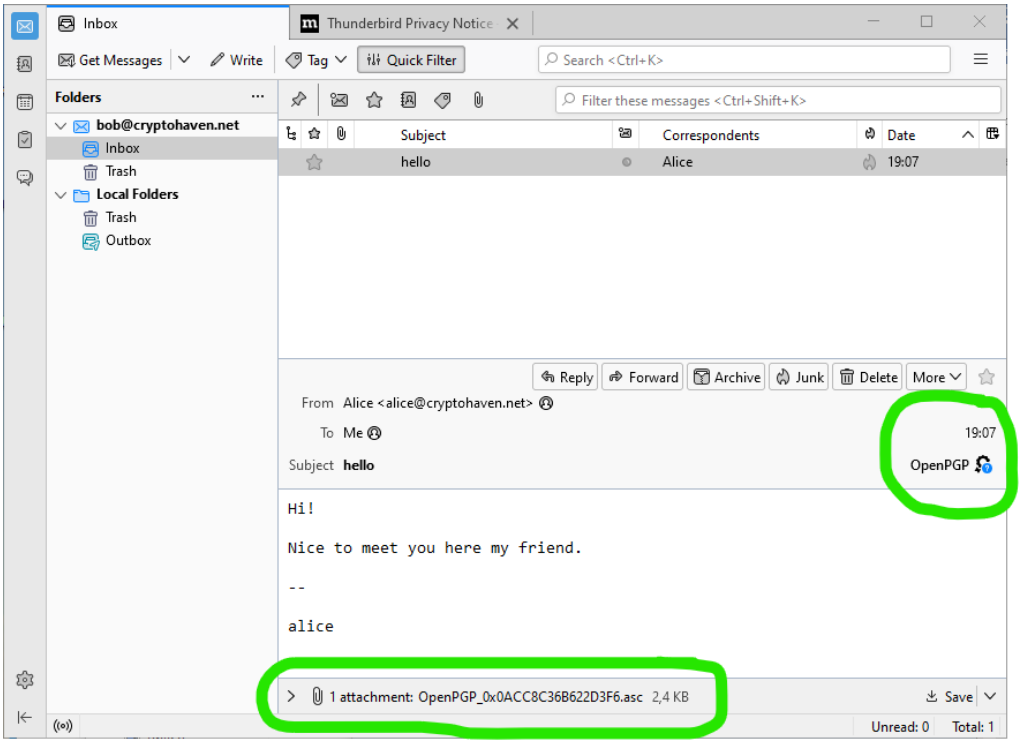

Рисунок 5.9 – Вид подписанного (и не проверенного) сообщение на стороне получателя

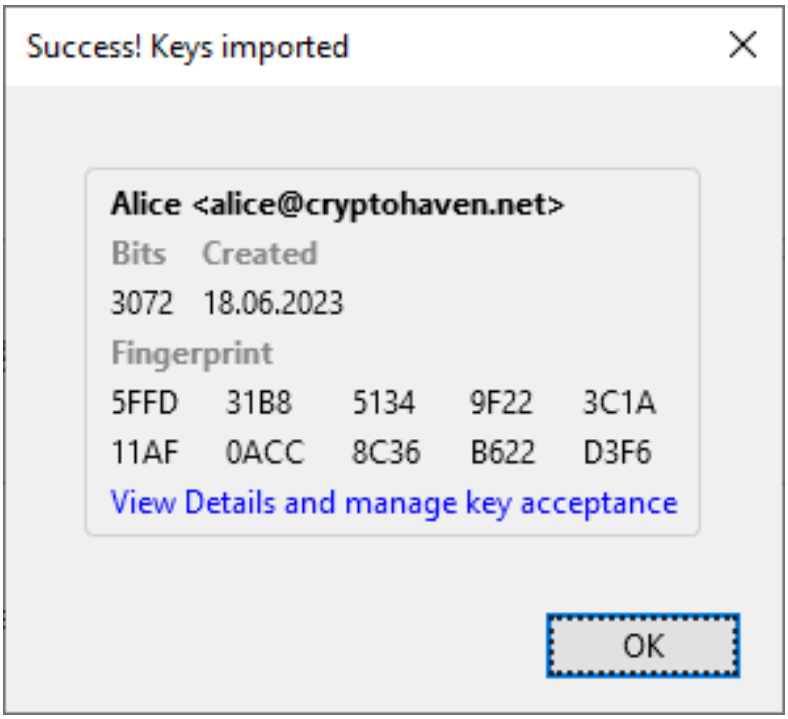

Рисунок 5.10 – Диалоговое окно импорта ключа

Предположим, что Боб не выполнил проверку ключа Алисы сразу же (не перешел по ссылке «View Details and manage key acceptance») и закрыл диалоговое окно импорта ключа. В этом случае, статус проверки электронной цифровой подписи несколько измениться (см. рисунок 5.11).

