**Лабораторные работы по дисциплине «Защита электронного (технологического) документооборота»**

**Лабораторная работа №1**

**Тема: *Использование цифровых сертификатов***

*Цель выполнения лабораторной работы:*

Изучение вопросов использования цифровых сертификатов.

*Порядок выполнения лабораторной работы:*

Обратиться к странице любого интернет-банка для установления защищенного соединения на основе использования протокола SSL/TSL. Получить контекстное меню для префикса https, выбрать пункт "Просмотр сертификата" и получить данные о сертификате (владелец, срок, субъект).

Проанализировать хранящиеся на учебном компьютере сертификаты.

Для этого из меню «Пуск —> Выполнить» запустить консоль командой mmc. В меню «Консоль» выбрать «Добавить или удалить оснастку», в списке оснасток выбрать «Сертификаты», пункт «Моя учетная запись» и просмотреть сертификаты текущего пользователя.

В разделе "Доверенные корневые центры сертификации" представлен достаточно список центров, чьи сертификаты поставляются вместе с операционной системой. Найти в нем сертификат VeriSign Class 3 Public Primary CA, на основе которого при подключении к системам Интернет-банкинга браузер может подтвердить подлинность узла.

Проанализировать находящиеся в разделе "Сертификаты, к которым нет доверия" отозванные сертификаты.

Получить на сайте одного из центров сертификации (например, Thawte http://www.thawte.com) бесплатный сертификат для электронной почты. Для этого необходимо заполнить анкету, подтвердить запрос и получить сертификат по электронной почте. Проверить появление личного сертификата.

Настроить почтовый клиент Microsoft Outlook на использование сертификата для защиты почты. Для этого можно использовать встроенную в поддержку протокола S/MIME. Для выбора сертификата надо выбрать меню «Сервис —> Параметры —> Безопасность» и в параметрах шифрованной электронной почты выбрать используемый сертификат и алгоритмы.

*Форма и содержание отчёта*

Отчёт должен содержать:

1. Титульный лист установленного образца.

2. Отчет о сертификате интернет-банка.

3. Отчет о хранящихся на учебном компьютере сертификатах.

4. Отчет о полученном и настроенном сертификате для электронной почты.

**Лабораторная работа №2**

**Тема: *Создание центра сертификации (удостоверяющего центра)*.**

*Цель выполнения лабораторной работы:*

Изучение возможностей центра сертификации.

*Порядок выполнения лабораторной работы:*

Изучить функции и архитектуру центра сертификации (ЦС).

Установить на компьютер виртуальную машину с серверной операционной системой.

Добавить серверу роль Active Directory Certificate Services с помощью оснастки Server Manager, которую можно запустить из раздела Administrative Tools в стартовом меню. В Server Manager раскрыть список ролей и выбрать добавление роли (Add Roles). В списке доступных ролей выбрать Active Directory Certificate Services.

Определить тип центра сертификации как корпоративный (Enterprise). Тип Certification Authority Enterprise может быть установлен только на сервер, являющийся членом домена, т.к. для его работы требуется служба каталога Active Directory. Certification Authority Standalone может работать вне домена, например, обрабатывая запросы пользователей, полученные через web-интерфейс.

Определить иерархический тип ЦС – корневой (Root) или подчиненный (Subordinate). Создаваемый ЦС является первым и единственным, поэтому для него определен тип Root.

Создаваемый центр сертификации должен будет использовать при работе как минимум одну ключевую пару - открытый и секретный ключ (иначе он не сможет подписывать выпускаемые сертификаты). Поэтому необходимо определить, нужно ли создать новый секретный ключ или будет использоваться уже существующий (тогда надо будет указать, какой ключ использовать). В лабораторной работе надо создать новый ключ, для чего. требуется выбрать "криптографический провайдер" (программный модуль, реализующий криптоалгоритмы) и алгоритм хеширования. Предлагается использовать настройки по умолчанию.

Необходимо также указать имя ЦС, размещение базы сертификатов и лог-файлов.

Управлять работой ЦC можно из оснастки Certification Authority, которая должна появиться в разделе Administrative Tools. Просмотреть сделанные настройки в свойствах данного сервера (пункт Properties контекстного меню).

На закладке Policy Module (пункт Properties) проверить текущую настройку, определяющую порядок выдачи сертификатов. Описать, какие шаблоны сертификатов (Certificate Templates) определены и для каких целей служит каждый тип сертификатов. Посмотреть, какие сертификаты выпущены (Issued Certificates), есть ли отозванные сертификаты (Revoked Certificates).

Выполнить процесс получения цифрового сертификата с помощью оснастки Certificates, в разделе сертификатов пользователя (Personal). Из перечня предложенных шаблонов сертификатов выберать User. Данный тип сертификатов может использоваться для шифрования файлов с помощью EFS, защиты электронной почты и аутентификации пользователей. Для пользователя будет сгенерирована ключевая пара, и на основе данных, взятых из базы службы Active Directory и шаблона, будет выпущен сертификат, удостоверяющий открытый ключ. Этот сертификат будет виден и в оснастке Certification Authority, в списке выпущенных данным сервером.

Изучить состав сертификата, его назначение.

