**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПбГУТ))) **Документ подписан простой электронной подписью**

Сертификат: 00fd759708ffd39703
Владелец: Бачевский Сергей Викторович
Действителен с 15.03.2021 по 14.03.2026

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
О.В. Колбанева
21 апреля 2021 г

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

по междисциплинарному курсу

МДК.02.01. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ЗАЩИТЫ

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

среднего профессионального образования

Санкт-Петербург
2021

СОДЕРЖАНИЕ

Лабораторная работа 1
СРЕДСТВА ИДЕНТИФИКАЦИИ АУТЕНТИФИКАЦИИ ОПЕРАЦИОННЫХ СИСТЕМ

1. Цель работы: изучить модели безопасности операционных систем, получить навыки практического использования средств обеспечения безопасности информационных систем.

2. Задачи работы:

− научиться работать со средствами идентификации аутентификации операционных систем

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

1. Запустите в программе Oracle VM Virtualbox виртуальную машину WinXP. Войдите в систему под учетной записью администратора, пароль узнайте у преподавателя. Все действия выполняйте в системе, работающей на виртуальной машине.

2. Создайте учетную запись нового пользователя testUser в оснастке «Управление компьютером» (compmgmt.msc). При создании новой учетной записи запретите пользователю смену пароля и снимите ограничение на срок действия его пароля. Создайте новую группу ”testGroup” и включите в нее нового пользователя. Удалите пользователя из других групп. Создайте на диске C: папку forTesting. Создайте или скопируйте в эту папку несколько текстовых файлов (*.txt).

3. С помощью команды runas запустите сеанс командной строки (cmd.exe) от имени вновь созданного пользователя. Командой whoami посмотрите SID пользователя и всех его групп, а также текущие привилегии пользователя. Строку запуска и результат работы этой и всех следующих консольных команд копируйте в файл протокола лабораторной работы.

4. Убедитесь в соответствии имени пользователя и полученного SID в реестре Windows. Найдите в реестре, какому пользователю в системе присвоен SID S-1-5-21-

1957994488-492894223-170857768-1004 (Используйте ключ реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList).

5. Командой whoami определите перечень текущих привилегий пользователя testUser. В сеансе командной строки пользователя попробуйте изменить системное время командой time. Чтобы предоставить пользователю подобную привилегию, запустите оснастку «Локальные параметры безопасности» (secpol.msc). Добавьте пользователя в список параметров политики «Изменение системного времени» раздела Локальные политики -> Назначение прав пользователя. После этого перезапустите сеанс командной строки от имени пользователя, убедитесь, что в списке привилегий добавилась SeSystemtimePriviege. Попробуйте изменить системное время командой time.

Убедитесь, что привилегия «Завершение работы системы» (SeShutdownPrivilege) предоставлена пользователю testUser . После этого попробуйте завершить работу системы из сеанса командной строки пользователя командой shutdown –s. Добавть ему привелегию «Принудительное удаленное завершение» (SeRemoteShutdownPrivilege). Попробуйте завершить работу консольной командой еще раз (отменить команду завершения до ее непосредственного выполнения можно командой shutdown –a).

6. Ознакомьтесь с справкой по консольной команде cacls. Используя эту команду, просмотрите разрешения на папку c:\forTesting. Объясните все обозначения в описаниях прав пользователей и групп в выдаче команды.

а) Разрешите пользователю testUser запись в папку forTesting, но запретите запись для группы testGroup. Попробуйте записать файлы или папки в forTesting от имени пользователя testUser. Объясните результат. Посмотрите эффективные разрешения пользователя testUser к папке forTesting в окне свойств папки.

б) Используя стандартное окно свойств папки, задайте для пользователя testUser такие права доступа к папке, чтобы он мог записывать информацию в папку forTesting, но не мог просматривать ее содержимое. Проверьте, что папка forTesting является теперь для пользователя testUser “слепой”, запустив, например, от его имени файловый менеджер и попробовав записать файлы в папку, просмотреть ее содержимое, удалить файл из папки.

в) Для вложенной папки forTesting\Docs отмените наследование ACL от родителя и разрешите пользователю просмотр, чтение и запись в папку. Проверьте, что для пользователя папка forTesting\Docs перестала быть “слепой” (например, сделайте ее текущей в сеансе работы файлового менеджера от имени пользователя и создайте в ней новый файл).

г) Снимите запрет на чтение папки forTesting для пользователя testUser. Используя команду cacls запретите этому пользователю доступ к файлам с расширением txt в папке forTesting. Убедитесь в недоступности файлов для пользователя.

д) Командой cacls запретите пользователю все права на доступ к папке forTesting и разреште полный доступ к вложенной папке forTesting\Docs. Убедитесь в доступности папки forTesting\Docs для пользователя. Удалите у пользователя testUser привилегию SeChangeNotifyPrivilege. Попробуйте получить доступ к папке forTesting\Docs. Объясните результат.

е) Запустите файловый менеджер от имени пользователя testUser и создайте в нем папку newFolder на диске C. Для папки newFolder очистите весь список ACL командой cacls. Попробуйте теперь получить доступ к папке от имени администратора и от имени пользователя. Кто и как теперь может вернуть доступ к папке? Верните полный доступ к папке для всех пользователей.

ж) Создайте в разделе HKLM\Software реестра раздел testKey. Запретите пользователю testUser создание новых разделов в этом разделе реестра. Создайте для раздела HKLM\Software\testKey SACL, позволяющий протоколировать отказы при создании новых подразделов, а также успехи при перечислении подразделов и запросе значений (предварительно проверьте, что в локальной политике безопасности соответствующий тип аудита включен). Попробуйте от имени пользователя testUser

запустить regedit.exe и создать раздел в HKLM\Software. Убедитесь, что записи аудита были размещены в журнале безопасности (eventvwr.msc).

7. Шифрование файлов и папок средствами EFS.

а) От имени пользователя testUser зашифруйте какой-нибудь файл на диске. Убедитесь, что после этого был создан сертификат пользователя, запустив оснастку certmgr.msc от имени пользователя (раздел Личные). Просмотрите основные параметры сертификата открытого ключа пользователя testUser (срок действия, используемые алгоритмы). Установите доверие к этому сертификату в вашей системе.

б) Создайте в папке forTesting новую папку Encrypt. В папке Encrypt создайте или скопируйте в нее текстовый файл. Зашифруйте папку Encrypt и все ее содержимое из меню свойств папки от имени администратора. Попробуйте просмотреть или скопировать какой-нибудь файл этой папки от имени пользователя testUser. Объясните результат. Скопируйте зашифрованный файл в незашифрованную папку (например, forTesting). Убедитесь что он остался зашифрованным. Добавьте пользователя testUser в список имеющих доступа к файлу пользователей в окне свойств шифрования файла. Повторите попытку получить доступ к файлу от имени пользователя testUser.

в) Создайте учетную запись нового пользователя agentUser, сделайте его членом группы Администраторы. Определите для пользователя agentUser роль агента восстановления EFS. Создайте в папке forTesting новый текстовый файл с произвольным содержимым. Зашифруйте этот файл от имени пользователя testUser. Убедитесь в окне подробностей шифрования файла, что пользователь agentUser является агентом восстановления для данного файла. Попробуйте прочитать содержимое файла от имени администратора и от имени пользователя agentUser. Объясните результат.

г) Зашифруйте все текстовые файлы папки forTesting с использованием консольной команды шифрования cipher от имени пользователя testUser (предварительно снимите запрет на доступ к этим файлам, установленный в задании 2.2.6г).

д) Убедитесь, что при копировании зашифрованных файлов на том с файловой системой, не поддерживающей EFS (например, FAT32 на флеш-накопителе), содержимое файла дешифруется.

2.2.8. После демонстрации результатов работы преподавателю восстановите исходное состояние системы: удалите созданные папки и файлы, разделы реестра, удалите учетную запись созданного пользователя и его группы, снимите с пользователя agentUser роль агента восстановления.

Представьте отчёт по лабораторной работе.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое аутентификация и на чем она базируется.
2. Что такое авторизация? Как и когда она осуществляется?
3. Примеры реализации мер безопасности ОС.
4. Какие ОС считаются наиболее защищенными и за счет чего?

Приложение 1

Краткие сведения из теории

Для начала рассмотрим проблему контроля доступа в систему. Наиболее распространенным способом контроля доступа является процедура регистрации. Обычно каждый пользователь в системе имеет уникальный идентификатор. Идентификаторы пользователей применяются с той же целью, что и идентификаторы любых других объектов, файлов, процессов. Идентификация заключается в сообщении пользователем своего идентификатора.

Для того чтобы установить, что пользователь именно тот, за кого себя выдает, то есть что именно ему принадлежит введенный идентификатор, в информационных системах предусмотрена процедура аутентификации (authentication, опознавание, в переводе с латинского означает "установление подлинности"), задача которой - предотвращение доступа к системе нежелательных лиц.

Обычно аутентификация базируется на одном или более из трех пунктов:

- То, чем пользователь владеет (ключ или магнитная карта);
- То, что пользователь знает (пароль);
- Атрибуты пользователя (отпечатки пальцев, подпись, голос).

Пароли, уязвимость паролей

Наиболее простой подход к аутентификации – применение пользовательского пароля.

Когда пользователь идентифицирует себя при помощи уникального идентификатора или имени, у него запрашивается пароль. Если пароль, сообщенный пользователем, совпадает с паролем, хранящимся в системе, система предполагает, что пользователь легитимен. Пароли часто используются для защиты объектов в компьютерной системе в отсутствие более сложных схем защиты.

Недостатки паролей связаны с тем, что трудно сохранить баланс между удобством пароля для пользователя и его надежностью. Пароли могут быть угаданы, случайно показаны или нелегально переданы авторизованным пользователем неавторизованному.

Есть два общих способа угадать пароль. Один связан со сбором информации о пользователе. Люди обычно используют в качестве паролей очевидную информацию (скажем, имена животных или номерные знаки автомобилей). Для иллюстрации важности разумной политики назначения идентификаторов и паролей можно привести данные исследований, проведенных в AT&T, показывающие, что из 500 попыток несанкционированного доступа около 300 составляют попытки угадывания паролей или беспарольного входа по пользовательским именам guest, demo и т. д.

Другой способ - попытаться перебрать все наиболее вероятные комбинации букв, чисел и знаков пунктуации (атака по словарю). Например, четыре десятичные цифры дают только 10 000 вариантов, более длинные пароли, введенные с учетом регистра символов и пунктуации, не столь уязвимы, но тем не менее таким способом удается разгадать до 25% паролей. Чтобы заставить пользователя выбрать трудноугадываемый пароль, во многих системах внедрена реактивная проверка паролей, которая при помощи собственной программы-взломщика паролей может оценить качество пароля, введенного пользователем.

Несмотря на все это, пароли распространены, поскольку они удобны и легко реализуемы.

Шифрование пароля

Для хранения секретного списка паролей на диске во многих ОС используется криптография. Система задействует одностороннюю функцию, которую просто вычислить, но для которой чрезвычайно трудно (разработчики надеются, что невозможно) подобрать обратную функцию.

Например, в ряде версий Unix в качестве односторонней функции используется модифицированный вариант алгоритма DES. Введенный пароль длиной до 8 знаков преобразуется в 56-битовое значение, которое служит входным параметром для процедуры crypt(), основанной на этом алгоритме. Результат шифрования зависит не только от введенного пароля, но и от случайной последовательности битов, называемой привязкой (переменная salt). Это сделано для того, чтобы решить проблему совпадающих паролей. Очевидно, что саму привязку после шифрования необходимо сохранять, иначе процесс не удастся повторить. Модифицированный алгоритм DES выполняется, имея входное значение в виде 64-битового блока нулей, с использованием пароля в качестве ключа, а на каждой следующей итерации входным параметром служит результат предыдущей итерации. Всего процедура повторяется 25 раз. Полученное 64-битовое значение преобразуется в 11 символов и хранится рядом с открытой переменной salt.

В ОС Windows NT преобразование исходного пароля также осуществляется многократным применением алгоритма DES и алгоритма MD4.

Хранятся только кодированные пароли. В процессе аутентификации представленный пользователем пароль кодируется и сравнивается с хранящимися на диске. Таким образом, файл паролей нет необходимости держать в секрете.

При удаленном доступе к ОС нежелательна передача пароля по сети в открытом виде. Одним из типовых решений является использование криптографических протоколов. В качестве примера можно рассмотреть протокол опознавания с подтверждением установления связи путем вызова - CHAP (Challenge Handshake Authentication Protocol).

Опознавание достигается за счет проверки того, что у пользователя, осуществляющего доступ к серверу, имеется секретный пароль, который уже известен серверу.

Пользователь инициирует диалог, передавая серверу свой идентификатор. В ответ сервер посылает пользователю запрос (вызов), состоящий из идентифицирующего кода, случайного числа и имени узла сервера или имени пользователя. При этом пользовательское оборудование в результате запроса пароля пользователя отвечает следующим ответом, зашифрованным с помощью алгоритма одностороннего хеширования, наиболее распространенным видом которого является MD5. После получения ответа сервер при помощи той же функции с теми же аргументами шифрует собственную версию пароля пользователя. В случае совпадения результатов вход в систему разрешается. Существенно, что незашифрованный пароль при этом по каналу связи не посылается.

В микротелефонных трубках используется аналогичный метод.

В системах, работающих с большим количеством пользователей, когда хранение всех паролей затруднительно, применяются для опознавания сертификаты, выданные доверенной стороной.

Авторизация. Разграничение доступа к объектам ос

После успешной регистрации система должна осуществлять авторизацию (authorization) - предоставление субъекту прав на доступ к объекту. Средства авторизации контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые были определены администратором, а также осуществляют контроль возможности выполнения пользователем различных системных функций. Система контроля базируется на общей модели, называемой матрицей доступа. Рассмотрим ее более подробно.

Компьютерная система может быть смоделирована как набор субъектов (процессы, пользователи) и объектов. Под объектами мы понимаем как ресурсы оборудования (процессор, сегменты памяти, принтер, диски и ленты), так и программные ресурсы (файлы, программы, семафоры), то есть все то, доступ к чему контролируется. Каждый объект имеет

уникальное имя, отличающее его от других объектов в системе, и каждый из них может быть доступен через хорошо определенные и значимые операции.

Операции зависят от объектов. Например, процессор может только выполнять команды, сегменты памяти могут быть записаны и прочитаны, считыватель магнитных карт может только читать, а файлы данных могут быть записаны, прочитаны, переименованы и т. д.

Желательно добиться того, чтобы процесс осуществлял авторизованный доступ только к тем ресурсам, которые ему нужны для выполнения его задачи. Это требование минимума привилегий, уже упомянутое в предыдущей лекции, полезно с точки зрения ограничения количества повреждений, которые процесс может нанести системе. Например, когда процесс P вызывает процедуру A, ей должен быть разрешен доступ только к переменным и формальным параметрам, переданным ей, она не должна иметь возможность влиять на другие переменные процесса. Аналогично компилятор не должен оказывать влияния на произвольные файлы, а только на их хорошо определенное подмножество (исходные файлы, листинги и др.), имеющее отношение к компиляции. С другой стороны, компилятор может иметь личные файлы, используемые для оптимизационных целей, к которым процесс P не имеет доступа.

Различают дискреционный (избирательный) способ управления доступом и полномочный (мандатный).

При дискреционном доступе, подробно рассмотренном ниже, определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам или группам субъектов. С концептуальной точки зрения текущее состояние прав доступа при дискреционном управлении описывается матрицей, в строках которой перечислены субъекты, в столбцах – объекты, а в ячейках – операции, которые субъект может выполнить над объектом.

Полномочный подход заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда это называют моделью многоуровневой безопасности, которая должна обеспечивать выполнение следующих правил.

Простое свойство секретности. Субъект может читать информацию только из объекта, уровень секретности которого не выше уровня секретности субъекта. (Генерал читает документы лейтенанта, но не наоборот).

Субъект может записывать информацию в объекты только своего уровня или более высоких уровней секретности. (Генерал не может случайно разгласить нижним чинам секретную информацию).

Некоторые авторы утверждают, что последнее требование называют *– свойством, потому что в оригинальном докладе не смогли придумать для него подходящего названия. В итоге во все последующие документы и монографии оно вошло как *– свойство.

