Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

МЕРЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

сборник учебно-методических материалов для направления подготовки 10.03.01 Информационная безопасность

Благовещенск, 2019

Печатается по решению
редакционно-издательского совета
факультета математики и информатики
Амурского государственного
Университета

Составитель: Баранов А.А.

Меры по обеспечению информационной безопасности: сборник учебно-методических материалов для направления подготовки 10.03.01 Информационная безопасность – Благовещенск: Амурский гос. ун-т, 2019.

Содержание

Краткое изложение лекционного материала.

Тема 1. Уязвимости информационных систем и угрозы информационной безопасности

Цель лекции. Рассмотреть основные принципы и средства защиты информации.

План

1. Понятие уязвимости.
2. Примеры уязвимостей программных систем.
3. Угрозы информационной безопасности.

Краткое содержание

Компания ISS(InternetSecuritySystems) разработала следующую классификацию уязвимостей:

- Уязвимости, реализованные или созданные продавцом (разработчиком) программного или аппаратного обеспечения. Включают: ошибки, не установленные обновления (SP, patchihotfix) операционной системы, уязвимые сервисы и незащищенные конфигурации по умолчанию.
- Уязвимости, добавленные администратором в процессе управления компонентами системы. Представляют собой доступные, но неправильно используемые настройки и параметры информационной системы, не отвечающие политике безопасности (например, требования к минимальной длине пароля и несанкционированные изменения в конфигурации системы).
- уязвимости, привнесенные пользователем в процессе эксплуатации системы. Включают уклонения от предписаний принятой политики безопасности, например, отказ запускать ПО для сканирования вирусов или использование модемов для выхода в сеть Internetв обход межсетевых экранов и другие, более враждебные действия.

В более общем виде уязвимости могут быть классифицированы по этапам жизненного цикла ИС:

- Уязвимости проектирования (проектирование)
- Уязвимости реализации (реализация)
- Уязвимости конфигурации (эксплуатация)

Уязвимости проектированиянаиболее серьезны — они обнаруживаются и устраняются с большим трудом. В этом случае уязвимость свойственна проекту или алгоритму и, следовательно, даже совершенная его реализация (что в принципе невозможно) не избавит от заложенной в нем слабости. Например, уязвимость стека протоколов TCP/IP. Недооценка требований по безопасности при создании этого стека протоколов привела к тому, что не проходит месяца, чтобы не было объявлено о новой уязвимости в протоколах стека TCP/IP. И раз и навсегда устранить эти недостатки уже невозможно — существуют только временные или неполные меры. Однако бывают и исключения. Например, внесение в проект корпоративной сети множества модемов, облегчающих работу персонала, но существенно усложняющих работу службы безопасности. Это приводит к появлению потенциальных путей обходов межсетевого экрана, обеспечивающего защиту внутренних ресурсов от несанкционированного использования. И обнаружить, и устранить эту уязвимость достаточно легко.

Уязвимости реализации состоят в появлении ошибки на этапе реализации в программном или аппаратном обеспечении корректного с точки зрения безопасности проекта или алгоритма. Яркий пример такой уязвимости —*"переполнение буфера"* во многих реализациях программ, например,sendmailилиInternetExplorer. Обнаруживаются и устраняются подобного рода уязвимости относительно легко. Если нет исходного кода программно-

го обеспечения, в котором обнаружена уязвимость, то ее устранение заключается или в обновлении версии уязвимого ПО или в полной его замене или отказе от него.

Уязвимости конфигурации состоят в ошибках при конфигурации программного или аппаратного обеспечения. Этот вид наряду с уязвимостями реализации является самой распространенной категорией уязвимостей. Существует множество примеров таких уязвимостей. К их числу можно отнести, например, доступный, но не используемый на узле сервисTelnet, разрешение "слабых" паролей или паролей длиной менее 6 символов, учетные записи и пароли, остановленные по умолчанию (например,SYSADMилиDBSNMPв СУБДOracle), и т. д. Локализовать и исправить такие уязвимости проще всего. Основная проблема — определить, является ли конфигурация уязвимой.

