ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Б1.Б.1.22 Безопасность операционных систем

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Форма обучения очная

СОДЕРЖАНИЕ

2.2 Лабораторная работа № ЛР-2 «Назначение, возможности систем клона UNIX, систем группы Windows»

2.3 Лабораторная работа № ЛР-3 «Управление ресурсами**»**

2.4 Лабораторная работа № ЛР-4 «Доменная политика конфигураций безопасности. Конфигурирование безопасности в Windows NT**»**

2.5 Лабораторная работа № ЛР-5 «Организация управления доступом и защиты ресурсов ОС**»**

2.6 Лабораторная работа № ЛР-6 «Разработка защищенных приложений. Программное управление файловыми ресурсами и сессиями**»**

2.7 Лабораторная работа № ЛР-7 «Анализ симптома атаки и методы защиты**»**

2.8 Лабораторная работа № ЛР-8 «Анализ установок безопасности системы**»**

2.9 Лабораторная работа № ЛР-9 «Основные механизмы безопасности: средства и методы аутентификации в ОС**»**

2.10 Лабораторная работа № ЛР-10 «Назначение, возможности систем клона UNIX, систем группы Windows**»**

2.11 Лабораторная работа № ЛР-11 «Аудит. Реализация политики аудита**»**

2.12 Лабораторная работа № ЛР-12-13 «Симметричное шифрование и формирование ключа на основе пароля**»**

2.13 Лабораторная работа № ЛР-14-15 «Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС**»**

2.14 Лабораторная работа № ЛР-16-17 «Цифровая подпись. Процедура оформления подписи и проверка**»**

2.1 Методические указания по проведению практических занятий

2.2 Практическое занятие № ПЗ-1 «Элементы безопасности системы. Учетные записи пользователей и групп в ОС Windows NT**»**

2.3 Практическое занятие № ПЗ-2 «Домены Windows NT. Локальная политика безопасности»

2.4 Практическое занятие № ПЗ-3 «Управление ресурсами»

2.5 Практическое занятие № ПЗ-4 «Доменная политика конфигураций безопасности. Конфигурирование безопасности в Windows NT»

2.6 Практическое занятие № ПЗ-5 «Управление программами»

2.7 Практическое занятие № ПЗ-6 «Разработка защищенных приложений. Программное управление учетной записью»

2.8 Практическое занятие № ПЗ-7 «Управление процессами»

2.9 Практическое занятие № ПЗ-8 «Политика безопасности. Управление правами и привилегиями пользователей».

2.10 Практическое занятие № ПЗ-9 «Организация управления доступом и защиты ресурсов ОС**»**

2.11 Практическое занятие № ПЗ-10 «Разработка защищенных приложений. Программное управление файловыми ресурсами и сессиями»

2.12 Практическое занятие № ПЗ-11 «Анализ симптома атаки и методы защиты»

2.13 Практическое занятие № ПЗ 12 «Анализ установок безопасности системы»….

2.14 Практическое занятие № ПЗ 13 «Основные механизмы безопасности: средства и методы аутентификации в ОС»

2.15 Практическое занятие № ПЗ 14 «Аудит. Реализация политики аудита»

2.16 Практическое занятие № ПЗ 15-16 «Модели разграничения доступа»

2.17 Практическое занятие № ПЗ 17-18 «Симметричное шифрование и формирование ключа на основе пароля»

2.18 Практическое занятие № ПЗ 19-22 «Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС»

2.19 Практическое занятие № ПЗ 23-26 «Цифровая подпись. Процедура оформления подписи и проверка»

1. КОНСПЕКТ ЛЕКЦИЙ

1. 1 Лекция № 1 (2 часа).

Тема: «Функции операционных систем. Поколения операционных систем»

1.1.1 Вопросы лекции:

1. Функции операционных систем.
2. Поколения операционных систем.
3. Сетевые операционные системы.

1.1.2 Краткое содержание вопросов:

1. Функции операционных систем.

Операционная система (operating system) – комплекс программ, предоставляющий пользователю удобную среду для работы с компьютерным оборудованием.

Операционная система позволяет запускать пользовательские программы; управляет всеми ресурсами компьютерной системы – процессором (процессорами), оперативной памятью, устройствами ввода вывода; обеспечивает долговременное хранение данных в виде файлов на устройствах внешней памяти; предоставляет доступ к компьютерным сетям.

Все компоненты можно разделить на два больших класса – программы или программное обеспечение (ПО, software) и оборудование илиаппаратное обеспечение (hardware). Программное обеспечение делится на прикладное, инструментальное и системное. Рассмотрим кратко каждый вид ПО.

Цель создания вычислительной системы – решение задач пользователя. Для решения определенного круга задач создается прикладнаяпрограмма (приложение, application). Примерами прикладных программ являются текстовые редакторы и процессоры (Блокнот, MicrosoftWord), графические редакторы (Paint, Microsoft Visio), электронные таблицы (Microsoft Excel), системы управления базами данных (Microsoft Access, Microsoft SQL Server), браузеры (Internet Explorer) и т. п. Все множество прикладных программ называется прикладным программным обеспечением (application software).

Создается программное обеспечение при помощи разнообразных средств программирования (среды разработки, компиляторы, отладчики и т. д.), совокупность которых называется инструментальным программным обеспечением. Представителем инструментального ПО являетсясреда разработки Microsoft Visual Studio.

Основным видом системного программного обеспечения являются операционные системы. Их основная задача – обеспечить интерфейс(способ взаимодействия) между пользователем и приложениями с одной стороны, и аппаратным обеспечением с другой. К системному ПОотносятся также системные утилиты – программы, которые выполняют строго определенную функцию по обслуживанию вычислительной системы, например, диагностируют состояние системы, выполняют дефрагментацию файлов на диске, осуществляют сжатие (архивирование) данных. Утилиты могут входить в состав операционной системы.

Взаимодействие всех программ с операционной системой осуществляется при помощи системных вызовов (system calls) – запросов программ на выполнение операционной

системой необходимых действий. Набор системных вызовов образует API – Application Programming Interface(интерфейс прикладного программирования).

Далее рассмотрим, какие функции должны выполнять современные операционные системы.

К основным функциям, выполняемым операционными системами, можно отнести:

- обеспечение выполнения программ – загрузка программ в память, предоставление программам процессорного времени, обработка системных вызовов;
- управление оперативной памятью – эффективное выделение памяти программам, учет свободной и занятой памяти;
- управление внешней памятью – поддержка различных файловых систем;
- управление вводом-выводом – обеспечение работы с различными периферийными устройствами;
- предоставление пользовательского интерфейса;
- обеспечение безопасности – защита информации и других ресурсов системы от несанкционированного использования;
- организация сетевого взаимодействия.

2. Поколения операционных систем.

40-е годы XX века.

Первые ЭВМ были построены на основе электронных ламп. Они не были предназначены для практических целей. Одни и те же люди проектировали эти машины, писали для них программы и их эксплуатировали. Первые электронные ЭВМ не имели ОС. Функции ОС включались в состав прикладных программ.

Первое поколение ОС.

50-е годы XXв.

Первое поколение ОС было создано для ЭВМ, построенных на полупроводниковых транзисторах. Такие ЭВМ могли работать более длительное время без ошибок и сбоев. Машинное время их стоило очень дорого, поэтому одной из основных функций первых ОС была организация пакетного режима работы. Этот режим позволял сокращать время простоя при переходе от решения одной задачи к другой.

Второе поколение ОС.

Середина 60-х г.

Это поколение ОС было связано с ЭВМ, построенными на основе модулей и первых интегральных схем. Стали появляться ЭВМ с несколькими CPU. ОС для таких машин должны были обладать способностями управлять работой нескольких процессоров, иметь многозадачный режим работы, а так же, обладать возможностью работы с несколькими пользователями. Это были системы коллективного пользования.

На многопроцессорной ЭВМ задача разбивалась на несколько частей, и эти часть параллельно выполнялись на отдельных процессорах, что позволяло резко увеличить вычислительную мощность. Мультипрограммный режим работы заключался в том, что в память ЭВМ загружалось одновременно несколько задач, ОС при этом выделяла процессор каждой задаче на определенное время, автоматически переключая его между всеми задачами.

Режим коллективного пользования заключался в том, что к вычислит.машине подключалось несколько терминалов (монитор и клавиатура), за которыми работали отдельные пользователи. ОС с большей скоростью переключала терминалы, и у каждого пользователя создавалось впечатление, что он один работает с ВМ.

ОС реального времени использовались в ВМ, которые управляли какими-либо машинами или устройствами. Как правило, скорость реакции устройства меньше скорости реакции ЭВМ, ОС реального времени искусственно замедляли работу ЭВМ, приближая ее к скорости устройства или машины.