Отметим, что данная модель разработана для хранения секретов, но не гарантирует целостности данных. Например, здесь лейтенант имеет право писать в файлы генерала.

Большинство операционных систем реализуют именно дискреционное управление доступом. Главное его достоинство - гибкость, основные недостатки - рассредоточенность управления и сложность централизованного контроля.

Выявление вторжений. Аудит системы защиты

Даже самая лучшая система защиты рано или поздно будет взломана. Обнаружение попыток вторжения является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения. Как правило, поведение взломщика отличается от поведения легального пользователя. Иногда эти различия можно выразить количественно, например подсчитывая число некорректных вводов пароля во время регистрации.

Основным инструментом выявления вторжений является запись данных аудита. Отдельные действия пользователей протоколируются, а полученный протокол используется для выявления вторжений.

Аудит, таким образом, заключается в регистрации специальных данных о различных типах событий, происходящих в системе и так или иначе влияющих на состояние безопасности компьютерной системы. К числу таких событий обычно причисляют следующие:

- вход или выход из системы;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- обращение к удаленной системе;
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. Следует предусматривать наличие средств выборочного протоколирования как в отношении пользователей, когда слежение осуществляется только за подозрительными личностями, так и в отношении событий. Слежка важна в первую очередь как профилактическое средство. Можно надеяться, что многие воздержатся от нарушений безопасности, зная, что их действия фиксируются.

Помимо протоколирования, можно периодически сканировать систему на наличие слабых мест в системе безопасности. Такое сканирование может проверить разнообразные аспекты системы:

- короткие или легкие пароли;
- неавторизованные set-uid программы, если система поддерживает этот механизм;
- неавторизованные программы в системных директориях;
- долго выполняющиеся программы;
- нелогичная защита как пользовательских, так и системных директорий и файлов. Примером нелогичной защиты может быть файл, который запрещено читать его автору, но в который разрешено записывать информацию постороннему пользователю;
- потенциально опасные списки поиска файлов, которые могут привести к запуску «троянского коня»;
- изменения в системных программах, обнаруженные при помощи контрольных сумм.

Любая проблема, обнаруженная сканером безопасности, может быть как ликвидирована автоматически, так и передана для решения менеджеру системы.

Анализ некоторых ос с точки зрения их защищенности

ОС должна способствовать реализации мер безопасности или непосредственно поддерживать их. Примерами подобных решений в рамках аппаратуры и операционной системы могут быть:

- разделение команд по уровням привилегированности;
- сегментация адресного пространства процессов и организация защиты сегментов;
- защита различных процессов от взаимного влияния за счет выделения каждому своего виртуального пространства;
- особая защита ядра ОС;
- контроль повторного использования объекта;
- наличие средств управления доступом;
- структурированность системы, явное выделение надежной вычислительной базы (совокупности защищенных компонентов), обеспечение компактности этой базы;
- следование принципу минимизации привилегий – каждому компоненту дается ровно столько привилегий, сколько необходимо для выполнения им своих функций.

Большое значение имеет структура файловой системы. Например, в ОС с дискреционным контролем доступа каждый файл должен храниться вместе с дискреционным списком прав

доступа к нему, а, например, при копировании файла все атрибуты, в том числе и ACL, должны быть автоматически скопированы вместе с телом файла.

В принципе, меры безопасности не обязательно должны быть заранее встроены в ОС – достаточно принципиальной возможности дополнительной установки защитных продуктов. Так, сугубо ненадежная система MS-DOS может быть усовершенствована за счет средств проверки паролей доступа к компьютеру и/или жесткому диску, за счет борьбы с вирусами путем отслеживания попыток записи в загрузочный сектор CMOS-средствами и т. п. Тем не менее, по-настоящему надежная система должна изначально проектироваться с акцентом на механизмы безопасности.

MS-DOS

ОС MS-DOS функционирует в реальном режиме (real-mode) процессора i80x86. В ней невозможно выполнение требования, касающегося изоляции программных модулей (отсутствует аппаратная защита памяти). Уязвимым местом для защиты является также файловая система FAT, не предполагающая у файлов наличия атрибутов, связанных с разграничением доступа к ним. Таким образом, MS-DOS находится на самом нижнем уровне в иерархии защищенных ОС.

OS/2

OS/2 работает в защищенном режиме (protected-mode) процессора i80x86. Изоляция программных модулей реализуется при помощи встроенных в этот процессор механизмов защиты памяти. Поэтому она свободна от указанного выше коренного недостатка систем типа MS-DOS. Но OS/2 была спроектирована и разработана без учета требований по защите от несанкционированного доступа. Это сказывается прежде всего на файловой системе. В файловых системах OS/2 HPFS (high performance file system) и FAT нет места ACL. Кроме того, пользовательские программы имеют возможность запрета прерываний. Следовательно, сертификация OS/2 на соответствие какому-то классу защиты не представляется возможной.

Считается, что такие операционные системы, как MS-DOS, Mac OS, Windows, OS/2, имеют уровень защищенности D (по оранжевой книге). Но, если быть точным, нельзя считать эти ОС даже системами уровня безопасности D, ведь они никогда не представлялись на тестирование.

Unix

Рост популярности Unix и все большая осведомленность о проблемах безопасности привели к осознанию необходимости достичь приемлемого уровня безопасности ОС, сохранив при этом мобильность, гибкость и открытость программных продуктов. В Unix есть несколько уязвимых с точки зрения безопасности мест, хорошо известных опытным пользователям, вытекающих из самой природы Unix. Однако хорошее системное администрирование может ограничить эту уязвимость.

Относительно защищенности Unix сведения противоречивы. В Unix изначально были заложены идентификация пользователей и разграничение доступа. Как оказалось, средства защиты данных в Unix могут быть доработаны, и сегодня можно утверждать, что многие клоны Unix по всем параметрам соответствуют классу безопасности С2.

Обычно, говоря о защищенности Unix, рассматривают защищенность автоматизированных систем, одним из компонентов которых является Unix-сервер. Безопасность такой системы увязывается с защитой глобальных и локальных сетей, безопасностью удаленных сервисов типа telnet и rlogin/rsh и аутентификацией в сетевой конфигурации, безопасностью X Window-приложений. На системном уровне важно наличие средств идентификации и аудита.

В Unix существует список именованных пользователей, в соответствии с которым может быть построена система разграничения доступа.

В ОС Unix считается, что информация, нуждающаяся в защите, находится главным образом в файлах.

По отношению к конкретному файлу все пользователи делятся на три категории:

- владелец файла;
- члены группы владельца;
- прочие пользователи.

Для каждой из этих категорий режим доступа определяет права на операции с файлом, а именно:

- право на чтение;
- право на запись;
- право на выполнение (для каталогов - право на поиск).

В итоге девяти (3x3) битов защиты оказывается достаточно, чтобы специфицировать ACL каждого файла.

Аналогичным образом защищены и другие объекты ОС Unix, например семафоры, сегменты разделяемой памяти и т. п.

Указанных видов прав достаточно, чтобы определить допустимость любой операции с файлами. Например, для удаления файла необходимо иметь право на запись в соответствующий каталог. Как уже говорилось, права доступа к файлу проверяются только на этапе открытия. При последующих операциях чтения и записи проверка не выполняется. В результате, если режим доступа к файлу меняется после того, как файл был открыт, это не сказывается на процессах, уже открывших этот файл. Данное обстоятельство является уязвимым с точки зрения безопасности местом.

Наличие всего трех видов субъектов доступа: владелец, группа, все остальные - затрудняет задание прав "с точностью до пользователя", особенно в случае больших конфигураций. В популярной разновидности Unix - Solaris имеется возможность использовать списки управления доступом (ACL), позволяющие индивидуально устанавливать права доступа отдельных пользователей или групп.

Среди всех пользователей особое положение занимает пользователь root, обладающий максимальными привилегиями. Обычные правила разграничения доступа к нему не применяются - ему доступна вся информация на компьютере.

В Unix имеются инструменты системного аудита - хронологическая запись событий, имеющих отношение к безопасности. К таким событиям обычно относят: обращения программ к отдельным серверам; события, связанные с входом/выходом в систему и другие. Обычно регистрационные действия выполняются специализированным syslog-демоном, который проводит запись событий в регистрационный журнал в соответствии с текущей конфигурацией. Syslog-демон стартует в процессе загрузки системы.

Таким образом, безопасность ОС Unix может быть доведена до соответствия классу С2. Однако разработка на ее основе автоматизированных систем более высокого класса защищенности может быть сопряжена с большими трудозатратами.

Windows NT/2000/XP/Vista

Принцип «тысячи глаз» всегда упоминают сторонники программного обеспечения с открытыми исходными кодами, подчеркивая, что продукты категории Open Source просматривает множество разработчиков, которые обязательно найдут ошибку, если она есть. Поэтому, по их словам, открытые коды более безопасны, чем закрытые, которые никто кроме разработчиков не видел. Между тем, существует огромное количество открытого кода, который фактически вообще не анализировался с точки зрения безопасности, в то время как самый известный коммерческий программный продукт — операционная система Windows — напротив, активно анализируется на предмет ее защищенности.

В отличие от семейства Unix где все задачи разграничения доступа решаются средствами управления доступом к объектам файловой системы в ОС семейства Windows разграничение доступа осуществляется собственным механизмом каждого ресурса. При рассмотрении механизмов защиты Windows встает задача определения что является объектом доступа.

Так же как и в Unix основными механизмами защиты Windows являются

- идентификация и аутентификация пользователя при входе в систему
- разграничение прав доступа к файловой системе в основе которой лежит дискреционный (произвольный) метод доступа
- аудит или регистрация событий

По сравнению с Unix в файловой системе NTFS существенно увеличены возможности разграничения прав доступа к файлам. За счет того что существенно увеличен набор атрибутов доступа к файловым объектам. Например, атрибут исполнения может устанавливаться и на каталог, при этом все файлы хранящиеся в каталоге автоматически наследуют это атрибут. Однако при этом существенно ограничены возможности управления доступом к другим защищаемым ресурсам. Например устройствам ввода. Например, здесь отсутствует атрибут исполнение. То есть невозможно запретить запуск несанкционированной программы с устройства ввода.

Основные недостатки защитных механизмов ОС Семейства Windows:

- в отличие от ОС семейства Unix в Windows не возможна реализация централизованной схемы администрирования механизмов защиты. То есть невозможно выполнение соответствующих формализованных требований. Это связано с тем, что в Windows используется другая концепция разграничительной политики доступа к ресурсам. В рамках этой концепции разграничение для файлов приоритетнее чем для каталогов. Это приводит к тому, что пользователь создавая файл и являясь его владельцем может назначать любые атрибуты доступа к такому файлу. То есть разрешить к нему доступ любому другому пользователю. При этому обратиться к этому файлу может пользователь вне зависимости от прав установленных администратором на каталог. Этот недостаток связан с той моделью которая реализована в ОС семейства Windows
- в ОС семейства Windows не полностью реализуется дискреционная модель доступа. В частности не могут разграничиваться права доступа к объектам, которые создает сама система. ОС семейства Windows есть пользовательские процессы и есть системные процессы. При этом разграничение доступа к системным процессам не существует. Отсюда системные процессы имеют неограниченный доступ к защищаемым ресурсам. На этом основывается большое количество атак, когда злоумышленник запускает собственный процесс с правами системного.
- в ОС семейства Windows не возможно в общем случае обеспечить замкнутость или целостность программной среды. При этом существует коренное отличие этого недостатка который был в ОС семейства Unix. Там это недостаток был связан с невозможностью установки атрибута исполнения на каталог.

Механизм замкнутости рабочей среды может быть обеспечен с помощью 2 подходов:

- заключается в том что задается список разрешенных к запуску процессов и пользователь может запускать процессы только из этого списка. При чем пользователь не имеет возможности изменять этот список.
- разрешение запуска пользователями программ из заданных каталогов при невозможности изменения этих каталогов. В ОС Windows некорректно реализован данный подход, т.к. в Windows невозможно установить атрибут исполнение на устройства ввода (CDROM, Flash), в соответствии с этим пользователь может запустить несанкционированную программу с этих устройств, следует также отметить, что с точки зрения реализации механизма обеспечивающего возможность пользователя запускать только санкционированные программы, действия пользователя могут быть как явными так и скрытыми. Явные действия предполагают запуск процессов, которые однозначно идентифицируются своим именем, скрытые действия позволяют осуществлять встроенные в некоторые приложения интерпретаторы команд, пример - Word, excel.. При запуске программы Word идентифицируется только сама программа Word, однако скрытые действия могут осуществляться с помощью макросов встроенных в программу, которые не идентифицируются, таким образом в ОС Windows в неполном объеме осуществляется

контроль. Кроме того отсутствуют механизмы, которые позволяют очищать остаточную информацию из ОЗУ. Отсутствует аудит твердой копии информации. Отсутствует механизм управление хостами.

С момента выхода версии 3.1 осенью 1993 года в Windows NT гарантировалось соответствие уровню безопасности С2. В настоящее время (точнее, в 1999г.) сертифицирована версия NT 4 с Service Pack 6a с использованием файловой системы NTFS в автономной и сетевой конфигурации. Следует помнить, что этот уровень безопасности не подразумевает защиту информации, передаваемой по сети, и не гарантирует защищенности от физического доступа.

Компоненты защиты NT частично встроены в ядро, а частично реализуются подсистемой защиты. Подсистема защиты контролирует доступ и учетную информацию. Кроме того, Windows NT имеет встроенные средства, такие как поддержка резервных копий данных и управление источниками бесперебойного питания, которые не требуются "Оранжевой книгой", но в целом повышают общий уровень безопасности.

ОС Windows 2000 сертифицирована по стандарту Common Criteria. В дальнейшем линейку продуктов Windows NT/2000/XP, изготовленных по технологии NT, будем называть просто Windows NT.

Ключевая цель системы защиты Windows NT - следить за тем, кто и к каким объектам осуществляет доступ. Система защиты хранит информацию, относящуюся к безопасности для каждого пользователя, группы пользователей и объекта. Единообразие контроля доступа к различным объектам (процессам, файлам, семафорам и др.) обеспечивается тем, что с каждым процессом связан маркер доступа, а с каждым объектом - дескриптор защиты. Маркер доступа в качестве параметра имеет идентификатор пользователя, а дескриптор защиты - списки прав доступа. ОС может контролировать попытки доступа, которые производятся процессами прямо или косвенно инициированными пользователем.

Windows NT отслеживает и контролирует доступ как к объектам, которые пользователь может видеть посредством интерфейса (такие, как файлы и принтеры), так и к объектам, которые пользователь не может видеть (например, процессы и именованные каналы). Любопытно, что, помимо разрешающих записей, списки прав доступа содержат и запрещающие записи, чтобы пользователь, которому доступ к какому-либо объекту запрещен, не смог получить его как член какой-либо группы, которой этот доступ предоставлен.

Система защиты ОС Windows NT состоит из следующих компонентов:

- Процедуры регистрации (Logon Processes), которые обрабатывают запросы пользователей на вход в систему. Они включают в себя начальную интерактивную процедуру, отображающую начальный диалог с пользователем на экране и удаленные процедуры входа, которые позволяют удаленным пользователям получить доступ с рабочей станции сети к серверным процессам Windows NT.
- Подсистемы локальной авторизации (Local Security Authority, LSA), которая гарантирует, что пользователь имеет разрешение на доступ в систему. Этот компонент - центральный для системы защиты Windows NT. Он порождает маркеры доступа, управляет локальной политикой безопасности и предоставляет интерактивным пользователям аутентификационные услуги. LSA также контролирует политику аудита и ведет журнал, в котором сохраняются сообщения, порождаемые диспетчером доступа.
- Менеджера учета (Security Account Manager, SAM), который управляет базой данных учета пользователей. Эта база данных содержит информацию обо всех пользователях и группах пользователей. SAM предоставляет услуги по легализации пользователей, применяющиеся в LSA.
- Диспетчера доступа (Security Reference Monitor, SRM), который проверяет, имеет ли пользователь право на доступ к объекту и на выполнение тех действий, которые он пытается совершить. Этот компонент обеспечивает легализацию доступа и политику аудита,

определяемые LSA. Он предоставляет услуги для программ супервизорного и пользовательского режимов, для того чтобы гарантировать, что пользователи и процессы, осуществляющие попытки доступа к объекту, имеют необходимые права. Данный компонент также порождает сообщения службы аудита, когда это необходимо.