Наиболее распространенные уязвимости

По статистике, опубликованной в 1998 году институтом SANS(System Administrator and Network Security), пятерка наиболее распространенных уязвимостей выглядела следующим образом:

1. Выслеживание информации, особенно паролей и иной конфиденциальной информации.
2. Переполнение буфера, приводящее к удаленному выполнению произвольных команд.
3. Уязвимости системы защиты узлов, например, уязвимости сценариев CGIили ошибки bsendmail.
4. Подверженность атакам типа *"отказ в обслуживании"*.
5. Допустимость загрузки враждебного кода, к которому можно отнести программы типа *"троянский конь",*вирусы, апплетыJava, элементы управленияActiveX.

Можно заметить, что в первую пятерку вошли все три категории уязвимостей. Выслеживание паролей возможно благодаря отсутствию механизмов шифрования в стандартных протоколах Internet. Переполнение буфера, уязвимости защиты узлов и подверженность атакам типа "отказ в обслуживании" могут быть отнесены к разряду уязвимостей реализации и конфигурации. Ну и, наконец, возможность загрузки враждебного кода может быть причислена к разряду уязвимостей конфигурации.

В 2001 году пятерка наиболее распространенных уязвимостей по данным SANS обновилась:

1. Слабости BIND(службы доменных имен в Internet).
2. Уязвимые CGI-сценарии и расширения приложений, установленные наWeb-сервере.
3. Уязвимости RPC.
4. Уязвимости Remote Data Services (RDS) в MS IIS.
5. Переполнение буфера в почтовой программе sendmail.

Эта пятерка частично совпадает с исследованиями компании ISS:

1. Подверженность атакам типа "отказ в обслуживании" (в том числе и распределенным атакам этого типа).
2. "Слабые" учетные записи (для серверов, маршрутизаторов и т. д.).
3. Уязвимости ПО MS IIS.
4. Уязвимости СУБД (неправильные права доступа к расширенным хранимым процедурам, пароли, заданные по умолчанию и т. д.).
5. Приложения eCommerce (Netscape FastTrack, MS FrontPage и др.).

Атаки

До сих пор у профессионалов в области информационной безопасности нет точного определения термина "атака". *Атаку* на информационную систему можно понимать как действие или последовательность связанных между собой действий нарушителя, которые приводят к реализации угрозы путем использования уязвимостей этой информационной системы. Таким образом, атака отличается от события безопасности тем, что в случае ата-

ки злоумышленник пытается достичь некоторого результата, противоречащего политике безопасности. Например, доступ пользователя к файлу или вход в систему — это событие безопасности. Однако, если этот доступ или вход осуществляется в нарушение прав доступа, то это уже атака.

Если построить неформальную модель атаки, которая расширяет описанную выше для события безопасности, то получится модель, состоящая из 4-х элементов.

Для того чтобы реализовать атаку, *злоумышленник* моделирует некоторое событие безопасности, которое приводит к искомому результату при помощи некоего средства, использующего уязвимости системы. Первые два элемента данной модели применяются для реализации события безопасности, т. е. некоторого действия по отношению к адресату для достижения результата, приводящего к нарушению политики безопасности.

Тема 2. Криптографические методы защиты информации

Цель лекции. Рассмотреть основные криптографические методы и средства защиты информации**.**

План

1. Основные термины и определения криптографии
2. Классификация криптосистем
3. Симметричные криптосистемы
4. Асимметричные криптосистемы.

Краткое содержание

Криптография – наука, изучающая математические методы защиты информации, методы преобразования, обеспечивающие ее конфиденциальность и аутентичность.

Конфиденциальность – невозможность получения информации из преобразованного массива, без знания дополнительной информации.

Аутентичность – проверка подлинности.

Криптоанализ – объединенные математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

Стеганография – обеспечение скрытности передаваемой информации.

Криптографическая стойкость – способность системы быть устойчивой к анализу аналитических методов перебора.

Алфавит – конечное множество, используемых для кодирования информации знаков.

Текст (сообщение) – упорядоченный набор из элементов алфавита.

Кодирование – любое преобразование данных из одной формы представления в другую.