Выполнить экспорт сертификата (в оснастке Certificates выделить сертификат и в контекстном меню выберать All Tasks —> Export). Экспортировать можно только сертификат или сертификат вместе с секретным ключом (private key). Второй вариант надо использовать аккуратно, чтобы не раскрыть случайно секретный ключ шифрования. Такой тип экспорта нужен, если необходимо сохранить резервную копию ключевой пары и сертификата.

*Форма и содержание отчёта*

Отчёт должен содержать:

1. Титульный лист установленного образца.

2. Описание функций и архитектуры центра сертификации.

3. Отчет о создании центра сертификации.

4. Отчет о получении цифрового сертификата в созданном центре сертификации.

**Лабораторная работа №3**

**Тема: *Шифрование данных при хранении***

*Цель выполнения лабораторной работы:*

Изучение шифрующей файловой системы Encrypting File System - EFS.

*Порядок выполнения лабораторной работы:*

Проанализировать необходимость шифрования отдельных папок и файлов и оценить возможность снижения рисков информационной безопасности.

Изучить работу EFS. Войти под своей учетной записью и с помощью оснастки Certificates запросить сертификат (можно выбрать шаблон User или Basic EFS). После этого появляется ключевая пара и сертификат открытого ключа. Для шифрования папки в ее свойствах на вкладке General нажать кнопку Advanced, получить доступ к атрибуту, указывающему на шифрование файла, и выполнить шифрование. Проверить выполнение операций добавления файлов в папку, переименования папки, копирования на другой диск с файловой системой NFTS на том же компьютере, копирования папки на сетевой диск или диск с FAT.

Войти под учетной записью другого пользователя и попытаться получить доступ к папке и файлам в ней для операций чтения, копирования, переименования и удаления.

Снова войти под своей учетной записью. В оснастке Certificates, удалить сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершить сессию пользователя в системе и войти заново. Попробовать открыть зашифрованный файл и выполнить с ним другие операции.

Войти под учетной записью администратора (агент восстановления по умолчанию). Попробовать расшифровать папку, открыть зашифрованный файл и выполнить с ним другие операции.

Отредактировать групповую политику таким образом, чтобы убрать из системы агента восстановления (удалить в политике сертификат). С помощью оснастки Group Policy Management в политике домена найти группу Public Key Policies, пункт Encrypting File System, где указан сертификат агента восстановления. Отредактировать политику (пункт Edit в контекстном меню, далее Policies —> Windows Settings —> Security Settings —> Public Key Policies —> Encrypting File System). Выполнить команду "gpupdate /force" (меню Start—>run—> gpupdate /force) и применить политику.

Повторить все предыдущие действия с папкой под разными учетными записями пользователей. Проанализировать результаты.

Вернуть в систему агента восстановления. Для шифрования определить использование нового сертификата, для чего в редакторе политик выбрать политику Encrypting File System, и в контекстном меню выбрать Create Data Recovery Agent. Это приведет к тому, что пользователь Administrator получит новый сертификат и с этого момента сможет восстанавливать шифруемые файлы. Проверить результат.

Сделать выводы.

*Форма и содержание отчёта*

Отчёт должен содержать:

1. Титульный лист установленного образца.

2. Описание шифрующей файловой системы EFS.

3. Отчет о шифровании папки и действиях с ней под разными учетными записями.

4. Выводы по работе.

**Лабораторная работа №4**

**Тема: *Реализация электронной подписи на основе открытого коллективного ключа***

*Цель выполнения лабораторной работы:*

Изучение возможности применения механизмов электронной подписи для технологического электронного документооборота.

*Порядок выполнения лабораторной работы:*

Изучить стандартные алгоритмы создания электронной подписи на основе открытого коллективного ключа (ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, RSA, схема Шнорра).

Разработать алгоритм формирования и проверки электронной подписи на основе открытого коллективного ключа (ЭП ОКК), который в общем виде состоит из трёх этапов: формирования ЭП ОКК на основе генерации индивидуальных параметров подписи и применения функции, отображающих их в коллективный параметр подписи; собственно, создание ЭП ОКК и отправка её вместе с электронным документом соответствующим пользователям АСУ предприятия; проверка ЭП ОКК с использованием открытого коллективного ключа.

На основе одного из указанных стандартов разработать схему формирования и проверки ЭП ОКК, соответствующую обобщенному методу ЭП ОКК.

Реализовать разработанную схему на языке программирования С++ (С#) и протестировать полученный код.

*Форма и содержание отчёта*

Отчёт должен содержать:

1. Титульный лист установленного образца.

2. Описание выбранного алгоритма ЭП ОКК с обоснованием.

3. Блок-схему формирования и проверки ЭП ОКК.

4. Результаты тестирования программы.

**Лабораторная работа №5**

**Тема: *Анализ существующих систем электронного документооборота***

*Цель выполнения лабораторной работы:*

Изучение существующих систем электронного документооборота и оценивание их с точки зрения защиты информации.

*Порядок выполнения лабораторной работы:*

Проанализировать и сравнить не менее 3 представленных на рынке систем электронного документооборота (СЭД) по основным функциональным характеристикам, архитектурным особенностям и встроенным механизмам защиты информации.

*Форма и содержание отчёта*

Отчёт должен содержать:

1. Титульный лист установленного образца.

2. Отчет по сравнительному анализу выбранных СЭД.

3. Выводы.