Microsoft Windows NT - относительно новая ОС, которая была спроектирована для поддержки разнообразных защитных механизмов, от минимальных до С2, и безопасность которой наиболее продумана. Дефолтный уровень называется минимальным, но он легко может быть доведен системным администратором до желаемого уровня.

Windows Vista

Управление учетными записями пользователей

Используя Windows XP и более ранние версии операционных систем, отделы IT должны были выбирать между высокой совместимостью приложений и удобством, которые обеспечивались при входе пользователей в систему под учетной записью администратора, и безопасностью и стабильностью работы, которые обеспечивались входом в систему пользователей под учетной записью стандартного пользователя. Управление учетными записями пользователей в Windows Vista позволяет администраторам использовать „ограниченные” разрешения, которые никак не влияют на работу большинства необходимых приложений.

Для обеспечения такой комбинации безопасности и совместимости, Windows Vista автоматически виртуализирует настройки реестра и папок всего компьютера. Изменения, вносимые в виртуализированные настройки реестра и папок, видны только под той учетной записью пользователя, который внес эти изменения, и в тех приложениях, которые запущены под его учетной записью, тем самым обеспечивается более надежная защита компьютера. Если для выполнения приложения действительно необходимы права администратора, то перед его запуском Windows Vista автоматически запросить их у пользователя.

Улучшения платформы

Возможности Windows Vista по аутентификации являются более гибкими, предоставляя широкий ассортимент в выборе специализированных механизмов аутентификации, таких как сканеры отпечатков пальцев и смарт карты. Инструменты развертывания и управления, такие как самообслуживаемый инструмент сброса личного идентификационного номера (PIN), позволяет проще управлять смарт картами и их развертывать. Теперь смарт карты также можно использовать и для входа в систему Windows Vista. Кроме этого, Windows Vista позволяет производить аутентификацию с использованием Internet протокола версии 6 (IPv6) или с использованием Web служб.

Подача заявок на сертификаты теперь сделана проще, поскольку Windows Vista включает в себя расширения Диспетчера Учетных данных (Credential Manager), позволяющего производить резервное копирование и восстановление учетных данных, сохраненных на локальном компьютере. Новая служба Digital Identity Management Service (DIMS) (Служба управления цифровыми удостоверениями) обеспечивает роуминг сертификатов и учетных данных внутри Active Directory и непрерывное сопровождение сертификата на протяжении его всего жизненного цикла с помощью управляющих сценариев.

Возможности Windows Vista по аудиту сейчас позволяют проще отслеживать действия пользователей. Категории аудита теперь включают множество подкатегорий, уменьшая количество несущественных событий. Встроенная в Windows Vista система перенаправления событий аудита накапливает и передает критические данные аудита в центральное хранилище, предоставляя возможность предприятиям лучше их систематизировать и анализировать.

Многоуровневая защита данных

Хищение или потеря корпоративной интеллектуальной собственности вызывают все большее беспокойство в организациях. Windows Vista имеет улучшенную поддержку для защиты данных в документах, файлах, директориях, и на разных уровнях оборудования. Встроенный клиент Управления правами (Rights Management) позволяет организациям принудительно устанавливать политику пользования документами. В файловую систему с шифрованием (Encrypting File System), обеспечивающую шифрование файлов и папок на основе данных о пользователе, было внесено расширение, позволяющее теперь хранить ключи шифрования на смарт картах, обеспечивая их лучшую защиту. Кроме того, новая функция для предприятия BitLocker добавляет защиту данных на уровне оборудования. Она обеспечивает шифрование всего системного тома, включая системные файлы Windows и файл (hibernation), создаваемый при использовании Спящего режима, тем самым помогая защитить данные, находящиеся на потерянном, похищенном ИЛИ СПИСАННОМ оборудовании. Чтобы обеспечить такое решение, которое можно было бы с легкостью разворачивать и управлять, используется чип Trusted Platform Module (TPM) 1.2 (Модуль Доверительной Платформы) для хранения ключей шифрования и дешифрования секторов на жестком диске Windows. Чтобы сделать эту функцию гарантированно простой в использовании для конечного пользователя, на предприятии необходимо наличие инфраструктуры управления TPM.

Windows Vista по умолчанию настроена таким образом, что все запускаемые приложения, которые могут навредить системе или данным запускаются только с согласия пользователя. С одной стороны это может предотвратить дестабилизацию системы и заражение вирусами. А с другой стороны постоянные подтверждения, надоев пользователю, будут им игнорироваться.

Лабораторная работа 2

НАСТРОЙКА ЛОКАЛЬНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ. ПОЛИТИКА ПАРОЛЕЙ. ПОЛИТИКИ УЧЕТНЫХ ЗАПИСЕЙ

1. **Цель работы**: изучить встроенные в операционную систему средства администрирования пользователей и управления безопасностью системы.

2. **Задачи работы:**

- настраивать локальную политику безопасности операционной системы;
- настраивать параметры политики безопасности локального компьютера на примере переименования гостевой учетной записи

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

1. Изучите процедуру настройки параметров политики безопасности локального компьютера на примере переименования гостевой учетной записи.

1.1. Открыть оснастку Локальные политики безопасности или перейти на вкладку Параметры безопасности оснастки Редактор локальной групповой политики.

1.2. Перейти последовательно на вкладку Локальные политики, затем вкладку Параметры безопасности.

1.3. Открыть параметр Учетные записи: Переименование учетной записи гостя, дважды щелкнув на нем или нажав на клавишу Enter.

1.4. В текстовом поле ввести Гостевая запись и нажать кнопку «ОК».

1.5. Перезагрузить компьютер. После перезагрузки компьютера следует убедиться, что политика безопасности была применена именно к данному компьютеру. Для этого необходимо открыть на панели управления компоненту Учетные записи пользователей и перейти по ссылке Управление другой учетной записью. В открывшемся окне будут

отображены все учетные записи, созданные на данном локальном компьютере, в том числе переименованная учетная запись гостя.

2. Для просмотра и изменения параметров аутентификации пользователя выполнить следующие действия.

2.1. Выбрать кнопку Пуск панели задач.

2.2. Открыть меню Панель управления.

2.3. В открывшемся окне выбрать ярлык Администрирование.

2.4. Далее выбрать пункт Локальная политика безопасности.

2.5. Выбрать опцию Политика учетных записей. Данная опция содержит два подпункта: Политика паролей и Политика блокировки учетной записи.

2.6. Открыть подпункт Политика паролей.

2.7. В правой части окна появится список настраиваемых параметров.

2.8. Открыть вкладку Свойства: Пароль должен отвечать требованиям сложности.

2.9. Изменить значение параметра и нажать кнопку ОК. Выбрать параметр Вести журнал паролей (в некоторых модификациях операционных систем данный параметр может называться Требование не повторяемости паролей) и изменить его значение на 1.

2.10. Настроить блокировку учетной записи. Для этого выбрать и открыть опцию Политика блокировки учетной записи.

3. Предоставить отчет.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Настройка «Локальной политики безопасности» в Windows 10.
2. Настройка политик учетных записей
3. Настройка параметров безопасности операционной системы

Приложение 1

Краткие сведения из теории

Политика паролей

При помощи этого узла вы можете изменять настройки паролей учетных записей пользователей, которые состоят как в домене, так и в рабочих группах. В организациях вы можете применять одинаковые политики паролей для всех пользователей, входящих в домен или только для отдельных групп при помощи оснастки **«Консоль управления групповыми политиками»**. В узле **«Политика паролей»** вы можете использовать до шести политик безопасности, при помощи которых можно указать наиболее важные параметры безопасности, применяемые для управления паролями учетных записей. Настоятельно рекомендую не игнорировать данные политики. Даже если вы уговорите своих пользователей использовать сложные пароли, не факт, что они действительно будут это делать. Если вы правильно настроите все шесть политик безопасности, расположенных в этом узле, безопасность паролей пользователей вашей организации значительно повысится. Применив все политики, пользователям действительно придется создавать безопасные пароли, в отличие от тех, которые они считают «сложными». Доступны следующие политики безопасности:

- **Вести журнал паролей**. Насколько не был бы ваш пароль безопасным, злоумышленник рано или поздно сможет его подобрать. Поэтому необходимо периодически изменять пароли учетных записей. При помощи этой политики вы можете указать количество новых паролей, которые назначаются для учетных записей до повторного использования старого пароля. После того как эта политика будет настроена, контроллер домена будет проверять кэш предыдущих хэш-кодов пользователей, чтобы в качестве нового пароля пользователи не могли использовать старый. Число паролей может варьироваться от 0 до 24. Т.е., если вы указали в качестве параметра число 24, то пользователь сможет использовать старый пароль с 25-ого раза.
- **Максимальные срок действия пароля**. Эта политика указывает период времени, в течение которого пользователь может использовать свой пароль до последующего изменения. По окончанию установленного срока пользователь обязан изменить свой пароль, так как без изменения пароля войти в систему ему не удастся. Доступные значения могут быть установлены в промежутке от 0 до 999 дней. Если установлено значения равное 0, срок действия пароля неограничен. В связи с мерами безопасности желательно отказаться от такого выбора. Если значения максимального срока действия пароля варьируется от 1 до 999 дней, значение минимального срока должно быть меньше максимального. Лучше всего использовать значения от 30 до 45 дней.
- **Минимальная длина пароля**. При помощи этой политики вы можете указать минимальное количество знаков, которое должно содержаться в пароле. Если активировать этот параметр, то при вводе нового пароля количество знаков будет сравниваться с тем, которое установлено в этой политике. Если количество знаков будет меньше указанного, то придется изменить пароль в соответствии с политикой безопасности. Можно указать значение политики от 1 до 14 знаков. Оптимальным значением для количества знаков для пароля пользователей является 8, а для серверов от 10 до 12.
- **Минимальные срок действия пароля**. Многие пользователи не захотят утруждать себя запоминанием нового сложного пароля и могут попробовать сразу при вводе изменить такое количество новых паролей, чтобы использовать свой хорошо известный первоначальный пароль. Для предотвращения подобных действий была разработана текущая политика безопасности. Вы можете указать минимальное количество дней, в течение которого пользователь должен использовать свой новый пароль. Доступные значения этой политики устанавливаются в промежутке от 0 до 998 дней. Установив значение равное 0 дней, пользователь сможет изменить пароль сразу после создания нового. Необходимо обратить внимание на то, что минимальный срок действия нового пароля не должен превышать значение максимального срока действия.

- **Пароль должен отвечать требованиям сложности**. Это одна из самых важных политик паролей, которая отвечает за то, должен ли пароль соответствовать требованиям сложности при создании или изменении пароля. В связи с этими требованиями, пароли должны:
  - содержать буквы верхнего и нижнего регистра одновременно;
  - содержать цифры от 0 до 9;
  - содержать символы, которые отличаются от букв и цифр (например, !, @, #, $, *);
  - Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

В том случае, если пользователь создал или изменил пароль, который соответствует требованиям, то пароль пропускается через математический алгоритм, преобразовывающий его в хэш-код (также называемый односторонней функцией), о котором шла речь в политике «Вести журнал паролей».

- **Хранить пароли, используя обратимое шифрование**. Для того чтобы пароли невозможно было перехватить при помощи приложений, Active Directory хранит только хэш-код. Но если перед вами встанет необходимость поддержки приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности, вы можете использовать текущую политику. Обратимое шифрование по умолчанию отключено, так как, используя эту политику, уровень безопасности паролей и всего домена, в частности, значительно понижается. Использование этой функции аналогично хранению пароля в открытом виде.

Политика блокировки учетной записи

Даже после создания сложного пароля и правильной настройки политик безопасности, учетные записи ваших пользователей все еще могут быть подвергнуты атакам недоброжелателей. Например, если вы установили минимальный срок действия пароля в 20 дней, у хакера достаточно времени для подбора пароля к учетной записи. Узнать имя учетной записи не является проблемой для хакеров, так как, зачастую имена учетных записей пользователей совпадает с именем адреса почтового ящика. А если будет известно имя, то для подбора пароля понадобится какие-то две-три недели.

Групповые политики безопасности Windows могут противостоять таким действиям, используя набор политик узла «Политика блокировки учетной записи». При помощи данного набора политик, у вас есть возможность ограничения количества некорректных попыток входа пользователя в систему. Разумеется, для ваших пользователей это может быть проблемой, так как не у всех получится ввести пароль за указанное количество попыток, но зато безопасность учетных записей перейдет на «новый уровень».

- **Время до сброса счетчиков блокировки.** Active Directory и групповые политики позволяют автоматически разблокировать учетную запись, количество попыток входа в которую превышает установленное вами пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Вы можете установить значение от одной минуты до 99999. Это значение должно быть меньше значения политики «Продолжительность блокировки учетной записи».
- **Пороговое значение блокировки.** Используя эту политику, вы можете указать количество некорректных попыток входа, после чего учетная запись будет заблокирована. Окончание периода блокировки учетной записи задается политикой «Продолжительность блокировки учетной записи» или администратор может разблокировать учетную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. Я рекомендую устанавливать допустимое количество от трех до семи попыток.

- **Продолжительность блокировки учетной записи.** При помощи этого параметра вы можете указать время, в течение которого учетная запись будет заблокирована до ее автоматической разблокировки. Вы можете установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0, учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную.

Политика Kerberos

В доменах Active Directory для проверки подлинности учетных записей пользователей и компьютеров домена используется протокол Kerberos. Сразу после аутентификации пользователя или компьютера, этот протокол проверяет подлинность указанных реквизитов, а затем выдает особый пакет данных, который называется «Билет предоставления билета (TGT – Ticket Granting Ticket)». Перед подключением пользователя к серверу для запроса документа на контроллер домена пересылается запрос вместе с билетом TGT, который идентифицирует пользователя, прошедшего проверку подлинности Kerberos. После этого контроллер домена передает пользователю еще один пакет данных, называемый билетом доступа к службе. Пользователь предоставляет билет на доступ службе на сервере, который принимает его как подтверждение прохождения проверки подлинности.

Данный узел вы можете обнаружить только на контроллерах домена. Доступны следующие пять политик безопасности:

- **Максимальная погрешность синхронизации часов компьютера.** Для предотвращения «атак повторной передачи пакетов» существует текущая политика безопасности, которая определяет максимальную разность времени, допускающую Kerberos между временем клиента и временем на контроллере домена для обеспечения проверки подлинности. В случае установки данной политики, на обоих часах должны быть установлены одинаковые дата и время. Подлинной считается та отметка времени, которая используется на обоих компьютерах, если разница между часами клиентского компьютера и контроллера домена меньше максимальной разницы времени, определенной этой политикой.
- **Максимальный срок жизни билета пользователя.** При помощи текущей политики вы можете указать максимальный интервал времени, в течение которого может быть использован билет представления билета (TGT). По истечении срока действия билета TGT необходимо возобновить существующий билет или запросить новый.
- **Максимальный срок жизни билета службы.** Используя эту политику безопасности, сервер будет выдавать сообщение об ошибке в том случае, если клиент, запрашивающий подключение к серверу, предъявляет просроченный билет сеанса. Вы можете определить максимальное количество минут, в течение которого полученный билет сеанса разрешается использовать для доступа к конкретной службе. Билеты сеансов применяются только для проверки подлинности на новых подключениях к серверам. После того как подключение пройдет проверку подлинности, срок действия билета теряет смысл.
- **Максимальный срок жизни для возобновления билета пользователя.** С помощью данной политики вы можете установить количество дней, в течение которых может быть восстановлен билет предоставления билета.
- **Принудительные ограничения входа пользователей.** Эта политика позволяет определить, должен ли центр распределения ключей Kerberos проверять каждый запрос билета сеанса на соответствие политике прав, действующей для учетных записей пользователей.

Лабораторная работа 3
НАЗНАЧЕНИЕ ПРАВ ПОЛЬЗОВАТЕЛЯ

1. Цель работы: научиться создавать учетные записи пользователей и группы, а также изучить управление ими.