Шифрование – преобразование текста, в результате которого прочитать зашифрованный текст может только тот, кто обладает специальным ключом.

Шифр – совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографическим преобразования.

Ключ (секретное слово) – конкретное секретное состояние некоторых параметров алгоритма криптографических преобразований.

Дешифрование – процесс преобразования закрытых данных в открытые, при неизмененном ключе, при условии, что данный ключ неизвестен и алгоритм который используется тоже неизвестен.

Стойкость шифра – (противостояние криптоанализу) должна быть такой, чтобы вскрытие его могло быть осуществлено только решением задачи перебора всех ключей, требованием созданием дорогих вычислительных машин.

Алгоритм – некий режим шифрования, который зависит от ситуации, ценности информации.

Тема 3. Информационная безопасность операционных систем.

Цель лекции. Определить основные угрозы безопасности персональных данных пути их реализации.

План

1. Средства идентификации и аутентификации пользователей.
2. Механизмы управления доступом.
3. Механизмы защиты данных в оперативной памяти.
4. Средства обеспечения целостности и доступности информации в операционных системах.

Краткое содержание

В открытой сетевой среде между сторонами *идентификации*/*аутентификации* не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от ***перехвата***, ***изменения*** и/или ***воспроизведения*** данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от *воспроизведения*. Нужны более сложные протоколы *аутентификации*.

Надежная *идентификация* и затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все *аутентификационные* сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью *аутентификации*, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить *аутентификационную* информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства *идентификации*/*аутентификации* должны поддерживать концепцию *единого входа в сеть*. *Единый вход в сеть* - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная *идентификация*/*аутентификация* становится слишком обременительной. К сожалению, пока нельзя сказать, что *единый вход в сеть* стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств *идентификации* и *аутентификации*.

Тема 4. Безопасность компьютерных сетей

Цель лекции. Рассмотреть основные методы обеспечения безопасности компьютерных сестей.

План

1. Межсетевое экранирование.
2. Виртуальные защищенные сети.

Краткое содержание

Одним из эффективных механизмом обеспечения информационной безопасности распределенных вычислительных сетях является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет **межсетевой экран** или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

- по месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
- по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов, например, при использовании сетевой операционной системы Novell Netware, следует принимать во внимание протокол SPX/IPX.

Тема 5. Методы и механизмы обеспечения информационной безопасности в системах баз данных.

Цель лекции. Рассмотрение методов и механизмов обеспечения информационной безопасности в системах баз данных

План

1. Средства управления транзакциями.
2. Механизмы обеспечения целостности информации в базах данных.
3. Механизмы управления доступом.
4. Средства резервирования.

Краткое содержание

В предложенной выше модели вычислений клиент/сервер при ориентации в основном на сервер базы данных предусматривается также использование по возможности элементов модели сервера приложений. Перенос на сервер часть логики приложений обеспе-

чит разгрузку ресурсов клиентов и более надежный контроль за выполняемыми клиентами действиями. При этом предполагается, что обращения к системе управления базами данных будут формировать не конечные клиенты, а части прикладной задачи, выполняющиеся на сервере. Такое построение системы требует специальной поддержки, обеспечивающей непротиворечивость функционирования и целостность данных при параллельной многопользовательской работе. Бойко В.В., Савинков В.М., Проектирование баз данных и информационных систем. - М.: Финансы и статистика, 2002. - 304 с. Такая поддержка обеспечивается программными средствами называемыми транзакциями.

SQL Server предлагает множество средств управления поведением транзакций. Пользователи в основном должны указывать только начало и конец транзакции, используя команды SQL или API (прикладного интерфейса программирования). Транзакция определяется на уровне соединения с базой данных и при закрытии соединения автоматически закрывается. Если пользователь попытается установить соединение снова и продолжить выполнение транзакции, то это ему не удастся. Когда транзакция начинается, все команды, выполненные в соединении, считаются телом одной транзакции, пока не будет достигнут ее конец.

SQL Server поддерживает три вида определения транзакций:

- - явное;
- - автоматическое;
- - подразумеваемое.