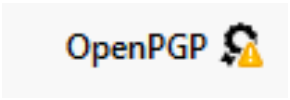

Рисунок 5.11 – Значок проверенной цифровой подписи, к ключу которой нет доверия

Для настройки уровня доверия полученному ключу, откройте Менеджер ключей OpenPGP в почтовом клиенте Боба, сделайте двойной щелчок по ключу Алисы и в открывшемся окне настройте уровень доверия полученному ключу (см. рисунок 5.12 ниже).

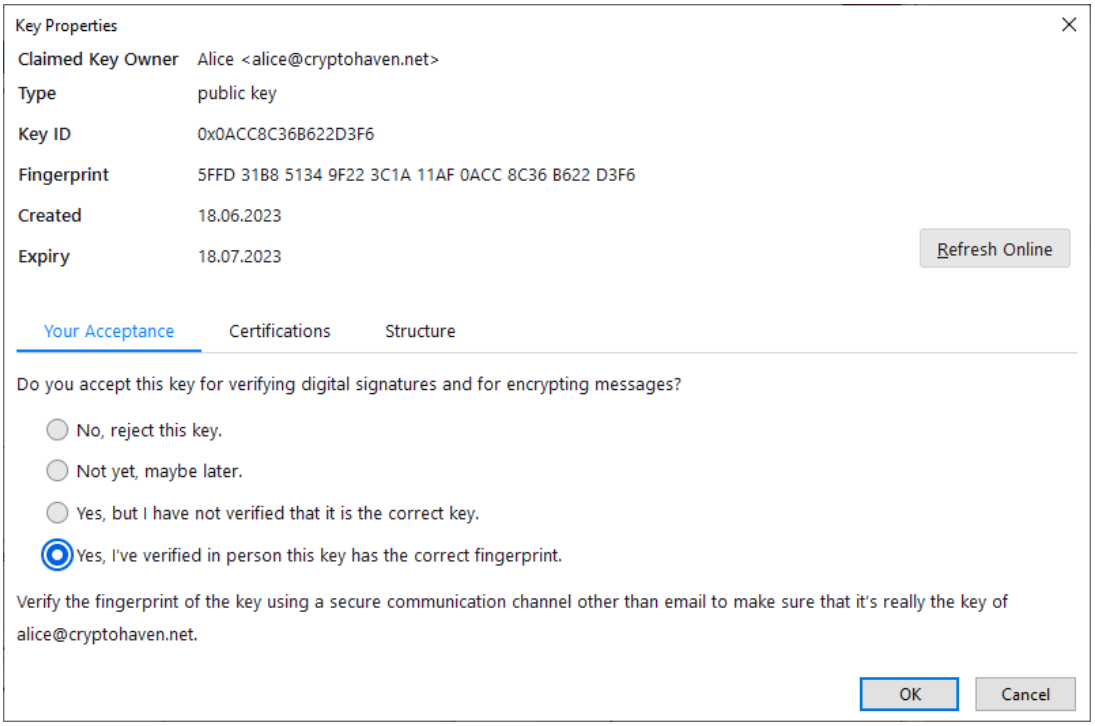

Рисунок 5.12 – Проверка отпечатка и подтверждение доверия ключу

После проверки отпечатка ключа (Fingerprint на рисунке 5.12) по телефону и настройки нужного уровня доверия ключу Алисы, статус проверки цифровой подписи у Боба должен поменяться на представленный на рисунке 5.13.

Рисунок 5.13 – Значок проверенной цифровой подписи, открытый ключ для которой был проверен

В случае, если сообщение было подделано, почтовый клиент отобразит проверку электронной цифровой подписи следующим образом (см. рисунок 5.14).