2. Задачи работы:

- создавать, редактировать и удалять учетные записи пользователей;
- назначать и отменять привилегии

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

1. Откройте оснастку Управление компьютером в разделе Администрирование Панели управления.
2. В оснастке Локальные пользователи и группы установите указатель мыши на папку Пользователи и нажмите правую кнопку.
3. В появившемся контекстном меню выберите команду Новый пользователь. Появится окно диалога Новый пользователь.
4. В поле Пользователь введите имя создаваемого пользователя, например, свою фамилию.

Примечание. Имя пользователя должно быть уникальным для компьютера. Оно может содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо: »/ \ []:; =,+*?<> Имя пользователя не может состоять целиком из точек и пробелов.

5. В поле Полное имя введите полное имя создаваемого пользователя.
6. В поле Описание введите описание создаваемого пользователя или его учетной записи, например, «студент …».

7. В поле Пароль введите пароль пользователя и в поле Подтверждение подтвердите его правильность вторичным вводом.

Примечание. Длина пароля не может превышать 14 символов.

8. Установите или снимите флажки:

- потребовать смену пароля при следующем входе в систему;
- запретить смену пароля пользователем;
- срок действия пароля не ограничен;
- отключить учетную запись.

9. Чтобы создать еще одного пользователя, нажмите кнопку Создать и повторите шаги с 1 по 8. Для завершения работы нажмите кнопку Создать и затем Закрыть.

11. В окне оснастки Локальные пользователи и группы установите указатель мыши на папке Группы и нажмите правую кнопку.

12. В появившемся контекстном меню выберите команду Новая группа.

13. В поле Имя группы введите имя новой группы, например, Студенты.

Примечание. Имя локальной группы должно быть уникальным в пределах компьютера. Оно может содержать до 256 символов в верхнем и нижнем регистрах.

14. В поле Описание введите описание новой группы.

15. В поле Члены группы можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку Добавить и выбрать их в списке. Для завершения нажмите кнопку Создать и затем Закрыть.

16.В окне оснастки Локальные пользователи и группы щелкните на папке Группы.

17.В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку.

18.В появившемся контекстном меню выберите команду Добавить в группу или Свойства.

19.Для того, чтобы добавить новые учетные записи в группу, нажмите кнопку Добавить (рис. 12).

20.Далее следуйте указаниям окна диалога Выбор: Пользователи или Группы.

21.Для того, чтобы удалить из группы некоторых пользователей, в поле Члены группы окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку Удалить.

Примечание. В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в нее пользователей.

22.Откройте оснастку Управление компьютером.

23.Для этого либо выберите на Рабочем столе ярлык Мой компьютер и нажмите правую клавишу мыши, после чего выберите пункт контекстного меню Управление, либо воспользуйтесь разделом Администрирование в Панели управления.

24.В открывшейся оснастке выберите пункты Служебные программы/Локальные пользователи и группы.

25.Откройте папку Пользователи и выберите учетную запись Гость.

26.Нажмите правую клавишу мыши и выберите пункт Свойства.

27.В открывшемся окне снимите отметку пункта Отключить учетную запись.

28.Нажмите кнопку ОК и сделайте вывод о состоянии учетной записи.

8.Выполните пункт 26 и отметьте пункт Отключить учетную запись.

6. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;

4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Что такое назначение прав пользователя?
2. Какие виды прав пользователей существуют?
3. Как определяются права пользователя в операционных системах?
4. Какие проблемы могут возникнуть при назначении прав пользователей?
5. Какие меры безопасности необходимо принять при назначении прав пользователей?
6. Как изменить назначенные права пользователей?
7. Какие роли пользователей могут быть определены в рамках системы управления правами?
8. Как управлять правами доступа к файлам и папкам?
9. Какие принципы обеспечивают правильное назначение прав пользователей?

Приложение 1

Краткие сведения из теории

Привилегии – это возможность выполнять связанные с системой операции, например выключение компьютера или изменение системного времени.

Право – разрешает или запрещает выполнять конкретный тип входа в систему, например локальный или вход по сети.

Для того чтобы управлять **привилегиями и правами**, нужно использовать MMC-оснастку "**Локальная политика безопасности**" (**secpol.msc**). В этой оснастке можно настроить и права и привилегии для пользователей или групп. Вы можете различить права от привилегий тем, что права связаны со входом в систему, а привилегии не связаны.

Права учетной записи

Права хоть и находятся в одной и той же оснастке с привилегиями, но технически отличаются т привилегий. Они не связаны с монитором безопасности SRM и не хранятся в маркерах доступа в отличие от привилегий.

Возможные права:

право локального входа в систему (logon locally);
возможность входить в систему по сети (logon over the network);
право входить в систему через службу терминалов (logon through Terminal Services);
возможность входить в систему в качестве службы (logon as a service);
возможность входить в систему в качестве пакетного задания (logon as a batch job).

Привилегии

- Привилегии пользователя находятся в маркере доступа. А вот не полный список привилегий:

- Резервное копирование файлов и каталогов. Заставляет NTFS предоставлять некоторый доступ к файлам, даже если дескриптор безопасности не дает таких разрешений.
- Восстановление файлов и каталогов. Заставляет NTFS предоставлять некоторый доступ к файлам, даже если дескриптор безопасности не дает таких разрешений.
- Повышение приоритета планирования. Требуется для повышения приоритета процесса.
- Загрузка и выгрузка драйверов устройств.
- Добавление рабочих станций в домен.
- Выполнение операций сопровождения с томом. Например, выполнение дефрагментации или проверка диска.
- Изменение маркера объекта. Например, разрешает запуск программ от имени администратора.
- Управление аудитом и журналом безопасности. Необходимо для обращения к списку SACL.
- Выключение системы.
- Изменение системного времени.
- Получение прав владения. Для файлов и других объектов.

Лабораторная работа 4
НАСТРОЙКА ИЗОЛИРОВАННОЙ СРЕДЫ

1. Цель работы: научиться разворачивать изолированные среды с помощью специального программного обеспечения, изучить программное обеспечение, предназначенное для этого.

2. Задачи работы:

- Выполнять развертывание и настройку изолированной среды

Студент должен:

Иметь практический опыт:

- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

1. Нажмите сочетание клавиш Win+x.
2. В открывшемся меню выберите пункт «Приложения и компоненты».
3. На открывшейся странице ищем ссылку «Программы и компоненты» и нажимаем по ней.
4. В открывшемся окне, в левой части, нажмите «Включение и отключение компонентов».
5. В появившемся перечне компонентов найдите «Песочница Windows» и поставьте напротив него галочку.
6. После применения изменений перезагрузите компьютер.

6. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

7. ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Как запустить песочницу Windows?
2. Для чего используется изолированная среда?
3. Какие ещё есть средства для изолирования среды?

Приложение 1

Краткие сведения из теории

Windows обладает достаточно обширным набором функций и утилит для изменения конфигурации и подключения новых устройств и ресурсов. С одной стороны эти функции облегчают работу квалифицированному пользователю, но с другой - могут служить источником НСД. Наиболее эффективным способом создания ИПС является использование дискреционного и мандатного механизма разграничения доступа СЗИ «Аккорд».

При использовании мандатного механизма в редакторе прав доступа ACED32.EXE автоматически включаются в список ПРД все задачи, которые в данный момент находятся в памяти. В дальнейшем этот список может корректироваться администратором на основе информации в журнале регистрации. Пользователь (или операционная система в сеансе этого пользователя) не сможет в процессе работы запустить процесс, который пытается получить доступ к ресурсу, но не включен в этот список, или его уровень доступа ниже метки доступа ресурса. Процессу можно назначить уровень доступа таким образом, чтобы обрабатывать данные(объекты) с определенной меткой доступа пользователь смог только процессами(задачами) с определенным уровнем доступа.

Доступ к пользовательским каталогам и файлам следует прописать в соответствии с полномочиями, установленными для данного пользователя (с использованием дискреционного или мандатного метода). Доступ к файлам и папкам операционной системы описываются так, чтобы обеспечить работоспособность системы, но исключить возможность несанкционированного изменения. После перезагрузки компьютера и входа в систему зарегистрированного пользователя запустится ОС Windows, в которой пользователь может работать только в разрешенных каталогах и только с установленным ПО. ПРД в этом случае могут выглядеть так:

Пользователь: MAIN_USER

- Права администратора: Нет
- Детальность журнала: Низкая

----------Объекты----------
A:\ [R VO G S] Общедоступно
C:\ [R VO G X0] Общедоступно
C:\ACCORD.X64\ [S] Общедоступно
C:\BOOT.INI [ ]
C:\DOCUMENTS AND SETTINGS\ [RWCDNV MEGn XS] Общедоступно
C:\PROGRAM FILES\ [R VO G XS] Общедоступно
C:\PROGRAM FILES\MICROSOFT OFFICE\ [R V G S] Общедоступно
C:\PROGRAM FILES\MICROSOFT OFFICE*.DLL [R V X]
C:\PROGRAM FILES\MICROSOFT OFFICE*.EXE [R V X]
C:\RECYCLED\ [RWCDNV MEGn S] Общедоступно
C:\WINNT\ [R VO G XS] Общедоступно
C:\WINNT\SYSTEM32\ACCESS.CPL [ ]
C:\WINNT\SYSTEM32\ACCORD.SCR [R V X]
C:\WINNT\SYSTEM32\ACGINA.DLL [R V X]
C:\WINNT\SYSTEM32\ACRUNVDD.DLL [R V X]
C:\WINNT\SYSTEM32\ACRUNVDD.EXE [R V X]
C:\WINNT\SYSTEM32\ALSNDMGR.CPL [ ]
C:\WINNT\SYSTEM32\APPWIZ.CPL [ ]
C:\WINNT\SYSTEM32\AUTOEXEC.NT [R]
C:\WINNT\SYSTEM32\AZIAHLP.DLL [R V X]
C:\WINNT\SYSTEM32\BDEADMIN.CPL [ ]
C:\WINNT\SYSTEM32\DESK.CPL [ ]
C:\WINNT\SYSTEM32\DRIVERS\ACRUN.SYS [ ]
C:\WINNT\SYSTEM32\FAX.CPL [ ]

C:\WINNT\SYSTEM32\HDWWIZ.CPL [ ]
C:\WINNT\SYSTEM32\IAMCPL.CPL [ ]
C:\WINNT\SYSTEM32\INETCPL.CPL [ ]
C:\WINNT\SYSTEM32\INTL.CPL [ ]
C:\WINNT\SYSTEM32\IRPROPS.CPL [ ]
C:\WINNT\SYSTEM32\JOY.CPL [ ]
C:\WINNT\SYSTEM32\MAIN.CPL [ ]
C:\WINNT\SYSTEM32\MMSYS.CPL [ ]
C:\WINNT\SYSTEM32\NCPA.CPL [ ]
C:\WINNT\SYSTEM32\NWC.CPL [ ]
C:\WINNT\SYSTEM32\ODBCCP32.CPL [ ]
C:\WINNT\SYSTEM32\POWERCFG.CPL [ ]
C:\WINNT\SYSTEM32\STICPL.CPL [ ]
C:\WINNT\SYSTEM32\SYSDM.CPL [ ]
C:\WINNT\SYSTEM32\TELEPHON.CPL [ ]
C:\WINNT\SYSTEM32\TIMEDATE.CPL [ ]
C:\WINNT\SYSTEM32\TMATTACH.DLL [R V X]
C:\WINNT\SYSTEM32\TMDRV32.DLL [R V X]
C:\WINNT\TEMP\ [RWCDNV MEGn S] Общедоступно
D:\ [R VO G 0] Общедоступно
D:\OPEN_DOC\ [RWCDNV MEGn S] Секретно
E:\ [R V G 0]
E:\RECYCLED\ [RWCDNV MEGn S]
E:\SYSTEM VOLUME INFORMATION\ [RW V G S]
----------Процессы----------
ACCORD.SCR [Общедоступно]
ACRUNNT.EXE [Общедоступно]
AUTOCHK.EXE [Общедоступно]
CSRSS.EXE [Общедоступно]
EXPLORER.EXE [Общедоступно]
INTERNAT.EXE [Общедоступно]
LSASS.EXE [Общедоступно]
MPNOTIFY.EXE [Общедоступно]
NDDEAGNT.EXE [Общедоступно]
OSA.EXE [Общедоступно]
PSTORES.EXE [Общедоступно]
REALPLAY.EXE [Общедоступно]
RPCSS.EXE [Общедоступно]
SERVICES.EXE [Общедоступно]
SETUP.EXE [Общедоступно]
SMSS.EXE [Общедоступно]
SPOOLSS.EXE [Общедоступно]
SYSTEM [Общедоступно]
SYSTRAY.EXE [Общедоступно]
TASKMGR.EXE [Общедоступно]
USERINIT.EXE [Общедоступно]
WINLOGON.EXE [Общедоступно]
WINWORD.EXE [Секретно]
_AVPCC.EXE [Общедоступно]

Пользователь сможет работать с документами в каталоге D:\OPEN_DOCтолько средствамиWinWord, и не может изменить конфигурацию системы.

Лабораторная работа 5
ПРИМЕРЫ ПОЛИТИК БЕЗОПАСНОСТИ VPN

1. Цель работы: изучить примеры существующих политик безопасности и научиться разрабатывать свои собственные политики.

2. Задачи работы:

- познакомиться с технологией VPN, как с инструментом обеспечения информационной безопасности;

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

1. Запустите виртуальную машину и присвойте первому виртуальному адаптеру Ethernet IP-адрес 192.168.200.2/24 и IP-адрес 10.11.1.210/24 для Ethernet2.

2. Добавьте в настроенной виртуальной машине новое входящее подключение VPN (Settings->Network and Dialup Connections->Make New Connection). С помощью мастера подключений последовательно установите следующие параметры: Accept Incoming Connections, Allow virtual private connections и укажите учетную запись, которая будет использована для этого подключения (при необходимости создайте новую учетную запись для удаленного подключения).

3. В свойствах созданного подключения (Incoming Connections -> Properties) установите «Allow others to make private connections to my computer by tunneling through the Internet or other network», сбросьте «Require all users to secure their passwords and data».

4. В настройках протокола TCP/IP установите «Allow callers to access my local network» и укажите пул IP адресов, выдаваемых клиентам (например, 11.1.1.211…10.11.1.215. Уточните у преподавателя, чтобы избежать конфликтов адресов в сети). Компоненты «File and Printer Sharing for Microsoft Networks» и «Client for Microsoft Networks» для входящих подключений должны быть установлены. Остальные параметры оставить по умолчанию.

5. Запустите виртуальную машину (пароль пользователя Administrator «labadmin») и присвойте первому виртуальному адаптеру Ethernet адрес 192.168.200.3/24. Убедитесь, что виртуальные хосты имеют различные сетевые имена и IP-адреса. Проверьте достижимость VPN - сервера (192.168.200.2).

Добавьте в ОС Клиента VPN подключение к виртуальной частной сети через Интернет:

6. Запустите мастер сетевых подключений (Settings->Network and Dial-up Connection -> Make new Connection) и создайте новое подключение «Connect to a private network through the Internet». При создании подключения укажите адрес хоста, к которому осуществляется подключение (IP-адрес назначения): 192.168.200.2.

7. В свойствах нового подключения укажите Type of VPN server I am calling:->PPTP. Компоненты «File and Printer Sharing for Microsoft Networks» и «Client for Microsoft Networks» для данного подключения должны быть установлены. Остальные параметры оставить по умолчанию.

8. Чтобы предотвратить возможность сетевого доступа к файлам и каталогам VPN-Сервера со стороны VPN-Клиента в обход туннеля, необходимо дополнительно установить следующие параметры для основного соединения Ethernet на Сервере (Settings-> Network and Dial-ip Connections -> Local Area Connection -> Properties):

Компоненты «File and Printer Sharing for Microsoft Networks» и «Client for Microsoft Networks» должны быть отключены. В свойствах протокола TCP/IP (Internet Protocol (TCP/IP) -> Properties -> Advanced -> WINS) отключите использование NetBIOS через TCP/IP (Disable NetBIOS over TCP/IP).

Аналогичные параметры должны быть установлены для подключения к локальной сети в ОС VPN-Клиента: Компоненты «File and Printer Sharing for Microsoft Networks» и «Client for Microsoft Networks» должны быть отключены. В свойствах протокола TCP/IP (Internet Protocol (TCP/IP) -> Properties -> Advanced -> WINS) отключите использование NetBIOS через TCP/IP (Disable NetBIOS over TCP/IP).