Третье поколение ОС.

70-е годы XXв.

Это поколение ОС предназначалось для ВМ, построенных на основе интегральных схем, как ЭВМ общего пользования. ЭВМ впервые стали использоваться в промышленности, медицине и т.д.

Появилось большое количество различных типов ЭВМ. Наиболее известным компьютером этого поколения был IBM PC 360. ОС третьего поколения должны были работать на разных типах машин, а, кроме того, должны быть многорежимными, т.е., поддерживать пакетный режим, многозадачный, многопроцессорный и т.д. ОС были громоздкими и сложными, часто содержали большое количество ошибок. Для эксплуатации таких ОС нужна была спецподготовка. Оператору ЭВМ приходилось изучать сложные языки управления задачами.

Но именно в этот период были заложены все основные черты современных ОС.

Четвертое поколение ОС.

80-е годы XXв.

Это поколение связано в первую очередь с ЭВМ на основе больших и сверхбольших интегральных микросхем. Основными классами ЭВМ этого поколения являются ЭВМ общего пользования, мини и микро ЭВМ, персональные ЭВМ и суперЭВМ (многопроцессорные).

Это поколение включает в себя все основные черты ОС предыдущих поколений, а так же имеют следующие особенности:

1. Управление работой сетей ЭВМ.
2. Управление работой сложных многопроцессорных вычислительных комплексов.
3. Появление ОС ПК.

4. ОС начали использовать «дружественный» интерфейс, т.е. ОС строятся в расчете на не подготовленных или малоподготовленных пользователей.

3. Сетевые операционные системы.

Сетевая операционная система (англ. Network operating system) – это операционная система, которая обеспечивает обработку, хранение и передачу данных в информационной сети.

Главными задачами сетевой ОС являются разделение ресурсов сети (например, дисковые пространства) и администрирование сети. Системный администратор определяет разделяемые ресурсы, задаёт пароли, определяет права доступа для каждого пользователя или группы пользователей. Отсюда сетевые ОС делят на сетевые ОС для серверов и сетевые ОС для пользователей.

Существуют специальные сетевые ОС, которым приданы функции обычных систем (например, Windows NT) и обычные ОС (Windows XP), которым приданы сетевые функции. Практически все современные ОС имеют встроенные сетевые функции.

Сетевая операционная система составляет основу любой вычислительной сети. Каждый компьютер в сети в значительной степени автономен, поэтому под сетевой операционной системой в широком смысле понимается совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам - протоколам. Эти протоколы обеспечивают основные функции сети: адресацию объектов, функционирование служб, обеспечение безопасности данных, управление сетью. В узком смыслесетевая ОС - это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

В зависимости от того, как распределены функции между компьютерами сети, сетевые операционные системы, а следовательно, и сети делятся на два класса: одноранговые и двухранговые, которые чаще называют сетями с выделенными серверами.

Если компьютер предоставляет свои ресурсы другим пользователям сети, то он играет роль сервера. При этом компьютер, обращающийся к ресурсам другой машины, является клиентом. Компьютер, работающий в сети, может выполнять функции либо клиента, либо сервера, либо совмещать обе функции.

Если выполнение серверных функций является основным назначением компьютера, то такой компьютер называется выделенным сервером. В зависимости от того, какой ресурс сервера является разделяемым, он называется файл-сервером, факс-сервером, принт-сервером, сервером приложений и т.д. Выделенный сервер не принято использовать в качестве компьютера для выполнения текущих задач, не связанных с его основным назначением, так как это может уменьшить производительность его работы как сервера.

На выделенных серверах желательно устанавливать ОС, специально оптимизированные для выполнения определенных серверных функций. Поэтому в подобных сетях с чаще всего используются сетевые операционные системы, в состав которых входит нескольких вариантов ОС, отличающихся возможностями серверных частей. Например, сетевая ОС Novell NetWare имеет серверный вариант, оптимизированный для работы в качестве файл-сервера.

В одноранговых сетях все компьютеры равны в правах доступа к ресурсам друг друга. Каждый пользователь может по своему желанию объявить какой-либо ресурс своего компьютера разделяемым, после чего другие пользователи могут его использовать. В таких сетях на всех компьютерах устанавливается одна и та же ОС.

1. 2 Лекция № 3 (2 часа).

Тема: «Элементы безопасности системы. Учетные записи пользователей и групп в ОС Windows NT »

1.2.1 Вопросы лекции:

1. Система национальной безопасности Российской Федерации.
2. Основные принципы и функции.

1.2.2 Краткое содержание вопросов:

1. Система национальной безопасности Российской Федерации.

Национальная безопасность Российской Федерации — это то, что обеспечивает потенциал развития страны на длительный исторический период, а также стабильность и благополучие общества. Национальная безопасность предполагает защищенность жизненно важных интересов личности, общества и государства в различных сферах жизнедеятельности от внутренних и внешних угроз.

Особенности существующей в России системы обеспечения национальной безопасности заключаются в специфике президентской формы правления, определенных Конституцией Российской Федерации полномочиях должностных лиц и органов, отвечающих за состояние национальной безопасности. Свои особенности в систему обеспечения национальной безопасности привносят сущностные характеристики национальных интересов и целей Российской Федерации, определяемых се геополитическими положениями, исторической самобытностью, традициями. Направления и задачи по обеспечению национальной безопасности определены в**Концепции национальной безопасности Российской Федерации,**утвержденной Указом Президента Российской Федерации от 10 января 2000 г. № 24.

Интересы государства состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

Основными задачами в области обеспечения национальной безопасности Российской Федерации являются:

- своевременное прогнозирование и выявление внешних и внутренних угроз национальной безопасности Российской Федерации;
- реализация оперативных и долгосрочных мер по предупреждению и нейтрализации внутренних и внешних угроз;
- обеспечение суверенитета и территориальной целостности Российской Федерации, безопасности ее пограничного пространства;
- подъем экономики страны, проведение независимого и социально ориентированного экономического курса;
- преодоление научно-технической и технологической зависимости Российской Федерации от внешних источников;
- обеспечение на территории России личной безопасности человека и гражданина, его конституционных прав и свобод;
- совершенствование системы государственной власти Российской Федерации, федеративных отношений, местного самоуправления и законодательства Российской Федерации, формирование гармоничных межнациональных отношений, укрепление правопорядка и сохранение социально-политической стабильности общества;
- обеспечение неукоснительного соблюдения законодательства Российской Федерации всеми гражданами, должностными лицами, государственными органами, политическими партиями, общественными и религиозными организациями;
- обеспечение равноправного и взаимовыгодного сотрудничества России, прежде всего с ведущими государствами мира;
- подъем и поддержание на достаточно высоком уровне военного потенциала государства;
- укрепление режима нераспространения оружия массового уничтожения и средств его доставки;
- принятие эффективных мер по выявлению, предупреждению и пресечению разведывательной и подрывной деятельности иностранных государств, направленной против Российской Федерации;
- коренное улучшение экологической ситуации в стране.

2. Основные принципы и функции.

Важнейшей гарантией защиты прав и законных интересов личности, общества и государства служит правоохранительная деятельность системы органов обеспечения безопасности.
Правовую основу этой деятельности составляют: Конституция РФ, Закон «О безопасности», указы и распоряжения Правительства РФ и другие нормативные акты РФ, республик в составе РФ, других субъектов Федерации, международные договоры и соглашения, заключенные или признанные РФ.
К основным **объектам безопасности** относятся: личность – ее права и свободы; общество – его материальные и духовные ценности; государство – его конституционный строй, суверенитет итерриториальная целостность.
Основной **субъект обеспечения безопасности** – государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной власти.
Государство в соответствии с действующим законодательством обеспечивает безопасность каждого гражданина на территории Российской Федерации. Гражданам России, находящимся за ее пределами, государством гарантируется защита и покровительство.

Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности.
Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического и организационного характера.
Систему безопасности образуют органы законодательной, исполнительной и судебной власти, государственные, общественные организации и объединения, граждане, принимающие участие в обеспечении безопасности согласно закону, а также законодательство, регламентирующее отношения в данной сфере.
В соответствии с Законом «О безопасности» органами обеспечения безопасности РФ являются: органы Федеральной службы безопасности, внешней разведки, федеральные органы государственной охраны, органы федеральной фельдъегерской связи, органы пожарной безопасности.
Создание органов обеспечения безопасности, не установленных законом РФ, не допускается (ст. 8).
Основными функциями системы органов обеспечения безопасности являются:
– выявление и прогнозирование внутренних и внешних угроз жизненно важным интересам объектов безопасности;
– осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации;
– создание и поддержание в готовности сил и средств обеспечения безопасности;
– управление силами и средствами безопасности в повседневных условиях и при чрезвычайных ситуациях;
– реализация системы мер по восстановлению нормального функционирования объектов безопасности в регионах, пострадавших в результате возникновения чрезвычайной ситуации;
– участие в мероприятиях по обеспечению безопасности за пределами России в соответствии с международными договорами и соглашениями, заключенными или признанными Россией.
Общее руководство государственными органами обеспечения безопасности осуществляет Президент РФ, который возглавляет Совет Безопасности; контролирует и координирует деятельность государственных органов обеспечения безопасности и принимает необходимые оперативные решения.