По умолчанию SQL Server работает в режиме автоматического начала транзакций, когда каждая команда рассматривается как отдельная транзакция. Если команда выполнена успешно, то ее изменения фиксируются. Если при выполнении команды произошла ошибка, то сделанные изменения отменяются и система возвращается в первоначальное состояние.

Когда пользователю понадобится создать транзакцию, включающую несколько команд, он должен явно указать транзакцию.

Сервер работает только в одном из двух режимов определения транзакций: автоматическом или подразумевающемся. Он не может находиться в режиме исключительно явного определения транзакций. Этот режим работает поверх двух других.

Для установки режима автоматического определения транзакций используется команда «SET IMPLICIT_TRANSACTIONS OFF».

При работе в режиме неявного (подразумевающегося) начала транзакций SQL Server автоматически начинает новую транзакцию, как только завершена предыдущая. Установка режима подразумевающегося определения транзакций выполняется посредством другой команды «SET IMPLICIT_TRANSACTIONS ON».

Тема 6. Методы обнаружения уязвимостей и атак.

Цель лекции. Рассмотреть основные методы обнаружения уязвимости и атак.

План

1. Основные термины и определения.
2. Принципы обнаружения уязвимостей и атак.
3. Антивирусные системы.
4. Системы обнаружения вторжений.
5. Сканеры уязвимостей.
6. Методы и средства верификации программного обеспечения и баз данных..

Краткое содержание

Система обнаружения атак — это программный или программноаппаратный комплекс, предназначенный для выявления и по возможности предупреждения действий, угрожающих безопасности информационной системы.

Первые прототипы СОА появились в начале 1980-хгодов и были ориентированы в первую очередь на защиту автономных ЭВМ, не объединенных в сеть. Обнаружение атак производилось путем анализа журналов регистрации событий постфактум. Современные системы в основном ориентированы на защиту от угроз, направленных из сети, поэтому их архитектура существенным образом поменялась. Вместе с тем основные подходы к обнаружению атак остались прежними. Рассмотрим классификацию и принципы работы СОА более подробно.

Основные подходы к обнаружению атак практически не изменились за последнюю четверть века, и, несмотря на громкие заявления разработчиков, можно с уверенностью утверждать, что концептуально обнаружение атак базируется либо на методах *сигнатурного анализа*, либо на методах*обнаружения аномалий*. Возможно также совместное использование указанных выше методов.

Сигнатурный анализ основан на предположении, что сценарий атаки известен и попытка ее реализации может быть обнаружена в журналах регистрации событий или путем анализа сетевого трафика. В идеале администратор информационной системы должен устранить все известные ему уязвимости. На практике, однако, данное требование может оказаться невыполнимым, так как в результате может существенным образом пострадать функциональность ИС. Не исключено также, что людские и материальные затраты, необходимые для устранения этих уязвимостей, могут превысить стоимость информации, обрабатываемой системой. Системы обнаружения атак, использующие методы сигнатурного анализа, предназначены для решения обозначенной проблемы, так как в большинстве случаев позволяют не только обнаружить, но и предотвратить реализацию атаки на начальной стадии ее выполнения.

Процесс обнаружения атак в данных системах сводится к поиску *заранее известной* последовательности событий или строки символов в упорядоченном во времени потоке информации. Механизм поиска определяется способом описания атаки.

Наиболее простым является описание атаки при помощи набора правил (условий). Применительно к анализу сетевых пакетов эти правила могут включать определенные значения отдельных полей заголовка пакета

Методические указания к практическим занятиям

Практическая работа 1.

Угрозы информационной безопасности..

Цель занятия. Изучение основных понятий и определений, связанных с дисциплиной..

Задание

1. Разграничение доступа к устройствам.
2. Выполнить контроль печати конфиденциальных данных.
3. Построить глоссарий по теме

Контрольные вопросы

1. Что такое информационная безопасность?
2. Перечислить виды угроз.
3. Назвать методы защиты информации?
4. Раскрыть понятие компьютерное преступление.
5. Что такое конфиденциальность информации?
6. Что такое целостность данных?
7. Что такое доступность данных?
8. В каком случае информация считается защищенной?
9. Назвать источники информации, требующие защиты?
10. Что относится к способам получения доступа к информации?