9. Запустите созданное виртуальное частное соединение. (Network and Dial-up Connections -> Virtual Private Connection) и укажите пароль той учетной записи, которая была указана при создании входящих подключений на сервере. Выясните адреса, выделенные серверу и клиенту. При установленном параметре «Allow callers to access my local network» (Разрешить звонящим доступ к локальной сети), пройдя авторизацию на PPTP сервере, клиентский хост получит адрес из диапазона внешней сети 10.11.1.* и станет узлом локальной сети, но только на сетевом уровне модели OSI и выше.

10. Проверьте достижимость сервера с адресом 192.168.0.1

11. На основном компьютере запустите анализатор трафика и настройте его на перехват пакетов.

12. Отправьте из ОС Клиента VPN несколько ECHO-запросов в адрес Сервера VPN двумя способами: сначала напрямую через сеть 192.168.200.0 (адрес сервера 192.168.200.2), а затем через туннельное соединение (адрес сервера необходимо выяснить при помощи диалогового окна состояния соединения). В чем отличие передаваемых пакетов? Обратите внимание, что пакеты, посылаемые через туннельное соединение, не опознаются как ICMP-пакеты.

13. Запустите на виртуальном хосте 192.168.200.3 Internet Explorer и подключитесь к запущенному в локальной сети web-серверу. При помощи анализатора трафика

посмотрите передаваемые пакеты. Есть ли возможность установить, пакеты какого содержания передавались? Зашифрованы ли поля заголовков? Какая информация может быть перехвачена злоумышленником в случае его подключения к линии связи?

14. Отключите виртуальное соединение (Virtual Private Connection -> Disconnect).

6. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Для чего используется VPN?
2. Какие есть типы VPN по технологиям?
3. Какие есть типы VPN по подключению?

Приложение 1

Краткие сведения из теории

Технология VPN шифрует все ваши действия в интернете. Все, что вы отправляете и получаете. Если вы входите только через VPN, виден не ваш подлинный источник подключения, а один из многочисленных VPN-маршрутизаторов.

Технологии VPN помогают приблизиться к настоящей анонимности, не прибегая к использованию сети TOR, в которой подключение петляет по широкой сети ретрансляторов, постоянно меняя положение действий в интернете, чтобы на них никто мог сфокусироваться. Сети VPN такой протокол не используют, но они обеспечивают достаточную — и очень важную — защиту во время вашего путешествия по нерегулируемым и полным злоумышленников дорогам.

Сетевой нейтралитет — это принцип, согласно которому поставщики услуг интернета должны работать со всеми данными одинаково, без дискриминации и учета личных предпочтений.

Типы VPN по используемым технологиям

IPSec VPN - обеспечивает безопасность пакетов на 3-м уровне OSI и может быть использована в Site-to-Site VPN и Remote-Acess VPN

SSL VPN - Secure Sockets Layer обеспечивает безопасность TCP Sessions на 6-м уровне OSI (Presentation)

MPLS - Multiprotocol Label Switching и MPLS Layer 3 VPNs выполняются провайдером и обеспечивает логическое соединение между офисами клиента. Такое соединение называется MPLs L3VPN.

Типы VPN по подключению

Remote-access VPN - это подключение от юзерской машины на сервер VPN. Remote-access VPN могут быть IpSec или SSL.

Site-to-Site VPNs - как понятно из названия, данный тип обеспечивает подключение двух и более офисов. Site-to-Site VPNs базируются на технологиях IPSec

Преимущества VPN

Confidentiality - только участвующие стороны должны понимать передающиеся данные. Любой другой, даже в случае перехвата данных, не имеет возможности их прочитать, поскольку данные зашифрованы.

Несмотря на то, что все алгоритмы шифрования известны, большинство из них базируются на ключе key, который знают лишь участники VPN. С помощью ключа производится шифрование и расшифрование данных.

Data Integrity - другой важный фактор - обеспечение целостности передаваемых данных их точки А в точку Б. Механизм Data Integrity проверяет цлостность данных и в случае несоответствия запросит повторную передачу.

Authentication - позволяет участникам VPN предварительно удостовериться что они будут общаться именно с тем с кем нужно.

Antireplay protection - Replay - метод атаки, при котором участнику отсылается копия перехваченного трафика. Функция Antireplay гарантирует, что если какой то зашифрованный пакет был выслан, то любая другая его копия будет недействительной.

Лабораторная работа 6

ПРОТОКОЛЫ ЗАЩИТЫ ДАННЫХ КАНАЛЬНОГО УРОВНЯ (PPTP, L2F И L2TP). СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ ЗАЩИТЫ НА КАНАЛЬНОМ УРОВНЕ.

1. **Цель работы**: изучить существующие протоколы защиты данных канального уровня.

2. **Задачи работы:**

- применить протоколы защиты данных на канальном уровне

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;

Уметь:

- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание**

Заполните таблицу сравнения протоколов PPTP, L2F и L2TP

	PPTP	L2F	L2TP
Совместимость			
Шифрование			
Поддерживаемые ОС			
Стабильность			
Безопасность			
Настройка			
…			

5. **Содержание отчета**
    1. название и цель работы;
    2. перечень осваиваемых компетенций;
    3. задание;
    4. исходные данные по заданию/варианту;
    5. ход выполнения работ;
    6. выводы по работе;
    7. ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
    1. К какой модели относится протокол PPTP?
    2. Что входит в набор PPP?
    3. Что такое «Деинкапсуляция»

Приложение 1

Краткие сведения из теории

Протоколы PPTP (Point-to-Point Tunneling Protocol), L2F (Layer-2 Forwarding) и L2TP (Layer-2 Tunneling Protocol) — это протоколы туннелирования канального уровня модели OSI. Общим свойством этих протоколов является то, что они используются для организации защищенного многопротокольного удаленного доступа к ресурсам корпоративной сети через открытую сеть, например через Интернет.

Все три протокола — PPTP, L2F и L2TP — обычно относят к протоколам формирования защищенного канала, однако этому определению точно соответствует только протокол PPTP, который обеспечивает туннелирование и шифрование передаваемых данных. Протоколы L2F и L2TP поддерживают только функции туннелирования. Для защиты туннелируемых данных в этих протоколах необходимо использовать некоторый дополнительный протокол, в частности IPSec.

Клиентское ПО обычно использует для удаленного доступа стандартный протокол канального уровня PPP (Point-to-Point Protocol). Протоколы PPTP, L2F иL2TP основываются на протоколе PPP и являются его расширениями. Первоначально протокол PPP, расположенный на канальном уровне, был разработан для инкапсуляции данных и их доставки по соединениям типа «точка—точка». Этот протокол служит также для организации асинхронных (например, коммутируемых) соединений. В частности, в настройках коммутируемого доступа удаленных систем Windows 2000 или Windows 9x обычно указывается подключение к серверу по протоколу PPP.

В набор PPP входят протокол управления соединением LCP (Link Control Protocol), ответственный за конфигурацию, установку, работу и завершение соединения «точка—точка», и протокол управления сетью NCP (Network Control Protocol), способный инкапсулировать в PPP протоколы сетевого уровня для транспортировки через соединение «точка—точка». Это позволяет одновременно передавать пакеты Novell IPX и Microsoft IP по одному соединению PPP.

Для доставки конфиденциальных данных из одной точки в другую через сети общего пользования сначала производится инкапсуляция данных с помощью протокола PPP, затем протоколы PPTP и L2TP выполняют шифрование данных и собственную инкапсуляцию. После того как туннельный протокол доставляет пакеты из начальной точки туннеля в конечную, выполняется деинкапсуляция.

Лабораторная работа 7

ЗАЩИТА ДАННЫХ НА СЕТЕВОМ УРОВНЕ (ПРОТОКОЛ IPSEC). ПРОТОКОЛЫ ТУННЕЛЬНОГО И ТРАНСПОРТНОГО РЕЖИМОВ.

1. Цель работы: изучить существующие протоколы сетевого уровня,

2. Задачи работы:

- применить протоколы защиты данных на сетевом уровне

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое IP Security?
2. Какие протоколы используют алгоритмо-зависимые спецификации?
3. Какие протоколы используются в IPsec?
4. Какие проблемы решает туннельный режим работы IPsec?
5. Какие проблемы решает транспортный режим работы IPsec?
6. Каковы преимущества и недостатки туннельного режима работы IPsec?
7. Каковы преимущества и недостатки транспортного режима работы IPsec?

Приложение 1

Краткие сведения из теории

IP Security — это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов; в его состав сейчас входят почти 20 предложений по стандартам и 18 RFC.

Спецификация IP Security (известная сегодня как IPsec) разрабатывается Рабочей группой IP Security Protocol IETF. Первоначально IPsec включал в себя 3 алгоритмо-независимые базовые спецификации, опубликованные в качестве RFC-документов "Архитектура безопасности IP", "Аутентифицирующий заголовок (AH)", "Инкапсуляция зашифрованных данных (ESP)" (RFC1825, 1826 и 1827). Необходимо заметить, что в ноябре 1998 года Рабочая группа IP Security Protocol предложила новые версии этих спецификаций, имеющие в настоящее время статус предварительных стандартов, это RFC2401 — RFC2412. Отметим, что RFC1825-27 на протяжении уже нескольких лет считаются устаревшими и реально не используются. Кроме этого, существуют несколько алгоритмо-зависимых спецификаций, использующих протоколы MD5, SHA, DES.

Гарантии целостности и конфиденциальности данных в спецификации IPsec обеспечиваются за счет использования механизмов аутентификации и шифрования соответственно. Последние, в свою очередь, основаны на предварительном согласовании сторонами информационного обмена т.н. "контекста безопасности" – применяемых криптографических алгоритмов, алгоритмов управления ключевой информацией и их параметров. Спецификация IPsec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей. При этом результатом согласования контекста безопасности является установление индекса параметров безопасности (SPI), представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности.

По сути, IPSec, который станет составной частью IPv6, работает на третьем уровне, т. е. на сетевом уровне. В результате передаваемые IP-пакеты будут защищены прозрачным для сетевых приложений и инфраструктуры образом. В отличие от SSL (Secure Socket Layer), который работает на четвертом (т. е. транспортном) уровне и теснее связан с более высокими уровнями модели OSI, IPSec призван обеспечить низкоуровневую защиту.

Транспортный режим

Транспортный режим используется для шифрования поля данных IP пакета, содержащего протоколы транспортного уровня (TCP, UDP, ICMP), которое, в свою очередь, содержит информацию прикладных служб. Примером применения транспортного режима является передача электронной почты. Все промежуточные узлы на маршруте пакета от отправителя к получателю используют только открытую информацию сетевого уровня и, возможно, некоторые опциональные заголовки пакета (в IPv6). Недостатком транспортного режима является отсутствие механизмов скрытия конкретных отправителя и получателя пакета, а также возможность проведения анализа трафика. Результатом такого анализа может стать информация об объемах и направлениях передачи информации, области интересов абонентов, расположение руководителей.

Туннельный режим предполагает шифрование всего пакета, включая заголовок сетевого уровня. Туннельный режим применяется в случае необходимости скрытия информационного обмена организации с внешним миром. При этом, адресные поля заголовка сетевого уровня пакета, использующего туннельный режим, заполняются межсетевым экраном организации и не содержат информации о конкретном отправителе пакета. При передаче информации из внешнего мира в локальную сеть организации в качестве адреса назначения используется сетевой адрес межсетевого экрана. После расшифровки межсетевым экраном начального заголовка сетевого уровня пакет направляется получателю.

Лабораторная работа 8
ЗАЩИТА НА СЕАНСОВОМ УРОВНЕ (ПРОТОКОЛЫ SSL, TLS, SOCKS)

1. Цель работы: изучить существующие протоколы на сеансовом уровне,

2. Задачи работы:

− применить протоколы защиты данных на сеансовом уровне

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..
- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Заполнить таблицу сравнения SSL/TLS и SOCKS

	SSL	SOCKS
Функциональность		
Скорость/производительность		
Безопасность/конфиденциальность		
Совместимость		
…		

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Какие протоколы используются на сеансовом уровне?
2. Как обеспечивается конфиденциальность в протоколах SSL/TLS
3. Какие основные отличия SSL от SOCKS?

Приложение 1

Краткие сведения из теории

Самым высоким уровнем модели OSI, на котором возможно формирование защищенных виртуальных каналов, является пятый — сеансовый уровень, При построении защищенных виртуальных сетей на сеансовом уровне появляется возможность криптографической защиты информационного обмена, включая аутентификацию, а также реализации ряда функций посредничества между взаимодействующими сторонами.

Однако на сеансовом уровне начинается непосредственная зависимость от приложений, реализующих высокоуровневые протоколы. Поэтому реализация протоколов защиты информационного обмена, соответствующих этому уровню, в большинстве случаев требует внесения изменений в высокоуровневые сетевые приложения.

Для защиты информационного обмена на сеансовом уровне широкое распространение получил протокол SSL (Secure Sockets Layer). Для выполнения на сеансовом уровне функций посредничества между взаимодействующими сторонами организацией IETF (Internet Engineering Task Force) в качестве стандарта принят протокол SOCKS.

Протоколы SSL/TLS

Протокол SSL применяется в качестве протокола защищенного канала, работающего на сеансовом уровне модели OSI. Этот протокол использует криптографические методы защиты информации для обеспечения безопасности информационного обмена. Протокол SSL выполняет все функции по созданию защищенного канала между двумя абонентами сети, включая их взаимную аутентификацию, обеспечение конфиденциальности, целостности и аутентичности передаваемых данных. Ядром протокола SSL является технология комплексного использования асимметричных и симметричных криптосистем.

Взаимная аутентификация обеих сторон в SSL выполняется путем обмена цифровыми сертификатами открытых ключей пользователей (клиента и сервера), заверенными цифровой подписью специальных сертификационных центров. Протокол SSL поддерживает сертификаты, соответствующие общепринятому стандарту X.509, а также стандарты инфраструктуры открытых ключей PKI (Public Key Infrastructure), с помощью которой организуется выдача и проверка подлинности сертификатов.

Конфиденциальность обеспечивается шифрованием передаваемых сообщений с использованием симметричных сессионных ключей, которыми стороны обмениваются при установлении соединения. Сессионные ключи передаются также в зашифрованном виде, при этом они шифруются с помощью открытых ключей, извлеченных из сертификатов абонентов. Использование для защиты сообщений симметричных ключей связано с тем, что скорость процессов шифрования и расшифрования на основе симметричного ключа существенно выше, чем при использовании несимметричных ключей. Подлинность и целостность циркулирующей информации обеспечивается за счет формирования и проверки электронной цифровой подписи.

В качестве алгоритмов асимметричного шифрования используются алгоритм RSA, а также алгоритм Диффи — Хеллмана. Допустимыми алгоритмами симметричного шифрования являются RC2, RC4, DES, 3DES и AES. Для вычисления хэш-функций могут применяться стандарты MD5 и SHA-1. В протоколе SSL версии 3.0 набор криптографических алгоритмов является расширяемым.

Согласно протоколу SSL криптозащищенные туннели создаются между конечными точками виртуальной сети. Инициаторами каждого защищенного туннеля являются клиент и сервер, функционирующие на компьютерах в конечных точках туннеля.

Протокол SSL предусматривает следующие этапы взаимодействия клиента и сервера при формировании и поддержке защищаемого соединения:

- установление SSL-сессии;
- защищенное взаимодействие.

В процессе установления SSL-сессии решаются следующие задачи:

• аутентификация сторон;

• согласование криптографических алгоритмов и алгоритмов сжатия, которые будут использоваться при защищенном информационном обмене;

• формирование общего секретного мастер-ключа;

• генерация на основе сформированного мастер-ключа общих секретных сеансовых ключей для криптозащиты информационного обмена.

Протокол SOCKS

Протокол SOCKS организует процедуру взаимодействия клиент-серверных приложений на сеансовом уровне модели OSI через сервер-посредник, илиproxy-сервер.

В общем случае программы-посредники, которые традиционно используются в МЭ, могут выполнять следующие функции:

• идентификацию и аутентификацию пользователей;

• криптозащиту передаваемых данных;

• разграничение доступа к ресурсам внутренней сети;

• разграничение доступа к ресурсам внешней сети;

• фильтрацию и преобразование потока сообщений, например поиск вирусов и прозрачное шифрование информации;

• трансляцию внутренних сетевых адресов для исходящих потоков сообщений.