1. 3 Лекция № 3 (2 часа).

Тема: Назначение, возможности систем клона UNIX, систем группы Windows».

1.3.1 Вопросы лекции:

1.Классификация ОС.
2.Общая характеристика ОС Windows, UNIX.

1.3.2 Краткое содержание вопросов:

1.Классификация ОС.
Операционные системы классифицируются по:

- количеству одновременно работающих пользователей: однопользовательские, многопользовательские;

- числу процессов, одновременно выполняемых под управлением системы: однозадачные, многозадачные;
- количеству поддерживаемых процессоров: однопроцессорные, многопроцессорные;
- разрядности кода ОС: 8-разрядные, 16-разрядные, 32-разрядные, 64-разрядные;
- типу интерфейса: командные (текстовые) и объектно-ориентированные (графические);
- типу доступа пользователя к ЭВМ: с пакетной обработкой, с разделением времени, реального времени;
- типу использования ресурсов: сетевые, локальные.

В соответствии с первым признаком классификации многопользовательские операционные системы, в отличие от однопользовательских, поддерживают одновременную работу на ЭВМ нескольких пользователей за различными терминалами.

Второй признак предполагает деление ОС на многозадачные и однозадачные. Понятие многозадачности означает поддержку параллельного выполнения нескольких программ, существующих в рамках одной вычислительной системы, в один момент времени. Однозадачные ОС поддерживают режим выполнения только одной программы в отдельный момент времени.

В соответствии с третьим признаком многопроцессорные ОС, в отличие от однопроцессорных, поддерживают режим распределения ресурсов нескольких процессоров для решения той или иной задачи.

Четвертый признак подразделяет операционные системы на 8-, 16-, 32- и 64-разрядные. При этом подразумевается, что разрядность операционной системы не может превышать разрядности процессора.

В соответствии с пятым признаком ОС по типу пользовательского интерфейса делятся на объектно-ориентированные (как правило, с графическим интерфейсом) и командные (с текстовым интерфейсом). Согласно шестому признаку ОС подразделяются на системы:

- пакетной обработки, в которых из программ, подлежащих выполнению, формируется пакет (набор) заданий, вводимых в ЭВМ и выполняемых в порядке очередности с возможным учетом приоритетности;
- разделения времени (TSR), обеспечивающих одновременный диалоговый (интерактивный) режим доступа к ЭВМ нескольких пользователей на раз¬ных терминалах, которым по очереди выделяются ресурсы машины, что координируется операционной системой в соответствии с заданной дисциплиной обслуживания;
- реального времени, обеспечивающих определенное гарантированное время ответа машины на запрос пользователя с управлением им какими-либо внешними но отношению к ЭВМ событиями, процессами или объектами.

В соответствии с седьмым признаком классификации ОС делятся на сетевые и локальные. Сетевые ОС предназначены для управления ресурсами компьютеров, объединенных в сеть с целью совместного использования данных, и предоставляют мощные средства разграничения доступа к данным в рамках обеспечения их целостности и сохранности, а также множество сервисных возможностей по использованию сетевых ресурсов.

В большинстве случаев сетевые операционные системы устанавливаются на один или более достаточно мощных компьютеров-серверов, выделяемых исключительно для обслуживания сети и совместно используемых ресурсов. Все остальные ОС будут считаться локальными и могут использоваться на любом персональном компьютере, а

также на отдельном компьютере, подключенном к сети в качестве рабочей станции или клиента.

В настоящее время распространены следующие семейства операционных систем: DOS; OS/2; UNIX; Windows; ОС реального времени.

Основные критерии подхода к выбору операционной системы:

В настоящее время имеется большое количество операционных систем, и перед пользователем стоит задача определить, какая операционная система лучше других (по тем или иным критериям). Очевидно, что идеальных систем не бывает, любая из них имеет свои достоинства и недостатки. Выбирая операционную систему, пользователь должен представлять, насколько та или иная ОС обеспечит ему решение его задач.

Чтобы выбрать ту или иную ОС, необходимо знать:

- на каких аппаратных платформах и с какой скоростью работает ОС;
- какое периферийное аппаратное обеспечение ОС поддерживает;
- как полно удовлетворяет ОС потребности пользователя, то есть каковы функции системы;
- каков способ взаимодействия ОС с пользователем, то есть насколько нагляден, удобен, понятен и привычен пользователю интерфейс;
- существуют ли информативные подсказки, встроенные справочники и т. д.;
- какова надежность системы, то есть ее устойчивость к ошибкам пользователя, отказам оборудования и т. д.;
- какие возможности предоставляет ОС для организации сетей;
- обеспечивает ли ОС совместимость с другими операционными системами;
- какие инструментальные средства имеет ОС для разработки прикладных программ;
- осуществляется ли в ОС поддержка различных национальных языков;
- какие известные пакеты прикладных программ можно использовать при работе с данной системой;
- как осуществляется в ОС защита информации и самой системы.

1 Общая характеристика ОС Windows, UNIX.

ОС UNIX является удачной реализацией многопользовательской и многозадачной ОС. Она спроектирована как инструменталь-ная система для разработки программного обеспечения. Система UNIX обладает простым, но очень мощным командным языком и независимой от устройств файловой системой. Системы и приложения, выполняющиеся в ней, легко переносимы.

При создании ОС UNIX имелось три цели:

1.) стремление сохранить простоту и обойтись минимальным количеством функций.

2.) использование общих механизмов во множестве случаев, например при обраще-нии к файлам, прерываниях, именовании и др.;

3.) предоставление возможности решать большие задачи, комбинируя более мелкие.

Процесс может выполняться в одном из двух состояний – пользовательском или систем-ном.

В пользовательском состоянии процесс выполняет пользовательскую программу и имеет доступ к пользовательскому сегменту данных.

В системном состоянии процесс выполняет программы ядра и имеет доступ к системному сегменту данных.

В UNIX-системах используется разделение времени, то есть каждому процессу выделяется квант времени. Процесс либо завершается сам до истечения отведенного ему кванта времени, либо он откладывается по истечении кванта. Чем меньше отведенное процессу время – тем выше его приоритет. Все системные процессы имеют более высокие приоритеты по сравнению с пользовательскими и поэтому всегда обслуживаются в первую очередь.

Linux – это современная POSIX-совмести-мая и UNIX-подобная ОС для ПК и рабочих станций.
Изначально Linux создавался как самодель-ная UNIX-подобная реализация для ПК типа IBM PC с процессором i80386. Однако Linux стал настолько популярен и его на сегодня-шний день поддерживает такое большое число компаний, что в настоящее время имеется реализация этой ОС практически для всех типов процессоров и компьютеров на их основе.
Ядро Linux сразу было создано с учетом возможностей защищенного режима процессоров Intel 80386 и 80486. В частно-сти, Linux использует парадигму описания памяти в защищенном режиме и другие новые свойства процессоров. В настоящее время имеются ядра для этой системы, оптимизированные для работы с процесс-сорами Intel и AMD последнего поколения, хотя основные архитектурные особенности защищенного режима работы изменились мало.

1. 4 Лекция № 4 (2 часа).

Тема: «Домены Windows NT. Локальная политика безопасности».

1.4.1 Вопросы лекции:

1. Домены Windows NT.
2. Локальная политика безопасности.

1.4.2 Краткое содержание вопросов:

1. Домены Windows NT.

Домен - это основная единица администрирования и обеспечения безопасности в Windows NT. Для домена существует общая база данных учетной информации пользователей домена (user accounts) и ресурсов домена - компьютеров (computer accounts) и принтеров (printer accounts). Пользователь домена выполняет один логический вход в домен и получает доступ сразу ко всем разрешенным ресурсам этого домена.

Членами домена являются как пользователи, так и компьютеры. При отсутствии доменной организации каждый компьютер Windows NT Workstation и Windows NT Server хранит собственную базу учетных данных пользователей - SAM (Security Access Manager). В этой базе хранится вся необходимая системе информация о пользователе - имя, пароль (в зашифрованном виде) и так называемый SID - Security Identifier. Идентификатор SID играет ключевую роль в процессе предоставления пользователю доступа к защищенным

ресурсам системы - файлам, принтерам и т.п. В списке прав доступа ресурса ACL хранится информация о конкретных номерах SID, которым разрешен тот или иной вид доступа. Каждый SID является уникальным числом. При изменении имени пользователя его SID не изменяется.