Практическая работа 2.

Криптографические методы защиты информации

Цель занятия. Научиться использовать криптографические методы защиты информации

Задание

1. Основные понятия и определения темы «криптографические методы защиты информации»
2. Алгоритмы криптографических методов защиты информации.
3. Решение задач.

Контрольные вопросы

1. Какие основные виды политики безопасности известны?
2. В чем суть дискреционной политики безопасности?
3. Какими условиями определяется мандатная политика безопасности?
4. Чем отличается политика безопасности информационных потоков от политики ролевого разграничения доступа?
5. Какова цель реализации политики изолированной программной среды?
6. Что такое матрица доступов?
7. Перечислить классические угрозы безопасности?
8. Как описываются информационные потоки по времени и по памяти?
9. Какие математические понятия используются в моделях безопасности?
10. Какая задача является алгоритмически разрешимой?

Практическая работа 3.

Информационная безопасность операционных систем

Цель занятия. Выявить проблемы, связанные с информационной безопасностью операционных систем

Задание

1. Рассмотреть теоретические вопросы информационной безопасности операционных систем
2. Методы обеспечения информационной безопасности операционных систем

Контрольные вопросы

1. Что такое разграничение доступа?
2. В чем суть ролевого управления?
3. Почему протоколирование и аудит относят к пассивным сервисам безопасности?
4. Какие функции выполняет экранирование как сервис безопасности?
5. Для каких целей используется туннелирование?

Практическая работа 4

Безопасность компьютерных сетей.

Цель занятия. Выявить проблемы, связанные с информационной безопасностью компьютерных сетей

Задание

1. Рассмотреть теоретические вопросы информационной безопасности компьютерных сетей
2. Методы обеспечения информационной безопасности компьютерных сетей

Контрольные вопросы

1. Что такое замкнутая программная среда?
2. Что такое UEL-список?
3. Как настраивается замкнутая программная среда?
4. Какими сервисами обладает Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 для отслеживания работы замкнутой программной среды.
5. Что такое мягкий режим замкнутой программной среды?
6. Чем отличается мягкий режим замкнутой программной среды от жесткого режима.

Практическая работа 5

Методы и механизмы обеспечения информационной безопасности в системах баз данных

Цель занятия. Рассмотреть методы и механизмы обеспечения информационной безопасности в системах баз данных

Задание.

1. Рассмотреть теоретические вопросы информационной безопасности в системах баз данных

2. Методы обеспечения информационной безопасности в системах баз данных

Контрольные вопросы

1. Что такое компьютерный вирус? Какими свойствами обладают компьютерные вирусы?
2. По каким признакам классифицируют компьютерные вирусы? Перечислите типы вирусов.
3. Какие вирусы называются резидентными и в чем особенность таких вирусов?
4. Каковы отличия вирусов-репликаторов, стелс - вирусов, мутантов и «троянских» программ?
5. Опишите схему функционирования загрузочного вируса.
6. Опишите схему функционирования файлового вируса.
7. Опишите схему функционирования загрузочно-файловых вирусов.
8. Что такое полиморфный вирус? Почему этот тип вирусов считается наиболее опасным?

Практическая работа 6

Методы обнаружения уязвимостей и атак

Цель занятия. Рассмотреть методы обнаружения уязвимостей и атак.

Задание

1. Изучение документа "Руководящий документ средства вычислительной техники защита от несанкционированного доступа к информации показатели защищенности от несанкционированного доступа к информации " (утв. Гостехкомиссией при президенте рф от 30.03.92)
2. В соответствии с руководящим документом выполнить классификацию средств вычислительной техники для медицинского учреждения.
3. Определить план проведения аудита событий в АС

Контрольные вопросы

1. Перечислить классы защищенности СВТ?
2. Назвать характеристики, положенные в основу определения классов защищенности СВТ.
3. Какие характеристики рассматриваются при выполнении оценки защищенности сетевых ресурсов?
4. Какой документ определяет защищенность средств вычислительной техники.
5. Сколько классов защищённости СВТ от НСД существует?
6. Верно ли утверждение «Требования ужесточаются с уменьшением номера класса»?
7. Какой вид контроля доступа реализуется для всех классов СВТ?