Первоначально протокол SOCKS разрабатывался только для перенаправления запросов к серверам со стороны клиентских приложений, а также возврата этим приложениям полученных ответов. Перенаправление запросов и ответов между клиент-серверными приложениями уже позволяет реализовать функцию трансляции сетевых IP-адресов NAT (Network Address Translation). Замена у исходящих пакетов внутренних IP-адресов отправителей одним IP-адресом шлюза позволяет скрыть топологию внутренней сети от внешних пользователей и тем самым усложнить задачу НСД.

На основе протокола SOCKS могут быть реализованы и другие функции посредничества по защите сетевого взаимодействия. Например, протокол SOCKSможет применяться для контроля над направлениями информационных потоков и разграничения доступа в зависимости от атрибутов пользователей и информации. Эффективность использования протокола SOCKS для выполнения функций посредничества обеспечивается его ориентацией на сеансовый уровень модели OSI. По сравнению с посредниками прикладного уровня на сеансовом уровне достигается более высокое быстродействие и независимость от высокоуровневых протоколов (HTTP, FTP, POP3, SMTP и др.). Кроме того, протокол SOCKS не привязан к протоколу IP и не зависит от ОС. Например, для обмена информацией между клиентскими приложениями и посредником может использоваться протокол IPX.

Протокол SOCKS v5 одобрен организацией IETF (Internet Engineering Task Force) в качестве стандарта Internet и включен в RFC 1928.

Общая схема установления соединения по протоколу SOCKS v5 может быть описана следующим образом:

• запрос прикладного клиента, желающего установить соединение с каким-либо прикладным сервером в сети, перехватывает установленный на этом же компьютере SOCKS-клиент;

• соединившись с SOCKS-сервером, SOCKS-клиент сообщает ему идентификаторы всех методов аутентификации, которые он поддерживает;

• SOCKS-сервер решает, каким методом аутентификации воспользоваться (если SOCKS-сервер не поддерживает ни один из методов аутентификации, предложенных SOCKS-клиентом, соединение разрывается);

• при поддержке каких-либо предложенных методов аутентификации SOCKS-сервер в соответствии с выбранным методом аутентифицирует пользователя, от имени которого выступает SOCKS-клиент; в случае безуспешной аутентификации SOCKS-сервер разрывает соединение;

• после успешной аутентификации SOCKS-клиент передает SOCKS-серверу DNS-имя или IP-адрес запрашиваемого прикладного сервера в сети и далееSOCKS-сервер на основе имеющихся правил разграничения доступа принимает решение об установлении соединения с этим прикладным сервером;

• в случае установления соединения прикладной клиент и прикладной сервер взаимодействуют друг с другом по цепочке соединений, в которой SOCKS-сервер ретранслирует данные, а также может выполнять функции посредничества по защите сетевого взаимодействия; например, если в ходе аутентификации SOCKS-клиент и SOCKS-сервер обменялись сеансовым ключом, то весь трафик между ними может шифроваться.

Лабораторная работа 9
ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ (ИОК). МОДЕЛИ APKI И PKIX

1. Цель работы: изучить инфраструктуру ключей, её объекты, а также изучить её применение и различные модели.

2. Задачи работы:

- рассмотреть инфраструктуру открытых ключей PKI

Студент должен:

Иметь практический опыт:

- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;

Уметь:

- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;

ПК:

- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.

3. Подготовка к работе

Практическое задание может быть выполнено в среде с открытым исходным кодом, такой как OpenSSL или LibreSSL. Для выполнения задания необходимо иметь понимание работы сетевых протоколов, уметь работать с командной строкой и иметь базовые знания программирования.

Подготовить бланк отчета.

4. Задание и порядок работы

- создание сертификатов на основе моделей APKI и PKIX с помощью OpenSSL и настройка их использования в простом приложении, например, веб-сервере.
- тестирование защиты информации с помощью созданных сертификатов, например, попытавшись получить доступ к защищенному ресурсу без использования сертификата.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Какие критерии безопасности информационных технологий существуют?
2. Какие технологии были созданы благодаря открытым и закрытым ключам?
3. Что такое Сертификат?

Приложение 1

Краткие сведения из теории

Комплексная безопасность информационной системы определяется возможностью противодействовать широкому спектру угроз, как внутренних, так и внешних. Для противодействия и сведения к минимуму ущерба от различного рода вредоносных воздействий необходимо реализовать соответствующие подсистемы защиты. В общем случае конкретная подсистема защиты представляет собой комплекс мероприятий, направленный на снижение риска и ущерба от определенного рода угроз, обеспеченный необходимой ресурсной базой: нормативно-правовые документы, программно-аппаратные средства, квалифицированный персонал.

Для оценки безопасности информационных систем и технологий возможно использование различных методик. В частности, в интерпретации ГОСТ Р ИСО/МЭК 15408-2002 (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.) выделяют следующие критерии безопасности информационных технологий:

- Идентификация пользователей (возможность однозначно идентифицировать субъекта);

-Аутентификация пользователей (проверка принадлежности субъекту предъявленного им идентификатора, подтверждение подлинности);

-Авторизация доступа к ресурсам (информация должна быть доступна только для того, для кого она предназначена);

-Целостность информации (информация должна быть защищена от несанкционированной модификации, как при хранении, так и при передаче);

-Невозможность отказа от совершенных действий (субъект не может отказаться от совершенного действия);

-Конфиденциальность информации (информация должна быть защищена от несанкционированного прочтения, как при хранении, так и при передаче).

Критерии безопасности подразумевают реализацию соответствующих подсистем информационной безопасности. Большинство из задач, описываемых данными критериями, можно решать с использованием Инфраструктуры Открытых Ключей (ИОК).

Инфраструктура Открытых Ключей – это комплекс организационно-технических мероприятий и программно-аппаратных средств, необходимых для использования технологии с открытым распределением ключей (асимметричной криптографии). Инфраструктура открытых ключей позволяет решать широкий спектр задач по защите информации в корпоративных информационно-телекоммуникационных системах: электронный документооборот, сдача отчетности, медицина и телемедицина, платежные и трейдинговые системы и пр.

Одной из самых распространенных информационных технологий реализованных на базе ИОК является **Электронная Цифровая Подпись** (ЭЦП).

Инфраструктура открытых ключей (ИОК) базируется на асимметричной криптографии (криптография с открытыми ключами). Асимметричная криптография как раздел науки криптографии появилась в конце 70-х годов 20-го века. В настоящее время в системах защиты информации широко используются, как симметричная, так и асимметричная криптографии.

Криптография является разделом математики и занимается поиском и исследованием методов преобразования информации с целью сокрытия ее содержания.

Криптографические алгоритмы

Процесс криптографического преобразования (шифрования) информации выглядит следующим образом. ***Открытый текст*** (информацию, которую требуется зашифровать) шифруют с помощью определенного ***криптографического алгоритма*** и ***ключа шифрования***. Зашифрованный по надежному криптографическому

алгоритму текст практически невозможно расшифровать без дополнительных данных, которые называются ***ключом расшифрования***.

Характеристика шифра (криптографического алгоритма), определяющая его стойкость к расшифрованию без знания ключа расшифрования называется ***криптостойкостью***.

Криптография с симметричным, или секретным, ключом использует одинаковые ключи для шифрования и расшифровывания сообщений (см. рис.13.1). Ключ этот знают только отправитель и адресат, он не должен быть известен третьему лицу. Поэтому главная проблема симметричной криптографии состоит в предварительной **передаче секретного ключа одним абонентом другому по надежному каналу**. Кроме того, ее применение требует хранения множества ключей для разных абонентов и разных типов сообщений.

Существует огромное разнообразие конкретных реализаций алгоритмов шифрования симметричными ключами. Наибольшее распространение получил алгоритм DES (Data Encryption Standard), принятый национальным бюро стандартов США в 1977 году. В 1991 году аналогичный алгоритм был принят в качестве отечественного стандарта (ГОСТ 28147-89). Определенное распространение получили также алгоритмы RC4, RC5, IDEA и пр.

В алгоритмах этого типа для шифрования и расшифровки информации используются пара ключей: ***открытый и закрытый***, каждый из которых не может быть получен из другого (см. рис.13.2). Открытый ключ рассылается всем абонентам, закрытый держится в тайне. Для того чтобы отправить сообщение абоненту, нужно при шифровании использовать его открытый ключ, получатель же расшифровывает сообщение при помощи своего закрытого секретного ключа. Никто, кроме получателя, не может расшифровать сообщение, так как никто больше не имеет доступа к этому закрытому ключу. Даже тот, кто зашифровал сообщение с помощью открытого ключа, не сможет его расшифровать. Такой протокол обеспечивает приватность без необходимости обладания надежным каналом, которого требует обычная криптография с секретным ключом.

При использовании алгоритма с открытым ключом отпадает потребность в секретном канале связи для передачи ключа, т.к. открытый ключ не является секретной информацией. Различие ключей – открытого и закрытого – в криптографии с открытыми ключами позволило создать следующие технологии:

-**электронные цифровые подписи** *(задачи обеспечения целостности, авторства, актуальности информации, аутентификации субъекта и информации, неотказуемости)*;

-**распределенная проверка подлинности**

(задачи идентификации, аутентификации субъекта, авторизация доступа субъекта к

информации);

-согласование общего секретного ключа сессии

(задачи обеспечения конфиденциальности информации при передаче по открытым каналам связи);

- **шифрование больших объемов данных без предварительного обмена общим секретным ключом** *(задачи обеспечения конфиденциальности информации)*.

В настоящее время хорошо известен целый ряд алгоритмов шифрования с открытым ключом. Некоторые алгоритмы, например RSA (Rivest-Shamir-Adleman) и ECC (Elliptic Curve Cryptography), универсальны, они поддерживают все перечисленные выше операции. Другие алгоритмы более специализированы и поддерживают не все возможности.

К числу алгоритмов шифрования с открытым ключом относятся:

- российский алгоритмы электронной цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001;

-алгоритм электронной цифровой подписи DSA (Digital Signature Algorithm, входящий в принятый в США государственный стандарт цифровой подписи Digital Signature Standard, FIPS 186);

-алгоритм DH (Diffie-Hellman), применяемый для выработки общего секретного ключа сессии.

Сертификаты открытых ключей

В алгоритмах криптографии с открытыми ключами важным аспектом является определение принадлежности конкретного открытого ключа конкретному пользователю. В общем случае открытые ключи пользователей системы хранятся в общедоступном справочнике открытых ключей, и существует вероятность перехвата или подмены злоумышленниками открытого ключа какого-либо пользователя. Поэтому нужен механизм, который может обеспечить уверенность в том, что имеющийся открытый ключ принадлежит нужному пользователю, а не кому-либо другому. Один из таких механизмов основан на сертификатах открытых ключей, выдаваемых Удостоверяющими Центрами.

Сертификаты открытого ключа обеспечивают механизм надежной связи между открытым

ключом и субъектом, которому принадлежит соответствующий закрытый ключ (см. рис.13.3).

Сертификат – это цифровой документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью удостоверяющего центра выдавшего сертификат.

Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель (удостоверяющий центр) удостоверяет подлинность связи между открытым ключом субъекта и информацией, его идентифицирующей

В настоящее время наиболее часто используются сертификаты на основе стандарта Международного союза телекоммуникаций ITU-T X.509 v3 и рекомендаций IETF (Internet Engineering Task Force) RFC 2459.

Удостоверяющий Центр

Удостоверяющий Центр - это служба, которая выдает сертификаты. Удостоверяющий Центр является гарантом связи между открытым ключом субъекта и содержащейся в сертификате информацией по идентификации этого субъекта. Различные УЦ устанавливают и гарантируют эту связь различными способами, поэтому прежде чем доверять сертификатам того или иного УЦ, следует ознакомиться с его политикой и регламентом.

Удостоверяющие центры являются одной из основных составляющих ИОК. При построении ИОК в информационной системе с существенно распределенной структурой (например, организация с большим количеством подразделений или информационная система, объединяющая несколько организаций) встает задача построения и объединения в единую сеть нескольких Удостоверяющих центров.

Наибольшее распространение получила иерархическую модель построения Удостоверяющих центров. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом коммерческих продуктов и УЦ различных поставщиков. Простейшая форма иерархии УЦ состоит из одного УЦ, а в общем случае – из множества УЦ с явно определенными отношениями родительский – дочерний (см. рис.13.5).

В иерархической модели дочерние Удостоверяющие Центры сертифицируются родительским. Удостоверяющий центр, находящийся на самом верхнем уровне иерархии,

обычно называется корневым. Подчиненные УЦ являются промежуточными или выдающими УЦ. Выдающим УЦ называется тот удостоверяющий центр, который выдает сертификаты конечным пользователям. Промежуточным УЦ называется тот УЦ, который

не является корневым и выдает сертификаты только другим УЦ, а не конечным пользователям.

Фундаментальное преимущество этой модели состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых УЦ. В то же время эта модель позволяет иметь различное число УЦ, выдающих сертификаты.

Список отозванных сертификатов

Удостоверяющие центры периодически выпускают списки отозванных сертификатов, в которых фиксируются сертификаты пользователей, вышедшие из обращения в системе.

Список отозванных сертификатов (CRL – Certificate Revocation List) – это цифровой документ, который содержит перечень сертификатов, являющихся отозванными из обращения в УЦ. Удостоверяющий центр поддерживает отзыв сертификатов и публикацию списков отозванных сертификатов. Абоненты могут получить эту информацию и записать ее в свое локальное хранилище, чтобы использовать для последующей проверки сертификатов.

Лабораторная работа 10

СЕРТИФИКАТ ОТКРЫТОГО КЛЮЧА. ФОРМАТ СЕРТИФИКАЦИИ ОТКРЫТОГО КЛЮЧА. АННУЛИРОВАНИЕ СЕРТИФИКАТОВ

1. **Цель работы**: изучить принцип работы цифровых сертификатов, ознакомиться с сертификатами установленных приложений.
2. **Задачи работы:**
   - получить навык применения программного продукта OpenSSL для создания сертификатов X.509 и их преобразования, изучить структуру сертификата X.509 и форматы DER и PEM.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- возможные угрозы безопасности информации в ИТКС;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание и порядок работы**
   - Зарегистрируйте свой собственный сертификат открытого ключа в любой публичной инфраструктуре открытых ключей (например, Let's Encrypt).
   - Ознакомьтесь с форматом сертификации открытого ключа X.509.
   - Проверьте, можно ли аннулировать свой сертификат открытого ключа и как это сделать.

5. **Содержание отчета**
   1. название и цель работы;
   2. перечень осваиваемых компетенций;
   3. задание;
   4. исходные данные по заданию/варианту;
   5. ход выполнения работ;
   6. выводы по работе;
   7. ответы на контрольные вопросы.
6. **Контрольные вопросы к защите**
   1. Что такое криптография?
   2. Какие есть алгоритмы шифрования с открытым ключом?
   3. Что такое «Инфраструктура открытых ключей»?

Приложение 1

Краткие сведения из теории

Критерии безопасности подразумевают реализацию соответствующих подсистем информационной безопасности. Большинство из задач, описываемых данными критериями, можно решать с использованием Инфраструктуры Открытых Ключей (ИОК).

Инфраструктура Открытых Ключей – это комплекс организационно-технических мероприятий и программно-аппаратных средств, необходимых для использования технологии с открытым распределением ключей (асимметричной криптографии). Инфраструктура открытых ключей позволяет решать широкий спектр задач по защите информации в корпоративных информационно-телекоммуникационных системах: электронный документооборот, сдача отчетности, медицина и телемедицина, платежные и трейдинговые системы и пр.

Одной из самых распространенных информационных технологий реализованных на базе ИОК является **Электронная Цифровая Подпись** (ЭЦП).

Инфраструктура открытых ключей (ИОК) базируется на асимметричной криптографии (криптография с открытыми ключами). Асимметричная криптография как раздел науки криптографии появилась в конце 70-х годов 20-го века. В настоящее время в системах защиты информации широко используются, как симметричная, так и асимметричная криптографии.

Криптография является разделом математики и занимается поиском и исследованием методов преобразования информации с целью сокрытия ее содержания.