Компьютер домена также характеризуется именем и идентификатором SID, между которыми имеется такое же соотношение, как и между именем и идентификатором SID пользователя.

В домене обязательно есть сервер Windows NT Server, выполняющий роль первичного контроллера домена - Primary Domain Controller, PDC. Этот контроллер хранит первичную копию базы данных учетной информации пользователей домена - SAM PD. Все изменения учетной информации сначала производятся именно в этой копии. Основной контроллер домена всегда существует в единственном экземпляре.

Кроме основного контроллера, в домене могут существовать несколько резервных контроллеров - Backup Domain Controllers, BDC. Эти контроллеры хранят реплики базы учетных данных. Все резервные контроллеры в дополнение к основному могут обрабатывать запросы пользователей на логический вход в домен. База данных SAM BD всегда является копией (с точностью до интервала синхронизации) базы SAM PD.

Резервный контроллер домена решает две задачи:

1. Он становится основным контроллером при отказе последнего.
2. Уменьшает нагрузку на основной контроллер по обработке запросов на логический вход пользователей.

Если сеть состоит из нескольких сетей, соединенных глобальными связями, то в каждой из составляющих сетей должен быть по крайней мере один резервный контроллер домена.

Членами домена могут быть также компьютеры, на которых установлены Windows NT Server, не назначенные на роль PDC или BDC. Такие серверы называются *отдельно стоящими серверами (Stand-alone servers)* или серверами - членами доменами *(Member servers)*. На таких компьютерах, освобожденных от функций аутентификации пользователей и ведения справочной базы данных, могут более производительно выполняться ответственные приложения или файл- и принт-сервисы. Stand-alone серверы не могут быть оперативно переконфигурированы в PDC или BDC, для этого требуется переинсталляция.

Рабочая станция Windows NT Workstation и сервер Windows NT Server, не выполняющий роль PDC или BDC, могут динамически изменять свое членство в домене, а серверы PDC и BDC - только при инсталляции системы. Поэтому при инсталляции очень важно правильно выбрать принадлежность компьютера, назначенного на роль контроллера домена, тому или иному домену.

2.Локальная политика безопасности.

Локальная политика безопасности – это оснастка консоли управления, позволяющая устанавливать различные системные параметры безопасности. Данная оснастка также является частью групповой политики.

Для запуска этой оснастки откройте Панель управления, в категории Система и безопасность щелкните на ссылке Администрирование, после этого дважды щелкните на

значке Локальная политика безопасности и подтвердите ваши действия в окне UAC (если оно появится)
Наиболее актуальные параметры безопасности собраны в разделе Локальные политики.
• Политика аудита. Здесь вы можете определить, какие события будут записываться в журнал безопасности. Для включения аудита дважды щелкните на нужном событии и в появившемся окне установите нужные флажки: Успех – для занесения в журнал удачных попыток, Отказ – для фиксации неудачных попыток выбранного действия.
• Назначение прав пользователя. В этой категории имеется довольно обширный список параметров, определяющих, что можно и что нельзя делать на компьютере отдельным пользователям и группам. Например, вы можете указать, каким пользователям разрешить локальный вход, а каким – доступ по сети, кто может выполнять завершение работы или изменять системное время.
• Параметры безопасности. Здесь собраны различные административные параметры, определяющие поведение системы при входе в нее, доступе к компьютеру из сети, работе с устройствами и др.

1. 5 Лекция № 5 (2 часа).

Тема: «Управление ресурсами».

1.5.1 Вопросы лекции:

1.Управление процессорами.
2.Управление памятью.

1.5.2 Краткое содержание вопросов:

1.Управление процессорами.
.

Основные задачи управления процессором сводятся к решению двух взаимосвязанных проблем:
 Создание условий, при которых каждый процесс и приложение получат достаточную часть рабочего времени процессора, чтобы обеспечивалось их нормальное функционирование

 Использование стольких циклов процессора, сколько возможно для нормальной работы.

Основной единицей программного обеспечения, с которой операционная система работает при планировании работы процессора, является либо процесс, либо поток, в зависимости от операционной системы.

Было бы заманчиво рассматривать процесс как приложение, однако такой подход дает неполную картину того, какая устанавливается взаимосвязь процессов с операционной системой и аппаратными средствами. Видимое пользователем приложение (текстовый редактор, электронная таблица или игра) действительно является процессом, однако это приложение может инициировать запуск некоторых других процессов для решения таких задач, как связь с другими устройствами или компьютерами. Имеется также большое число процессов, которые протекают, не проявляя себя. Например, в Windows XP и UNIX могут быть десятки фоновых процессов, предназначенных для управления сетью, памятью и дисками, проверки на наличие вирусов и т.д.

Таким образом, процесс – это программа, выполняющая определенное действие, и которой можно управлять – силами пользователя, с помощью других приложений или с помощью операционной системы.

Операционная система осуществляет контроль и планирует выполнение центральным процессором процессов, а не приложений. В однозадачной системе планирование выполнения простое. Операционная система разрешает приложению запуститься, временно приостанавливая его выполнение на достаточно длительное время лишь в случае необходимости обслуживания прерываний и пользовательского ввода данных.

Прерывания – специальные сигналы, отправляемые на центральный процессор аппаратными средствами или программами. Это похоже на то, как если бы во время оживленного собрания какая-то часть компьютера вдруг подняла руку, требуя к себе внимания центрального процессора. Иногда операционная система устанавливает приоритеты процессов таким образом, что прерывания маскируются, то есть операционная система игнорирует прерывания от некоторых источников, чтобы определенная операция была завершена как можно скорее. Существуют некоторые прерывания (например, вызванные состоянием ошибки или проблемами с памятью), которые настолько важны, что их нельзя игнорировать. Эти немаскируемые прерывания (non-maskable interrupts, NMIs) требуют немедленного решения проблемы, несмотря на то, что должны выполняться другие задачи.

Учитывая, что прерывания создают определенные сложности при выполнении процессов даже в однозадачной системе, функционирование операционной системы становится намного более сложным в многозадачной системе. В последнем случае операционная система должна организовать выполнение приложений таким образом, чтобы создавалось впечатление, что определенные события происходят одновременно. Это сложно осуществить, поскольку центральный процессор в каждый момент времени может делать только одну операцию. Современные многоядерные процессоры и многопроцессорные компьютеры могут выполнять по нескольку операций одновременно, однако каждое ядро процессора, как и прежде, в каждый момент времени может делать только одну операцию.

Чтобы создавалось впечатление, что множество событий происходит одновременно, операционная система должна осуществлять переключение между разными процессами тысячи раз в секунду. Это делается следующим образом:

 Процесс занимает определенную часть оперативной памяти. Кроме того, он использует регистры, стеки и очереди в центральном процессоре, а также в пространстве памяти операционной системы.

 Допустим, имеется два многозадачных процесса. Операционная система выделяет на каждую программу по определенному количеству исполнительных циклов.

 После прохождения этого количества циклов операционная система делает копии всех регистров, стеков и очередей, использовавшихся в процессах, и отмечает место, на котором наступила пауза выполнения процесса.

 Затем производится загрузка всех регистров, стеков и очередей, используемых вторым процессом, и этому процессу разрешается прохождение определенного количества циклов

центрального компьютера.

 По завершении этих циклов делаются копии всех регистров, стеков и очередей, использовавшихся второй программой, и производится загрузка первой программы.

2. Управление памятью.

Основная (или как ее принято называть в отечественной литературе и документации, оперативная) память всегда была и остается до сих пор наиболее критическим ресурсом компьютеров. Если учесть, что большинство современных компьютеров обеспечивает 32-разрядную адресацию в пользовательских программах, и все большую силу набирает новое поколение 64-разрядных компьютеров, то становится понятным, что практически безнадежно рассчитывать, что когда-нибудь удастся оснастить компьютеры основной памятью такого объема, чтобы ее хватило для выполнения произвольной пользовательской программы, не говоря уже об обеспечении мультипрограммного режима, когда в основной памяти, вообще говоря, могут одновременно содержаться несколько пользовательских программ.