Методические указания к лабораторным занятиям

Лабораторная работа 1. Выявление уязвимостей программных систем.

Цель лабораторной работы. Изучение основных методов и средств идентификации уязвимостей, реализованных в специализированных сканерах безопасности программных приложений.

Задание

1. Выполнить ручные проверки наличия обнаруженных сканером уязвимостей в веб-приложении.
2. Выполнить сканирование того же приложения с помощью сканера W3AF, сравнить полученные результаты.
3. Реализовать веб-приложение, уязвимое к атаке XSS, которое инвертирует введенные пользователем данные и выводит их в HTML-документ.
4. Выполнить сканирование данного приложения с помощью любого сканера веб-приложений.

Контрольные вопросы

1. Каково назначение сканера W3AF?
2. Что такое атака XSS?
3. Как выполняется ручная проверка наличия обнаруженных сканером уязвимостей?
4. Какие известны сканеры веб-приложений?
5. Перечислить уязвимости программных приложений.

Лабораторная работа 2. Симметричные криптосистемы. Асимметричные криптосистемы.

Цель работы: Разработать криптографическую защиту информации, содержащейся в текстовом (двоичном) файле данных, с помощью алгоритма шифрования.

Задание

1. Разработать алгоритмы шифрования и расшифрования открытого текста из алфавита $A=Z_n$на заданном ключе с помощью метода
   - Шифр простой замены.
   - Шифр сдвига с числовым ключом. Алфавит A – ASCII..
   - Шифр сдвига с символьным ключом. Алфавит A– латинские буквы и символ пробела.
   - Аффинный шифр.
   - Преобразование биграмм аффинным шифром. (не путать с аффинным блочным шифром)
   - Преобразование триграмм аффинным шифром. (не путать с аффинным блочным шифром)
   - Шифр Виженера с ключевым словом. Алфавит A– латинские буквы и символ пробела.
   - Шифр Виженера с числовым ключом. Алфавит A – ASCII.
   - Многопетлевые подстановки. Алфавит A– латинские буквы и символ пробела.

– Многопетлевые подстановки. Алфавит *A*– ASCII.

2. Определить алфавит *A*криптосистемы (открытого текста и шифртекста). Если алфавит*A*не задан в варианте, выбрать его самостоятельно, так, чтобы он включал в себя символы используемого в примере открытого текста. Например, русский, английский, ASCII. Поставить символам исходного алфавита*A*в соответствие символы из алфавита Z_n(*n*– основание алфавита).

3. Написать функцию генерации случайных ключей шифра, оценить размерность ключевого пространства.

4. Написать функцию, реализующую шифрование на заданном ключе открытого текста, состоящего из символов заданного алфавита. Открытый текст, ключ и шифртекст должны быть представлены отдельными файлами.

5. Написать функцию для реализации алгоритма расшифрования полученного шифрованного файла при известном ключе.

Контрольные вопросы

1. Общая схема алгоритма шифрования DES.
2. Почему длина ключа для алгоритма DES равна 56 бит?
3. Как соотносятся между собой матрицы и в алгоритме DES?
4. Как происходит шифрование функции (( ) ( )) в алгоритме DES?
5. Алгоритм получения раундовых ключей ( ) в алгоритме DES.
6. В чём заключается процесс расшифрования данных в DES?
7. Что представляет собой функция () в алгоритме ГОСТ?
8. Как используется заданный ключ при шифровании в алгоритме ГОСТ?
9. Общие черты и отличия алгоритмов ГОСТ и DES.
10. Критерии оценки свойств лавинного эффекта.

Лабораторная работа3. Информационная безопасность операционных систем.

Цель работы: освоение средств защищенных версий операционной системы Windows, предназначенных для Разграничения доступа.