Криптографические алгоритмы

Процесс криптографического преобразования (шифрования) информации выглядит следующим образом. ***Открытый текст*** (информацию, которую требуется зашифровать) шифруют с помощью определенного ***криптографического алгоритма*** и ***ключа шифрования***. Зашифрованный по надежному криптографическому алгоритму текст практически невозможно расшифровать без дополнительных данных, которые называются ***ключом расшифрования***.

Характеристика шифра (криптографического алгоритма), определяющая его стойкость к расшифрованию без знания ключа расшифрования называется ***криптостойкостью***.

Криптография с симметричным, или секретным, ключом использует одинаковые ключи для шифрования и расшифровывания сообщений (см. рис.13.1). Ключ этот знают только отправитель и адресат, он не должен быть известен третьему лицу. Поэтому главная проблема симметричной криптографии состоит в предварительной **передаче секретного ключа одним абонентом другому по надежному каналу**. Кроме того, ее применение требует хранения множества ключей для разных абонентов и разных типов сообщений.

Существует огромное разнообразие конкретных реализаций алгоритмов шифрования симметричными ключами. Наибольшее распространение получил алгоритм DES (Data Encryption Standard), принятый национальным бюро стандартов США в 1977 году. В 1991 году аналогичный алгоритм был принят в качестве отечественного стандарта (ГОСТ 28147-89). Определенное распространение получили также алгоритмы RC4, RC5, IDEA и пр.

В алгоритмах этого типа для шифрования и расшифровки информации используются пара ключей: ***открытый и закрытый***, каждый из которых не может быть получен из другого (см. рис.13.2). Открытый ключ рассылается всем абонентам, закрытый держится в тайне. Для того чтобы отправить сообщение абоненту, нужно при шифровании использовать его открытый ключ, получатель же расшифровывает сообщение при помощи своего закрытого секретного ключа. Никто, кроме получателя, не может расшифровать сообщение, так как никто больше не имеет доступа к этому закрытому ключу. Даже тот, кто

зашифровал сообщение с помощью открытого ключа, не сможет его расшифровать. Такой протокол обеспечивает приватность без необходимости обладания надежным каналом, которого требует обычная криптография с секретным ключом.

При использовании алгоритма с открытым ключом отпадает потребность в секретном канале связи для передачи ключа, т.к. открытый ключ не является секретной информацией. Различие ключей – открытого и закрытого – в криптографии с открытыми ключами позволило создать следующие технологии:

-**электронные цифровые подписи** *(задачи обеспечения целостности, авторства, актуальности информации, аутентификации субъекта и информации, неотказуемости)*;

-**распределенная проверка подлинности**

(задачи идентификации, аутентификации субъекта, авторизация доступа субъекта к

информации);

-**согласование общего секретного ключа сессии**

(задачи обеспечения конфиденциальности информации при передаче по открытым каналам связи);

- **шифрование больших объемов данных без предварительного обмена общим секретным ключом** *(задачи обеспечения конфиденциальности информации)*.

В настоящее время хорошо известен целый ряд алгоритмов шифрования с открытым ключом. Некоторые алгоритмы, например RSA (Rivest-Shamir-Adleman) и ECC (Elliptic Curve Cryptography), универсальны, они поддерживают все перечисленные выше операции. Другие алгоритмы более специализированы и поддерживают не все возможности.

К числу алгоритмов шифрования с открытым ключом относятся:

- российский алгоритмы электронной цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001;

-алгоритм электронной цифровой подписи DSA (Digital Signature Algorithm, входящий в принятый в США государственный стандарт цифровой подписи Digital Signature Standard, FIPS 186);

-алгоритм DH (Diffie-Hellman), применяемый для выработки общего секретного ключа сессии.

Сертификаты открытых ключей

В алгоритмах криптографии с открытыми ключами важным аспектом является определение принадлежности конкретного открытого ключа конкретному пользователю. В общем случае открытые ключи пользователей системы хранятся в общедоступном справочнике открытых ключей, и существует вероятность перехвата или подмены злоумышленниками открытого ключа какого-либо пользователя. Поэтому нужен механизм, который может обеспечить уверенность в том, что имеющийся открытый ключ принадлежит нужному пользователю, а не кому-либо другому. Один из таких механизмов основан на сертификатах открытых ключей, выдаваемых Удостоверяющими Центрами.

Сертификаты открытого ключа обеспечивают механизм надежной связи между открытым

ключом и субъектом, которому принадлежит соответствующий закрытый ключ (см. рис.13.3).

Сертификат – это цифровой документ, который содержит открытый ключ субъекта и подписан электронной цифровой подписью удостоверяющего центра выдавшего сертификат.

Сертификат также содержит сведения о владельце открытого ключа, например, информацию, которая его дополнительно идентифицирует. Таким образом, выдавая сертификат, издатель (удостоверяющий центр) удостоверяет подлинность связи между открытым ключом субъекта и информацией, его идентифицирующей

Лабораторная работа 11
РЕАЛИЗАЦИЯ АЛГОРИТМОВ СКОРОСТНОЙ КРИПТОЗАЩИТЫ

1. Цель работы: получить знания и навыки монтажа оптических муфт

2. Задачи работы:

- реализовать алгоритмы скоростной криптозащиты

Студент должен:

Иметь практический опыт:

- поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

создание программы на языке программирования, которая использует алгоритм шифрования AES (Advanced Encryption Standard) для защиты передаваемых данных.

5. Порядок выполнения работы

- Изучить теоретические основы алгоритма шифрования AES.
- Определить язык программирования, на котором будет написана программа.
- Написать код программы, используя выбранный язык программирования.
- Протестировать программу на корректность работы.

6. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

7. Контрольные вопросы к защите

1. Перечислите условия современных алгоритмов шифрования.
2. Перечислите типы реализации криптографических алгоритмов.

3. Какие алгоритмы криптозащиты относятся к скоростной криптозащите?

Приложение 1

Краткие сведения из теории

На практике криптографические алгоритмы в зависимости от области применения имеют несколько типов реализации: программную, аппаратную и программно-аппаратную. Перед тем как перейти непосредственно к рассмотрению достоинств и недостатков перечисленных типов реализации, сформулируем общие требования к реализации криптографических алгоритмов. Современные алгоритмы шифрования должны удовлетворять следующим условиям:

• должны быть адаптированы к новейшей программно-аппаратной базе (например, алгоритмы блочного шифрования в программной реализации должны быть адаптированы к операциям с 64-разрядными числами);

• объем ключа должен соответствовать современным методам и средствам дешифрования зашифрованных сообщений (о минимальной длине ключа будет сказано позже);

• операции зашифрования и расшифрования должны но возможности быть простыми, чтобы удовлетворять современным требованиям но скоростным характеристикам;

• не должны допускать появления постоянно увеличивающегося числа ошибок;

• должны сводить к минимуму объем сообщения в ходе выполнения операций шифрования.

Аппаратная реализация

До недавних пор алгоритмы шифрования реализовывались в виде отдельных устройств, что обусловливалось использованием криптографии для засекречивания различных видов передачи информации (телеграф, телефон, радиосвязь). С развитием средств вычислительной техники и общедоступных сетей передачи данных появились новые возможности применения криптографических алгоритмов. Однако аппаратная реализация до сих пор широко используется не только в военной сфере, но и в коммерческих организациях. Подобная «живучесть» аппаратных средств криптографической защиты информации объясняется рядом факторов.

Во-первых, аппаратная реализация обладает лучшими скоростными характеристиками, нежели программно реализуемые алгоритмы шифрования. Использование специальных чипов, адаптированных к реализации на них процедур зашифрования и расшифрования, приводит к тому, что, в отличие от процессоров общего назначения, они позволяют оптимизировать многие математические операции, применяемые в алгоритмах шифрования.

Во-вторых, аппаратные средства защиты информации обладают несравнимо большей защищенностью как от побочных электромагнитных излучений, возникающих в ходе работы аппаратуры, так и от непосредственного физического воздействия на устройства, где осуществляются операции шифрования и хранение ключевой информации. Что касается побочных электромагнитных излучений, то они вполне могут служить каналом утечки критической информации, связанной с работой алгоритма шифрования и используемых ключей. Физические же воздействия являются удобным средством получения промежуточных сведений о работе алгоритма шифрования, а то и непосредственно ключевой информации, что, в свою очередь, позволит противнику более эффективно и с минимальными затратами провести атаку на используемые алгоритмы шифрования. Современные микросхемы, на которых реализуются алгоритмы шифрования и осуществляется хранение ключевой информации, способны успешно противостоять любым попыткам физического воздействия - в случае обнаружения несанкционированного доступа к микросхеме она саморазрушается. Реализовать защиту от побочного излучения и утечки по цепям электропитания на обычных персональных компьютерах можно, но

решить эту задачу будет гораздо сложнее, нежели использовать устройство, которое соответствует стандартам по защите от побочных электромагнитных излучений.

В-третьих, аппаратные средства более удобны в эксплуатации, так как позволяют осуществлять операции зашифрования и расшифрования для пользователя в прозрачном режиме; кроме того, их легко инсталлировать.

В-четвертых, учитывая многообразие вариантов применения средств криптографической защиты информации, аппаратные средства повсеместно используются для защиты телефонных переговоров, отправки факсимильных сообщений и других видов передачи информации, где невозможно использовать программные средства.

Программная реализация

К достоинствам программной реализации можно отнести ее гибкость и переносимость. Другими словами, программа, написанная под одну операционную систему, может быть модифицирована под любой тип ОС. Кроме того, обновить программное обеспечение можно с меньшими временными и финансовыми затратами. К тому же многие современные достижения в области криптографических протоколов недоступны для реализации в виде аппаратных средств.

К недостаткам программных средств криптографической защиты следует отнести возможность вмешательства в действие алгоритмов шифрования и получения доступа к ключевой информации, хранящейся в общедоступной памяти. Эти операции обычно выполняются при помощи простого набора программных инструментариев (отладчики программ и т.д.). Так, например, во многих операционных системах осуществляется аварийный дамп памяти на жесткий диск, при этом в памяти могут находиться ключи, найти которые не составит труда.

Таким образом, слабая физическая защищенность программных средств является одним из основных недостатков подобных методов реализации алгоритмов шифрования.

К этому можно добавить, что программная реализация средств криптографической защиты не в состоянии обеспечить выполнение некоторых характеристик, требуемых для надежного использования алгоритмов шифрования. Например, генерация ключевой информации не должна производиться программными датчиками случайных чисел; для этой цели необходимо использовать специальные аппаратные устройства.

Программно-аппаратная реализация

Программно-аппаратная реализация позволяет пользователям устранить некоторые недостатки программных средств защиты информации и при этом сохранить их достоинства (за исключением ценового критерия).

Основными функциями, возлагаемыми на аппаратную часть программно-аппаратного комплекса криптографической защиты информации, обычно являются генерация ключевой информации и хранение ключевой информации в устройствах, защищенных от несанкционированного доступа со стороны злоумышленника. Кроме того, посредством методик такого типа можно осуществлять аутентификацию пользователей с помощью паролей (статических или динамически изменяемых, которые могут храниться на различных носителях ключевой информации - смарт-карты, touch-memory и т.д.) либо на основе уникальных для каждого пользователя биометрических характеристик. Устройства считывания подобных сведений могут входить в состав программно-аппаратной реализации средств защиты информации.

Лабораторная работа 12
VPN НА БАЗЕ СЕТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМ

1. Цель работы: научиться создавать инфраструктуру защищенных виртуальных каналов на базе сетевых операционных систем.

2. Задачи работы:

- создание инфраструктуры VPN на базе сетевых операционных систем

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Выбрать одну из тем подготовить доклад:

1. Check Point Firewall-1/VPN-1
2. Криптографический комплекс «Шифратор IP-пакетов»
3. Системы блокировки корпоративных каналов связи
4. Системы защиты от утечек внутренней информации
5. Интегральная информационная безопасность

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Какие есть уязвимости PPTP?
2. Что из себя представляет Интегральная информационная безопасность?
3. Какие есть системы защиты от утечек внутренней информации?

Приложение 1

Краткие сведения из теории

Построение VPN на базе сетевой ОС является достаточно удобным и, главное, дешевым средством создания инфраструктуры защищенных виртуальных каналов. Сегодня в России наибольшее распространение среди сетевых операционных систем (ОС), позволяющих стоить VPN штатными средствами самой ОС, получила Windows NT. Данное решение оказалось популярным прежде всего благодаря общей распространенности данной ОС.

Для построения виртуальных защищенных туннелей в IP-сетях Windows NT использует разработанный фирмой Microsoft протокол PPTP (Point-to-Point Tunneling Protocol), который является расширением хорошо известного протокола PPP (Point-to-Point Protocol). Туннелирование трафика происходит за счет инкапсуляции и последующего шифрования (криптоалгоритм RSA RC4 с ключом 40 бит) стандартных PPP-фреймов в IP-датаграммы, которые и передаются по открытым IP сетям. С точки зрения обеспечения безопасности соединения, PPTP протокол унаследовал практически все качества PPP протокола.

По мнению специалистов данное решение является оптимальным для построения VPN внутри локальных сетей (localnet-VPN) или домена Windows NT, а также для построения intranet- и externet-VPN для небольших компаний с целью защиты некритичной для их бизнеса информации. В то же время крупный бизнес вряд ли доверит свои секреты этому решению, поскольку многочисленные испытания VPN, построенных на базе Windows NT показали, что протокол PPTP имеет достаточно большое количество уязвимостей с точки зрения безопасности:

- уязвимость, связанная с реализацией и применением функции хеширования паролей и протокола аутентификации CHAP;
- уязвимость протокола шифрования в одноранговых сетях (MPPE);
- открытость для атаки на этапе конфигурации соединения и атак типа «отказ в обслуживании»;
- недостаточная проработанность вопросов обеспечения безопасности в данной ОС и др.

Немаловажным также является тот факт, что из-за широкой распространенности Windows NT поиском дополнительных уязвимостей этой ОС постоянно заняты тысячи компьютерных специалистов, которые хотя и делают это с различными целями, но информацию о результатах их работы почти всегда можно найти на многочисленных хакерских сайтах в Интернете.

Понимая недостаточную защищенность PPTP протокола, в своей новой ОС - Windows 2000 - компания Microsoft сделала ставку на реализацию более современного протокола IPSec (см. далее). Однако, первые независимые тесты выявили серьезные проблемы с безопасностью и этой ОС.

Лабораторная работа 13
VPN НА БАЗЕ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Цель работы: научиться создавать инфраструктуру защищенных виртуальных каналов на базе специализированного программного обеспечения.

2. Задачи работы:

− создать инфраструктуру защищенных виртуальных каналов на базе специализированного ПО

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Подготовить презентацию и рассказать об одном из VPN:

1. AltaVista Tunnel
2. RRAS
3. F-Secure Virtual Private Network

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

6. Контрольные вопросы

1. Какие типы VPN существуют?
2. Какие компоненты входят в VPN?
3. Какие программные продукты используются для создания VPN?
4. Какие алгоритмы шифрования используются в VPN?
5. Какие методы аутентификации используются в VPN?
6. Какие меры безопасности необходимо принимать при использовании VPN?

7. Как настроить VPN на базе специализированного программного обеспечения?

Приложение 1

Краткие сведения из теории

Для построения VPN широко используются специализированные программные средства. Программные средства построения VPN позволяют формировать защищенные туннели чисто программным образом и превращают компьютер, на котором они функционируют, в маршрутизатор TCP/IP, который получает зашифрованные пакеты, расшифровывает их и передает по локальной сети дальше, к конечной точке назначения. В последнее время появилось достаточно много таких продуктов. В виде специализированного программного обеспечения могут быть выполнены VPN-шлюзы, VPN-серверы и VPN-клиенты.

VPN-продукты, реализованные программным способом, с точки зрения производительности уступают специализированным аппаратным устройствам, в то же время программные продукты легко обеспечивают производительность, достаточную для удаленного доступа. Несомненным достоинством программных продуктов является гибкость и удобство в применении, а также относительно невысокая стоимость. Многие компании-производители аппаратных шлюзов дополняют линейку своих продуктов чисто программной реализацией VPN-клиента, который рассчитан на работу в среде стандартной ОС.