Поэтому всегда первичной функцией всех операционных систем (более точно, операционных систем, обеспечивающих режим мультипрограммирования) было обеспечение разделения основной памяти между конкурирующими пользовательскими процессами. Мы не будем здесь слишком сильно вдаваться в историю этого вопроса. Заметим лишь, что применявшаяся техника распространяется от статического распределения памяти (каждый процесс пользователя должен полностью поместиться в основной памяти, и система принимает к обслуживанию дополнительные пользовательские процессы до тех пор, пока все они одновременно помещаются в основной памяти), с промежуточным решением в виде "простого своппинга" (система по-прежнему располагает каждый процесс в основной памяти целиком, но иногда на основании некоторого критерия целиком сбрасывает образ некоторого процесса из основной памяти во внешнюю память и заменяет его в основной памяти образом некоторого другого процесса), до смешанных стратегий, основанных на использовании "страничной подкачки по требованию" и развитых механизмов своппинга.

Операционная система UNIX начинала свое существование с применения очень простых методов управления памятью (простой своппинг), но в современных вариантах системы для управления памятью применяется весьма изощренная техника.

Поэтому в таких случаях используется техника копирования страниц при попытке записи. Несмотря на то, что в сегмент запись разрешена, для каждой его страницы устанавливается блокировка записи. Тем самым, во время попытки выполнения записи возникает прерывание, и ОС на основе анализа статуса соответствующего сегмента принимает решение о выделении новой страницы, копировании на нее содержимого оригинальной страницы и о включении этой новой страницы на место старой в виртуальную память либо процесса-предка, либо процесса-потомка (в зависимости от того, кто из них пытался писать).

На этом мы заканчиваем краткое описание механизма управления виртуальной памятью в ОС UNIX. Еще раз подчеркнем, что мы опустили множество важных технических деталей, стремясь продемонстрировать наиболее важные принципиальные решения.

1. 6 Лекция № 6 (2 часа).

Тема: «Доменная политика конфигураций безопасности. Конфигурирование безопасности в Windows NT».

1.6.1 Вопросы лекции:

1. Доменная политика конфигураций безопасности.
2. Основы безопасности в Windows NT

1.6.2 Краткое содержание вопросов:

1. Доменная политика конфигураций безопасности.

Подробные политики паролей можно использовать для определения нескольких политик паролей в одном домене. С помощью подробных политик паролей можно применять различные ограничения политик паролей и блокировки учетных записей к разным группам пользователей в домене.
Например, можно применить более строгие параметры к привилегированным учетным записям и менее строгие – к учетным записям других пользователей. Может также возникнуть необходимость применения особой политики паролей к тем учетным записям, пароли которых синхронизируются с другими источниками данных.

Подробные политики паролей применимы только к объектам пользователей (или объектам inetOrgPerson, если они используются вместо объектов пользователей) и глобальным группам безопасности. По умолчанию задавать подробные политики паролей могут только члены группы администраторов домена. Однако возможность задавать эти политики можно также делегировать другим пользователям. Домен должен работать в режиме Windows Server 2008.
Подробную политику паролей нельзя применить непосредственно к подразделению. Для применения подробной политики паролей к пользователям из подразделения можно использовать теневую группу.
Теневая группа – это глобальная группа безопасности, которая логически сопоставляется с подразделением для принудительного применения подробной политики паролей. После добавления пользователей подразделения в созданную теневую группу к ней можно применить подробную политику паролей. Для других подразделений можно по мере необходимости создавать дополнительные теневые группы. При перемещении пользователя из одного подразделения в другое необходимо обновлять его членство в соответствующих теневых группах.
В одном домене допускается использование подробных политик паролей одновременно с настраиваемыми фильтрами паролей. Если на контроллерах домена с Windows 2000 или Windows Server 2003 развернуты настраиваемые фильтры паролей, их можно использовать и в дальнейшем в целях обеспечения дополнительных ограничений для паролей.

Объекту пользователя или группы может быть привязано несколько объектов параметров паролей. Такая ситуация имеет место в случае, если этот объект является членом нескольких групп, к которым привязаны различные объекты параметров паролей, либо в случае, когда несколько объектов параметров паролей привязаны к этому объекту напрямую. Однако только один объект параметров паролей может быть применен в качестве действующей политики паролей. Только параметры этого объекта параметров паролей будут оказывать влияние на пользователя или группу. Слияние с параметрами других объектов параметров паролей, привязанных к этому пользователю или группе, невозможно.
Результирующая политика может быть определена только для объекта пользователя. Объект параметров паролей может быть применен к объекту пользователя двумя способами, указанными ниже.

1. Непосредственно: объект параметров паролей связывается с пользователем.

2. Косвенно: объект параметров паролей связывается с группами, членом которых является пользователь.

По умолчанию объекты параметров паролей могут создавать только члены группы администраторов домена. Только члены этой группы имеют разрешения "Создать дочерний" и "Удалить дочерний" на объект контейнера параметров паролей. Кроме того, только члены группы "Администраторы домена" по умолчанию имеют разрешение "Записать свойство" на объект параметров паролей. Поэтому только члены данной группы могут привязать объект параметров паролей к группе или пользователю. Это разрешение можно делегировать другим группам или пользователям.
Чтобы применить объект параметров паролей к объекту пользователя или группы, разрешения на работу с ними не требуются. Разрешения на запись объекта пользователя или группы не позволяют связать объект параметров паролей с пользователем или группой. Владелец группы не имеет разрешений на связывание объекта параметров паролей с группой, поскольку прямая ссылка содержится в объекте параметров паролей. Возможность связывания объекта параметров паролей с группой или пользователем имеется у владельца объекта параметров паролей.
Параметры объекта параметров паролей можно считать конфиденциальными; таким образом, по умолчанию пользователи, прошедшие проверку подлинности, не имеют разрешений "Чтение свойства" для объекта параметров паролей. По умолчанию только члены группы администраторов домена имеют эти разрешения для используемого по умолчанию дескриптора безопасности объекта параметров паролей в схеме.

2. Основы безопасности в Windows NT

Модель безопасности Windows NT базируется на концепции пользовательских бюджетов (user accounts). Можно создать неограниченное количество пользовательских бюджетов и сгруппировать их наиболее удобным методом. После этого для каждого бюджета или группы можно представить или ограничить доступ к любому из ресурсов компьютера.

В операционную систему Windows NT встроена возможность аудита. Это позволяет отслеживать, какие пользовательские бюджеты использовались для доступа в систему, и какого типа доступ к файлам и другим объектам был получен пользователями. Кроме того, аудит может использоваться для отслеживания попыток входа в систему, остановки и перезапуска системы и прочих аналогичных событий.

Модель безопасности Windows NT содержит следующие компоненты:

- Процессы входа в систему (Logon processes), принимающие от пользователей на регистрацию в системе. Сюда относятся начальный интерактивный процесс регистрации, отображающий диалоговое окно входа в систему, и процесс удаленной регистрации, позволяющий удаленным пользователям получить доступ к серверу Windows NT.

- Распорядитель локальной безопасности (Local Security Authority, LSA), гарантирующий, что каждый пользователь, регистрирующийся в системе, имеет право доступа к ней. Этот компонент является центральным для всей подсистемы безопасности Windows NT. Он создает маркеры безопасного доступа, управляет локальной политикой безопасности и обеспечивает интерактивный сервис аутентификации пользователей. Кроме того, LSA управляет политикой аудита и регистрирует сообщения аудита, генерируемые монитором безопасности (Security Reference Monitor).

- Диспетчер бюджетов безопасности (Security Accounts Monitor, SAM). Этот компонент поддерживает базу данных пользовательских бюджетов. База данных SAM содержит информацию обо всех пользовательских и групповых бюджетах. SAM обеспечивает сервис валидизации пользовательских паролей, используемый LSA. База данных SAM известна также под названием базы данных каталога (Directory Database).

- Монитор безопасности (Security Reference Monitor) - компонент системы безопасности, ответственный за проверку наличия у пользователей прав доступа к объектам и осуществления действий, которые они пытаются выполнить. Монитор безопасности принудительным образом устанавливает проверку прав доступа к объектам и устанавливает политику аудита заданную LSA. Монитор безопасности предоставляет сервис процессам, которые работают как в режиме ядра, так и в режиме пользователя. Это гарантирует, что все пользователи и процессы, пытающиеся получить доступ к объекту и выполнить над ним некоторые действия, обладают соответствующими правами доступа. Кроме того, монитор безопасности генерирует сообщения аудита в тех случаях, когда это необходимо.

Ключевой особенностью системы безопасности Windows NT является управление доступом к объектам. Модель безопасности поддерживает информацию защиты для каждого пользователя, группы и объекта. Она может идентифицировать попытки доступа, осуществленные непосредственно пользователем, а также способна выявлять непрямые попытки доступа, предпринятые не самим пользователем, а программой или иным процессом, действующими от лица пользователя. Windows NT отслеживает все попытки доступа и позволяет управлять доступом как к объектам, которые пользователи могут просматривать с помощью пользовательского интерфейса (например, файлам и принтерам), так и к абстрактным объектам, которые с помощью пользовательского интерфейса просмотреть нельзя (к ним относятся, например, процессы и именованные каналы).