Задание

Используя средства операционной системы Windows выполнить следующие задачи:

1. Обеспечить разграничение доступа субъектов к папкам и файлам;
2. Выполнить разграничение доступа субъектов к принтерам;
3. Организовать разграничение доступа к разделам реестра;
4. Обеспечить конфиденциальность папок и файлов с помощью шифрующей файловой системы.

Контрольные вопросы

1. Какие основные виды политики безопасности известны?
2. В чем суть дискреционной политики безопасности?
3. Какими условиями определяется мандатная политика безопасности?
4. Чем отличается политика безопасности информационных потоков от политики ролевого разграничения доступа?
5. Какова цель реализации политики изолированной программной среды?
6. Что такое матрица доступов?

7. Перечислить классические угрозы безопасности?
8. Как описываются информационные потоки по времени и по памяти?
9. Какие математические понятия используются в моделях безопасности?
10. Какая задача является алгоритмически разрешимой?

Лабораторная работа4. Безопасность компьютерных сетей

Цель работы. **Ознакомление с методами защиты от вторжений.**
Усвоить основные требования к защите вычислительной сети.

Задание

1. Выполнить проверку сетевой конфигурации тестовой среды;
2. Выполнить анализ трафика основных протоколов стека TCP/IP с помощью Wireshark;
3. Выполнить организацию доступа к веб-сайту по SSL;
4. Выполнить защиту электронной почты с помощью PGP.

Контрольные вопросы

1. В чем заключается политика безопасности сети?
2. Что представляет наибольшую угрозу безопасности сети?
3. В чем заключается физическая защита оборудования сети?
4. Модели защиты сети?
5. Что такое аудит?
6. Для чего используется шифрование?
7. В чем заключается защита от вирусов?
8. Как осуществляется защита данных от потерь?
9. Методы резервного копирования информации?
10. Назначение и уровни RAID-массивов?

Лабораторная работа 5. Методы и механизмы обеспечения информационной безопасности в системах баз данных

Цель работы: Изучить способы защиты решений в СУБД

Задание

1. Установить пароль доступа к базе данных, для примера взять БД, сформированную в Access в предыдущих лабораторных работах. Удалить пароль. Для выполнения задания выберите пункт меню Сервис ► Защита ► Задать пароль базы данных (Tools ► Sequirity ► Set Database Password). Удаление и изменение пароля исследовать самостоятельно.
2. Установить и снять пароль из программы. Для выполнения этого задания необходимо написать программу на VBA. Создайте кнопку для любой формы, на событие «нажатие кнопки» присоедините программу работы с паролями. В отчет включить программу на VBA и рекомендации по работу с паролями администратору безопасности и пользователю БД.
3. Установить защиту на уровне пользователей.
4. Создать учетные записи групп и пользователей.

5. Создать, учетную запись Администратора.

Контрольные вопросы

1. Какие мероприятий выполняются для контроля эффективности защиты информации?
2. Что составляет систему защиты информации?
3. Что относится к недостаткам аппаратных средств инженерно-технической защиты.
4. Перечислить направление инженерно-техническая защита.
5. Выполнить классификация средств инженерно-технической защиты.
6. Дать краткую характеристику основных классов средств инженерно-технической защиты.
7. Перечислить способы защиты информации.
8. Выделить классы способов защиты (мероприятий по защите информации).

Лабораторная работа6. Методы обнаружения уязвимостей и атак защиты

Цель работы: изучить основные принципы защиты программных продуктов от дизассемблирования и противодействия трассировки исполняемого кода с помощью отладчика; программно реализовать один из указанных способов защиты.

Задание

1. Выполнить защиту программы от дизассемблирования методами шифрования, архивации (как разновидность шифрования), использование самогенерируемых кодов, «обман» дизассемблера .
2. Защита программы от трассировки.
3. Защита программ от несанкционированного использования с помощью USB-ключей и программного обеспечения производителя.

Контрольные вопросы

1. Что такое дизассемблирование программного кода?
2. Какими методами выполняется дизассемблирование программного кода?
3. Чем опасна трассировка программы?
4. Что представляет собой самогенерируемый код?
5. Как происходит «обман» дизассемблера?
6. Как происходит защита программ от несанкционированного использования?