Отметим такие распространенные VPN-средства на базе специализированного программного обеспечения, как программные продукты RAS (Remote Access Service) и RRAS (Routing and Remote Access Service) от компании Microsoft и AltaVista Tunnel от компании Digital Equipment, которые поддерживают защищенную передачу данных от одной локальной сети к другой и от удаленного компьютера к локальной сети.

Лабораторная работа 14
VPN НА БАЗЕ АППАРАТНЫХ СРЕДСТВ

1. Цель работы: научиться создавать инфраструктуру защищенных виртуальных каналов на базе аппаратных средств.

2. Задачи работы:

− создать инфраструктуру защищенных виртуальных каналов на базе аппаратных средств

Студент должен:

Иметь практический опыт:

- защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание

Нарисовать схему, демонстрирующую пример работы VPN на базе аппаратных средств.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;

6. **Контрольные вопросы**

1. Какие компоненты входят в аппаратные VPN-средства?
2. Какие алгоритмы шифрования используются в аппаратных VPN-средствах?
3. Какие методы аутентификации используются в аппаратных VPN-средствах?
4. Какие меры безопасности необходимо принимать при использовании аппаратных VPN-средств?
5. Какие функции обеспечивает аппаратное VPN-средство?

Приложение 1

Краткие сведения из теории

Выделенные аппаратные шлюзы реализованы в виде отдельного аппаратного устройства. Основная функция которого – высокопроизводительное шифрование траффика. VPN-устройствами являются фактическими лидерами практически по всем показателям, кроме одного – стоимости. Аппаратные шлюзы высшего класса обязательно поддерживают IPsec, причем со многими расширениями в виде новых и мощных в криптографическом отношении алгоритмов. Обладают высокой производительностью за счет аппаратной поддержки операций шифрования. По удобству и простоте инсталляции, аппаратные шлюзы обычно намного превосходят программные шлюзы и такие комбинированные решения, как шлюзы на основе брандмауэров и маршрутизаторов. Аппаратное устройство уже при включении готово работать, ему не надо проходить громоздкий процесс инсталляции в среде какой-либо ОС, как это требуется для большинства программных или комбинированных продуктов, а для работы необходимо только задать значения конкретных адресов и, может быть, ключей для установления тоннелей. Многие специалисты считают, что специализированное аппаратное VPN-оборудование является наилучшим решением для ответственных применений. Пример: Permit Enterprise (PE) – IPsec-совместимый комплект VPN-продуктов, разработанный для организации информационного взаимодействия предприятий. PE легко развертывается в уже существующих сетях, не оказывая существенного влияния на производительность сети и конечных пользователей. Его масштабируемая архитектура дает возможность создавать и управлять несколькими VPN. PE является полным решением для построением корпоративных интросетей, экстрасетей и организации удаленного доступа через интернет. Компания «Time step» предлагает 4 различных модификации шлюза: Permit/Gate 1520, 2520, 4520, 7520, которые соответствуют различным размерам проектируемых VPN:

· Permit/Gate 1520 – недорогое автономное устройство для установки в сети предприятия, кроссплатформенна. Эта модель позиционируется компанией «Time step» для связи с другим высокопроизводительным шлюзом этой серии «Time step» Permit/Gate, размещаемом в центральном офисе компании.

· Permit/Gate 2520 и Permit/Gate 4520 – позиционируется для офисов, отделений и малых корпоративных LAN (локальных сетей). Эти устройства больше всего подходят для обеспечения безопасной связи по технологии VPN между несколькими филиалами предприятия.

· Permit/Gate 7520 – прекрасно подходит для приложений, использующих Fast Ethernet, а также имеют возможность поддерживать тысячи удаленных пользователей. В широкомасштабных проектах этот шлюз является очень хорошим средством для построения VPN, связывающей защищенными туннелями сеть центрального офиса предприятия с сетями его филиалов и отделений с сетями его партнеров, а также большим количеством удаленных пользователей, рабочие места которых оснащены другими продуктами линейки Permit Enterprise.

Каждый из шлюзов Permit/Gate поставляется с программной утилитой Permit/Config, которая позволяет удаленно конфигурировать, управлять и модифицировать ПО нескольких шлюзов из любой точки VPN.

Важнейшим достоинством шлюзов Permit/Gate является аппаратная реализация шифрования, что обеспечивает высокую производительность обработки траффика. Permit/Gate 7520 оснащен аппаратными средствами реализации IPsec, которая позволяет поддерживать тысячи VPN-соединений без уменьшения производительности. Это дает возможность относительно легко расширять корпоративную сеть по мере потребности в этом.

Лабораторная работа 15

ИСПОЛЬЗОВАНИЕ ТОКЕНА НА РАБОЧЕМ МЕСТЕ АДМИНИСТРАТОРА

1. **Цель работы**: изучить средства и методы применения рутокена на рабочем месте администратора.

2. **Задачи работы:**

- научиться применять токен на рабочем месте администратора

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. **Задание и порядок выполнения работы:**

настройка и тестирование аутентификации по токену для доступа к системе управления пользователями или ресурсами сети

Для этого необходимо выполнить следующие шаги:

1. Настроить инфраструктуру для использования токена, включая установку и настройку необходимого программного обеспечения (например, установка драйверов для считывателя токенов, установка ПО для аутентификации по токену и т.д.).
2. Создать учетную запись пользователя, которому будет предоставлен доступ к системе управления пользователями или ресурсами сети.
3. Настроить систему для аутентификации по токену для созданного пользователя.
4. Протестировать аутентификацию по токену, используя созданный пользовательский аккаунт.
5. Провести анализ уязвимостей системы и выработать меры по улучшению ее безопасности, если это необходимо.

5. **Содержание отчета**

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое «Рутокен»?
2. Для чего используется Рутокен VPN?
3. На чем основывается Рутокен для Windows?

Приложение 1

Краткие сведения из теории

Рутокен — это вид ключевого носителя (токена). Он хранит электронную подпись и цифровой сертификат. В отличие от флешки, на токенах данные защищены паролем и дополнительными средствами безопасности. Рутокены имеют сертификацию ФСТЭК/ФСБ, что соответствует требованиям 63-ФЗ.

Устройства предназначены для использования ключа электронной подписи и ключа проверки электронной подписи. Разработаны на базе криптографических алгоритмов электронной подписи, а также имеют сертификацию ФСБ и ФСТЭК России. Все смарт-карты и токены Рутокен могут дополняться RFID-метками.

Рутокен VPN

Решение для безопасного удалённого доступа. Является комплексной разработкой для доступа к корпоративным ИТ-системам из любой точки мира, предназначенная для компаний малого и среднего бизнеса. Решение базируется на закрытых ключах, хранимых на борту USB-токена, благодаря чему обеспечивается безопасность при удалённой работе с файлами, почтой и программами 1С. В устройстве реализовано стойкое шифрование трафика. Для построения VPN-канала используются криптографические алгоритмы RSA 2048 и AES 256, а все важные операции выполняются «на борту» токенов.

Рутокен для Windows

Позволяет за короткий срок внедрить аппаратную аутентификацию пользователей и защиту электронной переписки в сетях на базе Microsoft Windows Server. Решение построено на применении встроенных инструментов безопасности Windows и устройств Рутокен в качестве носителей ключевой информации. Основа продукта — подробная документация по настройке продуктов Microsoft и применению в них шифрования и электронной подписи.

Лабораторная работа 16
УСТАНОВКА И НАСТРОЙКА СКЗИ «КРИПТОПРО CSP»

1. Цель работы: научиться устанавливать и настраивать СКЗИ «КРПИПТОПРО CSP»

2. Задачи работы:

- Загрузить установочный файл СКЗИ «КриптоПро CSP» с официального сайта.
- Запустить установку и следовать инструкциям установщика.
- Выполнить настройку СКЗИ «КриптоПро CSP».
- Протестировать работу установленного СКЗИ.

Студент должен:

Иметь практический опыт:

- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;

Уметь:

- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
- проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

Знать:

- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

ПК:

- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей..
- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание и порядок выполнения работы

1. Загрузить установочный файл СКЗИ «КриптоПро CSP» с официального сайта. Для этого нужно зайти на сайт www.cryptopro.ru и найти раздел «СКЗИ «КриптоПро CSP»». После этого нужно выбрать нужную версию СКЗИ и скачать установочный файл.
2. Запустить установку и следовать инструкциям установщика. Для установки нужно запустить скачанный установочный файл и следовать инструкциям установщика. Во время установки необходимо выбрать папку, в которую будет установлен СКЗИ.
3. Выполнить настройку СКЗИ «КриптоПро CSP». После установки необходимо выполнить настройку СКЗИ. Для этого нужно открыть

приложение «КриптоПро CSP» и настроить параметры безопасности, выбрать алгоритмы криптографической защиты и настроить сертификаты.

4. Протестировать работу установленного СКЗИ. Для проверки работоспособности СКЗИ необходимо запустить программы, использующие криптографические функции, и проверить их работу.
5. Поставить отметку напротив «Включить кеширование».
6. Нажать «ОК».

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Что такое «Криптопровайдер»?
2. Для чего предназначен КриптоПро CSP?
3. Какие алгоритмы использует КриптоПро CSP?

Приложение 1

Краткие сведения из теории

КриптоПро CSP представляет собой криптопровайдер – программный модуль, позволяющий осуществлять криптографические операции в операционных системах, управление которым происходит с помощью функций CryptoAPI. КриптоПро CSP поддерживает российские криптографические алгоритмы (ГОСТ) и имеет сертификаты ФСБ России.

КриптоПро CSP предназначен для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
- контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

КриптоПро CSP реализует следующие алгоритмы:

- алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- алгоритмы формирования и проверки ЭЦП реализованы в соответствии с требованиями ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
- алгоритм зашифрования/расшифрования данных и вычисление имитовставки реализованы в соответствии с требованиями ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая».
- При генерации закрытых и открытых ключей обеспечена возможность генерации с различными параметрами в соответствии ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012.

При выработке значения хэш-функции и шифровании обеспечена возможность использования различных узлов замены в соответствии с ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 и ГОСТ 28147-89.

Лабораторная работа 17

РАБОТА С КОНТЕЙНЕРАМИ ЗАКРЫТОГО КЛЮЧА И СЕРТИФИКАТАМИ ПОЛЬЗОВАТЕЛЯ СРЕДСТВАМИ КРИПТО ПРО CSP

1. **Цель работы**: научиться работать с контейнерами закрытого ключа и сертификатами пользователя средствами КРИПТО ПРО CSP

2. **Задачи работы:**

− ознакомиться с процессом работы с контейнерами закрытого ключа и сертификатами пользователя средствами КриптоПро CSP.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
- проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации.

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. **Подготовка к работе**

Установите программное обеспечение КриптоПро CSP.

4. **Задание и порядок выполнения работы**

1. Запустите криптопровайдер. Для этого перейдите в меню Пуск → Панель управления → КриптоПро CSP.
2. В открывшемся окне перейдите на вкладку Сервис и нажмите на кнопку Установить личный сертификат.
3. В следующем окне нужно задать расположение файла сертификата. Для этого выберите путь к файлу с помощью кнопки Обзор.
4. Откроется окно Контейнер закрытого ключа. Чтобы задать контейнер вручную, нажмите на кнопку Обзор и выберите его из списка. Мастер установки также может находить контейнер автоматически. Для этого установите соответствующую галочку и в блоке Введённое имя задаёт ключевой контейнер выберите нужный Пользователя.

5. Выберите хранилище, в которое будет установлен сертификат. Проставьте флажок Установить сертификат в контейнер.
6. В окне Завершение работы мастера установки личного сертификата проверьте, правильно ли указаны параметры. Чтобы установить сертификат ЭП, нажмите кнопку Готово.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. Контрольные вопросы к защите

1. Для чего используется электронная подпись?
2. Что такое «Личный сертификат»?
3. Как создать сертификат в КриптоПро CSP?

Приложение 1

Краткие сведения из теории

ЭП - это электронная подпись, предназначенная для:

- Контроля целостности передаваемых данных
- Защиты от перехвата передаваемой информации
- Подтверждения авторства документа

ЭП состоит из связки открытого (личный сертификат) и закрытого ключа шифрования (ключевой контейнер).

Личный сертификат - это файл с расширением .cer, в нём указаны данные о владельце сертификата. Открытый ключ необходимо для проверки подлинности документа, а связанный с ним закрытого ключа для зашифровки данных.

Закрытый ключ (ключевой контейнер)- это папка с 6 файлами с расширением .key.Если это файлы будут повреждены или утеряны, закрытый ключ не будет работать. Восстановить ключевой контейнер невозможно, если нет в наличии его копии.

Лабораторная работа 18
ПРОЕКТИРОВАНИЕ СТЕНДА ДЛЯ РЕАЛИЗАЦИИ IDS

1. Цель работы: научиться проектировать стенд для реализации IDS

2. Задачи работы:

- Изучение требований к системе IDS в соответствии с целями и задачами проекта.
- Выбор программного обеспечения, необходимого для реализации системы IDS.
- Определение железных требований для стенда, например, процессора, памяти и дискового пространства.
- Настройка среды разработки и установка необходимых пакетов и библиотек для реализации IDS.
- Разработка алгоритмов и логики обработки данных в системе IDS.
- Настройка сетевого интерфейса и настройка мониторинга сетевого трафика.

Студент должен:

Иметь практический опыт:

- защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Уметь:

- выявлять и оценивать угрозы безопасности информации в ИТКС;
- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

Знать:

- возможные угрозы безопасности информации в ИТКС;
- способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё;
- порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

ПК:

- ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

3. Подготовка к работе

Познакомьтесь с материалами теоретической части работы, изложенных в приложении 1.

Подготовить бланк отчета.

4. Задание и порядок выполнения работы

- Необходимо выбрать операционную систему и программное обеспечение для реализации IDS на стенде. Для простоты, можно выбрать любую из популярных Linux-дистрибутивов и установить на нее средство IDS, например, Snort.
- Собрать компьютерное оборудование для создания стенда, включающее в себя: компьютер, необходимые кабели, сетевую карту, монитор и клавиатуру.
- Установить операционную систему на компьютер и настроить сетевую карту для соединения с локальной сетью.
- Установить и настроить средство IDS на компьютере. Настройки могут включать в себя выбор правил обнаружения, конфигурацию сетевых интерфейсов и т.д.
- Протестировать работу стенда, запустив его и подключив к нему другие компьютеры в локальной сети, включая компьютеры с вредоносным ПО.

- Проверить работу средства IDS на стенде, с помощью анализа журналов обнаружения и реакции на вредоносное ПО в локальной сети.
- Оформить отчет о выполнении задания, содержащий описание процесса создания стенда, настройки и тестирование средства IDS, а также полученные результаты и выводы.

5. Содержание отчета

1. название и цель работы;
2. перечень осваиваемых компетенций;
3. задание;
4. исходные данные по заданию/варианту;
5. ход выполнения работ;
6. выводы по работе;
7. ответы на контрольные вопросы.

6. **Контрольные вопросы**

1. Какие протоколы используются в IDS?
2. Какие алгоритмы используются в IDS?
3. Какие основные этапы проектирования стенда для реализации IDS?
4. Какие аппаратные компоненты необходимы для реализации IDS?
5. Какие программные компоненты необходимы для реализации IDS?
6. Какие меры безопасности необходимо принимать при использовании IDS?

Приложение 1

Краткие сведения из теории

IDS (Intrusion Detection System) - это система обнаружения вторжений, которая используется для защиты компьютерных сетей от несанкционированного доступа. IDS может обнаруживать попытки атак на сеть, такие как сканирование портов, внедрение вредоносного кода, взлом паролей и другие виды кибератак.

Проектирование стенда для реализации IDS включает в себя выбор аппаратных и программных компонентов, настройку системы обнаружения вторжений и настройку системы уведомлений и отчетности. Важным этапом является выбор подходящих средств мониторинга и обнаружения атак, таких как снифферы, IDS-сенсоры и анализаторы трафика.

При проектировании стенда IDS также необходимо учитывать факторы, такие как тип сети (локальная или глобальная), ее топологию, тип и количество устройств в сети, наличие фильтров и брандмауэров, а также уровень угроз и необходимость защиты. В результате проектирования должна быть создана система, которая обеспечивает эффективную защиту сети от внешних и внутренних угроз.