Администратор системы присваивает пользователям и группам права доступа (permissions), с помощью которых можно предоставить или отклонить пользовательский доступ к объектам. Возможность избирательного присвоения прав доступа по усмотрению владельца объекта (или пользователя, уполномоченного изменять права доступа), называется избирательным контролем доступа (discretionary access control).

Система безопасности идентифицирует пользователей с помощью идентификатора безопасности (security ID, SID). Уникальность идентификаторов безопасности гарантирована, и существование двух идентичных SID полностью исключено. Когда пользователь регистрируется в системе, Windows NT создает маркер безопасности доступа (security access token). В состав маркера безопасного доступа входят SID пользователя, SID всех групп, к которым этот пользователь принадлежит, а также дополнительная информация о пользователе и его группах. Кроме того, любой процесс, работающий от имени пользователя, получает копию его маркера безопасного доступа. Когда пользователь пытается получить доступ к объекту, Windows NT ссылается на содержащийся в маркере безопасного доступа SID. Идентификаторы безопасности (SID) сравниваются со списком контроля доступа к объекту, чтобы гарантировать, что пользователь имеет достаточные права.

Диапазон средств защиты файлов можно установить как на базе подхода "по файлам", так и на базе подхода "по каталогам". Чтобы воспользоваться всей властью над отдельными файлами, их следует расположить на томах с NTFS. Windows NT поддерживает для совместимости с MS DOS работу с FAT, но эта файловая система была разработана без

учета требований безопасности. Чтобы воспользоваться всеми преимуществами защиты Windows NT, необходимо использовать файловую систему NTFS.

Системные принтеры можно защитить, не позволяя конкретным пользователям отправлять на них задания (постоянно или только в течение указанного времени суток).

1. 7 Лекция № 7 (2 часа).

Тема: «Управление программами».

1.7.1 Вопросы лекции:

1.Понятие программы.
2.Виртуальные программы.

1.7.2 Краткое содержание вопросов:

1.Понятие программы.

Компьютерная программа — это последовательность инструкций, которая предназначена для исполнения вычислительной машиной. Образ программы, чаще всего, хранится в памяти машины (например, на *диске*) как исполняемый модуль (один или несколько файлов). Из образа на диске с помощью специального программного загрузчика может быть построена исполняемая программа уже в оперативной памяти машины.

Термин «*компьютерная программа*» в зависимости от своего контекста, может применяться также к *исходным текстам* (или кодам) программы. Их примеры могут быть просмотрены в специальных каталогах исходников. Вместе с правилами и процедурами, а также с документацией по функционированию программных систем обработки данных, компьютерные программы составляют понятие программного обеспечения.

В системном программировании имеет место более формальное определение *программы* как машинных кодов и данных, загруженных в оперативную память компьютера, и исполняемых процессором машины для достижения поставленной цели. В этом определении подчеркиваются две особенности компьютерной программы: нахождение ее в памяти и исполнение процессором машины.

Процесс создания компьютерной программы называется «программированием», а люди, занимающиеся этим видом деятельности, называются программистами. При разработке компьютерных программ в них довольно часто возникают ошибки. Считается, что в программе содержатся ошибки, если для каких-то данных программа дает неправильные результаты, сбои или отказы. Если программа выдает правильные результаты обработки для всех возможных входных данных, то можно считать, что она не содержит ошибок.

Процесс поиска ошибок в программах и их исправления называется отладкой программ. Обычно, заранее неизвестно, сколько ошибок содержит программа. По этой причине заранее неизвестна и продолжительность отладки программ.

Запись исходных текстов компьютерных программ при помощи специальных *языков программирования* (*ЯП*) облегчает человеку понимание и редактирование программ. Этому, также, помогают *комментарии*, допускаемые синтаксисом большинства языков программирования. Для выполнения программы на компьютере ее готовый исходный

текст преобразуется (*компилируется* или *интерпретируется*) в *машинный код*, исполняемый процессором.

Программы с исходными текстами, доступными для прочтения и изменения любым желающим, называются открытыми программами. Любая компьютерная программа является объектом авторского права. Авторы или собственники программ имеют право ограничивать и даже полностью закрывать доступ к их исходным текстам, которые являются интеллектуальной собственностью правообладателей.

Некоторые языки программирования (интерпретируемые) позволяют обойтись без предварительной компиляции написанных на них программ, и специальные *программы-интерпретаторы*переводят такие программы в машинный код уже во время исполнения программы. Этот процесс называется интерпретированием или динамической компиляцией. Он позволяет улучшить переносимость программ между различными программными и аппаратными платформами. Интерпретируемые программы часто называются сценариями или скриптами.

В большинстве распространенных ЯП исходные тексты программ состоят из списков инструкций, описывающих заложенный в программе алгоритм. Такой подход называется императивным. Но применяются и иные методологии программирования. Так, например, в декларативном программировании описываются исходные и требуемые характеристики обрабатываемых данных, а выбор подходящего алгоритма решения описанной задачи поручается специализированной программе-интерпретатору. Применяются также *логическое* и *функциональное* программирование.

2. Виртуальные программы.

Иногда возникает необходимость получить второй компьютер, на котором можно установить другую операционную систему или безопасно протестировать программы. С этой задачей Вам поможет справиться виртуальная машина.

Виртуальная машина – программа, которая эмулирует реальный (физический) компьютер со всем его компонентами (жёсткий диск, привод, BIOS, сетевые адаптеры и т.д.). На такой виртуальный компьютер можно установить операционную систему, драйверы, программы и т.д. Таким образом, Вы можете запустить на своем реальном компьютере еще несколько виртуальных компьютеров, с такой же или другой операционной системой. Вы можете без проблем осуществить обмен данными между Вашим реальным и виртуальным компьютером.

Зачем нужна виртуальная машина

Не каждому пользователя ПК нужна виртуальная машина, но продвинутые пользователи довольно часто используют ее. Виртуальную машину используют для различных целей и задач:
Установка второй/другой операционной системы;
Тестирование программного обеспечения;
Безопасный запуск подозрительных программ;
Эмуляция компьютерной сети;
Запуск приложений, которые нельзя запустить из Вашей операционной системы.
На Вашем реальном компьютер может быть установлена операционная система Windows 7, а на виртуальную машину можно поставить Windows XP, Windows 8 или Linux.

Если Вам нужно выбрать программу (например, видео плеер) Вам нужно установить несколько подобных программ, и определить какая из них Вам больше нравится. Что бы ни захламлять Ваш компьютер, протестируйте программы на виртуальной машине.

Обзор виртуальных машин
Существует большое количество различных программ для создания и управления виртуальными компьютерами. Сейчас мы рассмотрим 3 самые популярные программы.
Виртуальная машина VirtualBox

VirtualBox – бесплатная виртуальная машина, на которую можно установить все самые популярные операционные системы. VirtualBox поддерживает работу с Windows, Linux, FreeBSD, Mac OS.

Виртуальная машина VMware

VMware – наиболее известная и распространенная виртуальная машина. VMware как правило используют для работы крупные площадки или корпорации.
VMware поставляется в двух видах: Workstation и Player. VMware Workstation отличная, но платная виртуальная машина. VMware Player – бесплатная урезанная версия VMware Workstation.

1. 8 Лекция № 8 (2 часа).

Тема: «Разработка защищенных приложений. Программное управление учетной записью».

1.8.1 Вопросы лекции:

1. Методы разработки защищенных приложений.
2. Области применения.

1.8.2 Краткое описание проводимого занятия:

1. Методы разработки защищенных приложений.

Основная часть уязвимостей появляется на ранних стадиях создания программного обеспечения. Поэтому, наибольшей эффективностью обладает подход, который устраняет проблемы безопасности на начальной стадии разработки приложений, нежели стандартный метод их исправления по необходимости. Консультанты моделируют потенциальные угрозы безопасности еще до создания программного продукта, что позволяет закрыть всевозможные бреши на стадии его разработки.

Глубокие знания процесса разработки прикладных приложений, позволяют им устранять существующие бреши в программном обеспечении, а также избежать потенциальных уязвимостей при создании собственного продукта.

Специалисты регулярно проводят проверку безопасности:

- сайтов интернет торговли, банков, финансовых и других учреждений;
- программного продукта для разработчиков, интернет-порталов и настольных систем.