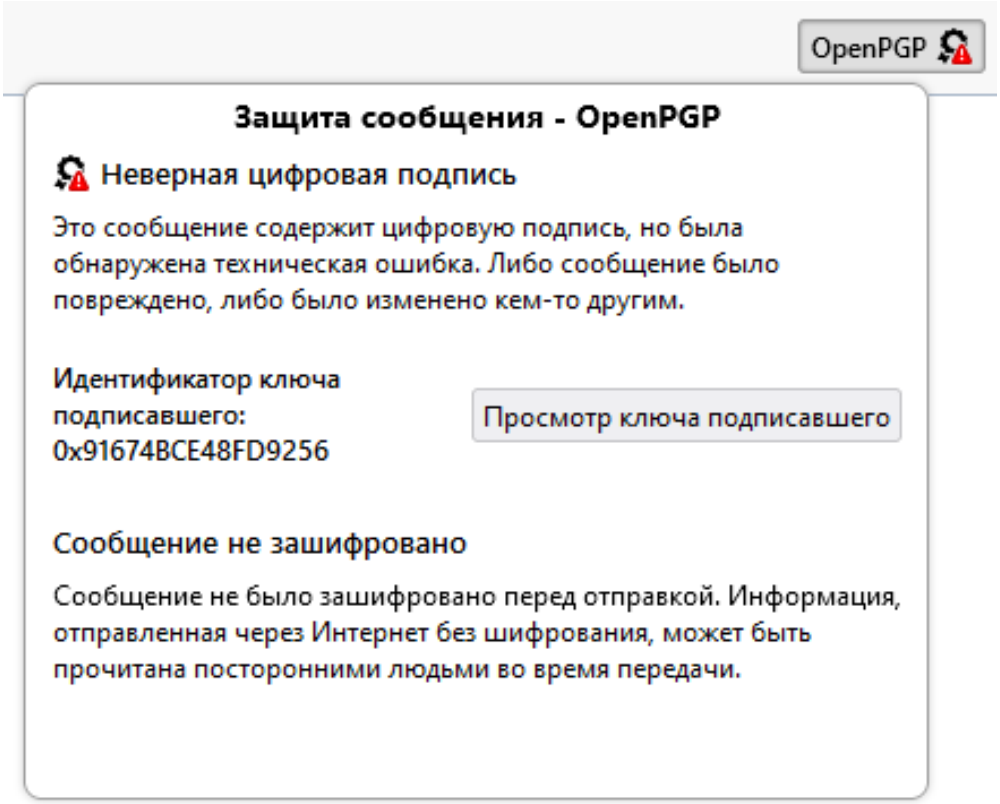

Рисунок 5.14 – Значок проверенной цифровой подписи для модифицированного сообщения

5.3 Задания для самостоятельной работы

Задание 1. Настройте необходимые параметры для подписи и последующей проверки ответного сообщения со второго аккаунта на первый. Продемонстрируйте корректную электронную цифровую подпись для ответного сообщения.

Задание 2. Попытайтесь изменить подписанное сообщение электронной почты и получить сообщение, аналогичное представленному на рисунке 5.14.

Задание 3. Подпишите (самоподписанным ключом) любое собственное приложение.

СПИСОК ЛИТЕРАТУРЫ

1. Security auditing – Windows Security | Microsoft Learn [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview.
2. Randy's Windows Security Log Encyclopedia [Электронный ресурс]. – Режим доступа: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx
3. Audit File System – Windows Security | Microsoft Learn [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-file-system
4. Appendix L – Events to Monitor | Microsoft Learn [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
5. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. – Москва: ДМК Пресс, 2010. – 544 с.
6. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей. – Москва: Инфра-М, 2014. – 416 с.
7. Как расшифровать данные EFS с помощью сертификата пользователя | Windows для системных администраторов [Электронный ресурс]. – Режим доступа: http://winitpro.ru/index.php/2014/01/24/kak-rasshifrovat-dannyx-efs-s-pomoshhyu-sertifikata-polzovatelya/. – Дата доступа: 19.06.2023.
8. Обзор BitLocker – Windows Security | Microsoft Learn [Электронный ресурс]. – Microsoft, 2023. – Режим доступа: https://docs.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-overview. – Дата доступа: 19.06.2023. (К)
9. Базовое развертывание BitLocker – Windows Security | Microsoft Learn [Электронный ресурс]. – Microsoft, 2023.
10. Использование manage-bde для управления BitLocker: [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/ru-ru/windows/security/information-protection/bitlocker/bitlocker-basic-deployment. – Дата доступа: 19.06.2023.
11. ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ 28 декабря 2009 г. № 113-З. 2/1665. (12.01.2010). Об электронном документе и электронной цифровой подписи [Электронный ресурс]. – Режим доступа: http://www.pravo.by/pdf/2010-15/2010-15(087-101).pdf. – Дата доступа: 19.06.2023.

Учебное издание

НОВЫЙ Вадим Владимирович

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические рекомендации
по выполнению лабораторных работ

Технический редактор *Г.В. Разбоева*
Компьютерный дизайн *Е.А. Барышева*

Подписано в печать 06.07.2023. Формат 60x84 $^{1}/_{16}$. Бумага офсетная.
Усл. печ. л. 1,86. Уч.-изд. л. 1,56. Тираж 45 экз. Заказ 69.

Издатель и полиграфическое исполнение – учреждение образования
«Витебский государственный университет имени П.М. Машерова».

Свидетельство о государственной регистрации в качестве издателя,
изготовителя, распространителя печатных изданий
№ 1/255 от 31.03.2014.

Отпечатано на ризографе учреждения образования
«Витебский государственный университет имени П.М. Машерова».
210038, г. Витебск, Московский проспект, 33.