Наша компания предлагает полный объем услуг по обеспечению информационной безопасности бизнес проектов, включая:

- оценка уязвимости встроенных систем;

- устранение брешей в системе предварительно записанных голосовых сообщений IVR;
- обнаружение «дыр» в настольных и мобильных приложениях, оценка величины рисков, практические рекомендации по их снижению;
- моделирование потенциальных угроз безопасности приложений, а также обнаружение и устранение их на ранней стадии разработки;
- определение уязвимостей, рисков, прочих угроз безопасности в инфраструктуре веб-подразделений организации;
- повышения уровня безопасности установленных приложений, проверка скриптов и исходного программного кода, устранение выявленных ошибок;
- оценка потенциальных способов проникновения хакеров в веб-приложение, обнаружение уязвимостей рабочих версий веб-порталов, определение степени коммерческих рисков и проведение консультаций по их снижению.

2. Области применения.

Как правило, при развертывании Web-приложения прежде всего требуется обеспечить, чтобы анонимные клиенты не могли обращаться к ценным ресурсам через интернет. Если приложение работает в интрасети, то для аутентификации клиентов обычно применяются средства Windows (подробнее об управлении доступом я расскажу чуть позже), а приложение защищается от внешнего доступа межсетевым экраном (брандмауэром). С интернет-приложениями дело обстоит сложнее, поскольку нужен хотя бы минимальный уровень доступа для анонимных пользователей, обращающихся через интернет. Если не принимать в расчет эти различия, можно руководствоваться следующими принципами, в равной мере применимыми к защите интернет-приложений и приложений интрасети. Идеальный вариант — в Web-пространстве имен вашего приложения не должно быть никаких файлов, которые не планируется передавать клиентам. То есть все такие файлы надо удалить из физической структуры каталогов, начинающейся с самого верхнего каталога, помеченного в конфигурации IIS как Web-приложение или виртуальный каталог. Если файл не принадлежит Web-пространству имен, он не будет доступен при запросах к этому пространству, если только ваше приложение не выполнит явные операции по открытию этого файла и передаче его содержимого. Если ваше приложение программно обращается к данным или вспомогательным файлам, размещайте их вне Web-пространства имен.

Сферы применения:

- Установление защищенного удаленного доступа к внутренним информационным ресурсам организации: электронной почте, календарям сотрудников, адресной книге организации, внутренним порталам, библиотекам файлов и документов, системам управления совещаниями, спискам задач и др.
- Обеспечение юридически значимого электронного документооборота с применением сертифицированных средств криптографической защиты информации.
- Взаимодействие с площадками электронных торгов и аукционов, b2b услуг, госуслуг.
- Обеспечение конфиденциальности электронных почтовых сообщений.
- Обеспечение конфиденциальности информации, хранимой на мобильном устройстве.

1. 9 Лекция № 9 (1 час).

Тема: «Управление процессами».

1.9.1 Вопросы лекции:

1.Понятия процесса и потока.
2.Состояния процессов.

1.9.2 Краткое содержание вопросов:

1.Понятия процесса и потока.

Термин «процесс» впервые появился при разработке операционной системы Multix и имеет несколько определений, которые используются в зависимости от контекста, согласно которым **процесс** — это:

1. программа на стадии выполнения
2. «объект», которому выделено процессорное время
3. асинхронная работа

Для описания состояний процессов используется несколько моделей. Самая простая — модель трех состояний. Она определяет следующие состояния процесса:

1. состояния выполнения
2. состояния ожидания
3. состояния готовности

Выполнение — это *активное состояние*, во время которого процесс обладает всеми необходимыми ему ресурсами. В этом состоянии процесс непосредственно выполняется процессором.

Ожидание — это *пассивное состояние*, во время которого процесс заблокирован и не может быть выполнен, потому что ожидает какое-то событие, например, ввода данных или освобождения нужного ему устройства.

Готовность — это тоже пассивное состояние, процесс тоже заблокирован, но в отличие от состояния ожидания, он заблокирован не по внутренним причинам (ведь ожидание ввода данных — это внутренняя, «личная» проблема процесса — он может ведь и не ожидать ввода данных и свободно выполняться — никто ему не мешает), а по внешним, независящим от процесса, причинам.

Потоки

Концепция процесса, пришедшая из мира UNIX, плохо реализуется в многозадачной системе, поскольку процесс имеет тяжелый контекст. Возникает понятие **потока (thread)**, который понимается как подпроцесс, или *легковесный процесс (light-weight process)*, выполняющийся в контексте полноценного процесса.

С помощью процессов можно организовать параллельное выполнение программ. Для этого процессы клонируются вызовами fork() или exec(), а затем между ними организуется взаимодействие средствами IPC. Это довольно дорогостоящий в отношении ресурсов способ.

С другой стороны, для организации параллельного выполнения и взаимодействия процессов можно использовать механизм многопоточности. Основной единицей здесь является **поток**, который представляет собой облегченную версию процесса. Чтобы понять, в чем состоит его особенность, необходимо вспомнить основные характеристики процесса.

1. Процесс располагает определенными ресурсами. Он размещен в некотором виртуальном адресном пространстве, содержащем образ этого процесса. Кроме того, процесс управляет другими ресурсами (файлы, устройства ввода/вывода и т.д.).
2. Процесс подвержен диспетчеризации. Он определяет порядок выполнения одной или нескольких программ, при этом выполнение может перекрываться другими процессами. Каждый процесс имеет состояние выполнения и приоритет диспетчеризации.

Если рассматривать эти характеристики независимо друг от друга (как это принято в современной теории ОС), то:

- владельцу ресурса, обычно называемому процессом или задачей, присущи:
  - виртуальное адресное пространство;
  - индивидуальный доступ к процессору, другим процессам, файлам, и ресурсам ввода — вывода.
- Модулю для диспетчеризации, обычно называемому потоком или облегченным процессом, присущи:
  - состояние выполнения (активное, готовность и т.д.);
  - сохранение контекста потока в неактивном состоянии;
  - стек выполнения и некоторая статическая память для локальных переменных;
  - доступ к пространству памяти и ресурсам своего процесса.

Все потоки процесса разделяют общие ресурсы. Изменения, вызванные одним потоком, становятся немедленно доступны другим.

При корректной реализации потоки имеют определенные преимущества перед процессами. Им требуется:

- меньше времени для создания нового потока, поскольку создаваемый поток использует адресное пространство текущего процесса;
- меньше времени для завершения потока;
- меньше времени для переключения между двумя потоками в пределах процесса;
- меньше коммуникационных расходов, поскольку потоки разделяют все ресурсы, и в частности адресное пространство. Данные, продуцируемые одним из потоков, немедленно становятся доступными всем другим потокам.

.

2.Состояния процессов

Состояние процессов

В многозадачной (многопроцессной) системе процесс может находиться в одном из трех основных состояний:

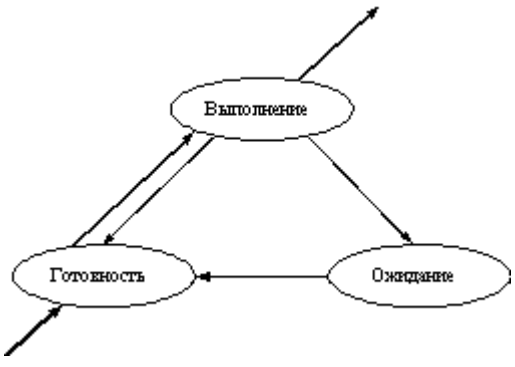
ВЫПОЛНЕНИЕ - активное состояние процесса, во время которого процесс обладает всеми необходимыми ресурсами и непосредственно выполняется процессором;

ОЖИДАНИЕ - пассивное состояние процесса, процесс заблокирован, он не может выполняться по своим внутренним причинам, он ждет осуществления некоторого события, например, завершения операции ввода-вывода, получения сообщения от другого процесса, освобождения какого-либо необходимого ему ресурса;

ГОТОВНОСТЬ - также пассивное состояние процесса, но в этом случае процесс заблокирован в связи с внешними по отношению к нему обстоятельствами: процесс имеет все требуемые для него ресурсы, он готов выполняться, однако процессор занят выполнением другого процесса.

В ходе жизненного цикла каждый процесс переходит из одного состояния в другое в соответствии с алгоритмом планирования процессов, реализуемым в данной операционной системе. Типичный граф состояний процесса показан на рисунке 2.1.

В состоянии ВЫПОЛНЕНИЕ в однопроцессорной системе может находиться только один процесс, а в каждом из состояний ОЖИДАНИЕ и ГОТОВНОСТЬ - несколько процессов, эти процессы образуют очереди соответственно ожидающих и готовых процессов. Жизненный цикл процесса начинается с состояния ГОТОВНОСТЬ, когда процесс готов к выполнению и ждет своей очереди. При активизации процесс переходит в состояние ВЫПОЛНЕНИЕ и находится в нем до тех пор, пока либо он сам освободит процессор, перейдя в состояние ОЖИДАНИЯ какого-нибудь события, либо будет насильно "вытеснен" из процессора, например, вследствие исчерпания отведенного данному процессу кванта процессорного времени. В последнем случае процесс возвращается в состояние ГОТОВНОСТЬ. В это же состояние процесс переходит из состояния ОЖИДАНИЕ, после того, как ожидаемое событие произойдет.



1. 10 Лекция № 10 (1 час).

Тема: «Организация управления доступом и защиты ресурсов ОС».

1.10.1 Вопросы лекции:

1. Функции управления.
2. Планирование в организации.
3. Основы доступа.

1.10.2 Краткое содержание вопросов:

1.Функции управления.

Функции управления — это особые виды специализированной управленческой деятельности, выделившиеся в процессе разделения управленческого труда.
Любая функция управления реализуется в комплексе управленческих задач. Различие задач и функций проявляется втом, что **функции —** это повторяющийся вид деятельности организации, а **задачи** — это деятельность, преследующая достижение требуемых результатов в заданное время.

Функция целиком может выполняться одним подразделением, но это же подразделение, одно или совместно с другими, может выполнять и другую функцию.

Состав функций подразделений и их объем зависят от следующих условий:

- масштаба, структуры и уровня развития производства;
- размера организации, ее самостоятельности, места в сложившейся системе общественного разделения труда;
- связей компании с другими предприятиями и организациями;
- уровня технической оснащенности управления.

Функции управления должны обеспечить в организации руководство, управление и обслуживание хозяйственной деятельности.

Каждая функция характеризуется назначением, повторяемостью, однородностью содержания, спецификой необходимого для ее выполнения персонала.

Функции управления носят объективный характер, что определяется необходимостью самого процесса управления в условиях совместного труда людей.

Управленческие функции являются основой для определения структуры и численности аппарата управления.

Деятельность аппарата управления направлена на то, чтобы объединить все относительно обособленные, хотя и неразрывно связанные функции.

Существует различная классификация функций управления. Причем различия обусловлены, как правило, признаками, положенными в основу классификации.

Наиболее простым и доступным для понимания является деление функций управления на две группы:

- общие;
- специальные.

Общие функции управления были сформулированы А. Файолем в начале XX в. Они проявляются принципиально одинаково в управлении организацией в любой сфере деятельности.

Среди общих функций менеджмента главной считается **титрование.** Реализуя ее, предприниматель или менеджер:

- формулирует цели и задачи на предстоящий период;
- разрабатывает стратегию действий (стратегическое планирование);
- составляет необходимые планы и программы для их реализации (текущее планирование).

Практическое воплощение планов и программ берет на себя **организационная функция.** Она реализуется через создание самой организации, формирование ее структуры, распределения работы среди подразделений, сотрудников и координация их деятельности.

Мотивиционния функция заключается в определении потребностей людей, выборе наиболее подходящего и действенного в данной ситуации способа их удовлетворения с тем, чтобы обеспечить максимальную заинтересованность работников в процессе достижения целей, стоящих перед организацией.

Контроль призван заблаговременно выявлять надвигающиеся опасности, обнаруживать ошибки, отклонения от существующих стандартов и тем самым создавать основу для совершенствования работы.

2. Планирование в организации.

Плановая деятельность фирмы — одна из первоочередных функций ее управления, взаимодействующая с такими функциями, как: организация, координация, контроль, регулирование, стимулирование и анализ. **Планирование на фирме — экономический метод управления, представляет собой процесс проектирования желаемого будущего, а также эффективных путей его достижения. Задачи планирования** заключаются в выявление перспектив изменения внешнего окружения фирмы, формирование целей и стратегии развития, определение первоочередных задач и действий для их решения. А также определение необходимых затрат и результатов, проектирование изменения состояния предприятия, согласование работы всех его подразделений, контроль за выполнением плановых заданий всеми подразделениями фирмы, анализ достигнутых плановых результатов.

Фирма как участник рыночной системы вынуждено подчиняться ценовому механизму, закону спроса и предложения и т.д. Однако во внутренней среде каждой фирмы, предприятия механизм цен вытеснен сознательными действиями и автономными решениями менеджеров и предпринимателей. Менеджер сознательно определяет основные направления внутрифирменной деятельности. Следовательно, внутренняя природа фирмы основывается на системе плановых показателей.

Планирование является естественной частью менеджмента. С этой позиции планирование отвечает на три основных вопроса:

1. **Где находится фирма в настоящее время?** Определяется экономическая позиция фирмы, каковы итоги и условия ее деятельности. Оцениваются сильные и слабые стороны в таких важных областях, как финансы, маркетинг, производство, научные исследования, трудовые ресурсы для того, чтобы определить, чего может реально добиться фирма.
2. **Куда мы хотим двигаться?** Оценивая конкуренцию, клиентов, законы, политические факты, экономические условия, технологию, снабжение и т.д., руководство определяет, какими должны быть цели организации и что может помешать их достижению.
3. **Как, при помощи каких ресурсов** фирма собирается достичь своих целей? Определяются функции и обязанности сотрудников?

Отвечая на эти вопросы, процесс планирования включает в себя **три основных этапа:**

1. **Установление своевременно** четких количественных показателей, целей, которые должна достигнуть фирма.
2. **Определение основных действий**, которые необходимо осуществлять для достижения целей, принимая во внимание воздействие внешних факторов и имеющиеся внутренние возможности фирмы.
3. **Разработка гибкой системы планирования**, обеспечивающая достижение поставленных целей.

Применение планирования на фирме позволяет:

- **предвидеть** перспективу развития фирмы в будущем;
- более **рационально использовать** все ресурсы предприятия;
- **избежать** риска банкротства;
- более **целеустремленно и эффективно** проводить научно-техническую политику;
- **улучшать** контроль в организации;
- **увеличивать возможности** в обеспечении фирмы необходимой информацией.

Постоянная неопределенность будущего является одной из причин, по которой планирование должно осуществляться непрерывно. В силу внешних изменений или ошибок управления события могут разворачиваться не так, как предполагало руководство при выработке планов. Поэтому **планы необходимо пересматривать**, чтобы они согласовывались с реальностью. Там, где есть планирование, неопределенность сокращается. Однако полностью удалить ее не под силу ни одной фирме в силу разнообразия рыночной системы. Но можно осуществлять некоторый **контроль над рынком**, и такие усилия приносят определенный успех.

3. Основы доступа.

В соответствии с законодательством об архивном деле пользователь архивными документами имеет право свободно искать и получать для изучения архивные документы. Данное право гарантированно Конституцией РФ.

Доступ к архивным документам обеспечивается путем предоставления пользователю архивными документами справочно-поисковых средств и информации об этих средствах, а также подлинников и (или) копий необходимых ему документов.

В соответствии с п. 2.3. раздела 2 «Правил» по категориям доступа архивные документы делятся на открытые, ограниченного доступа и на хранящиеся на особых условиях доступа к ним.

Открытыми являются все архивные документы, доступ к которым не ограничен в соответствии с международными договорами Российской Федерации, законодательством Российской Федерации, а также в соответствии с распоряжением собственника или владельца архивных документов, находящихся в частной собственности.

К архивным документам ограниченного доступа относятся:

– архивные документы, содержащие сведения, составляющие государственную тайну или иные охраняемые законодательством Российской Федерации тайны;

– архивные документы, содержащие сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу его безопасности;

– архивные документы, собственники или владельцы которых, передавая их в архив, установили в договоре условия их использования и доступа к ним.

Доступ к указанным архивным документам до утраты ими секретности или конфиденциальности, а также их использование осуществляются в установленном порядке.

Ограничивается доступ к подлинникам особо ценных, в том числе уникальных документов, и к документам Архивного фонда Российской Федерации с высокой степенью разрушения материальных носителей, угрожающей физической целостности документов.

Условия доступа к архивным документам, находящимся в частной собственности, за исключением архивных документов, доступ к которым регламентируется законодательством Российской Федерации, устанавливаются собственником или владельцем архивных документов.

Доступ к архивным документам может быть ограничен в соответствии с международным договором Российской Федерации, законодательством Российской Федерации, а также в соответствии с распоряжением собственника или владельца архивных документов, находящихся в частной собственности.

Ограничивается доступ к архивным документам, независимо от их форм собственности, содержащим сведения, составляющие государственную и иную охраняемую законодательством Российской Федерации тайну. Также доступ ограничен к подлинникам особо ценных документов, в том числе уникальных документов, и документам Архивного фонда Российской Федерации, признанным в неудовлетворительном физическом состоянии.

Отмена ограничения на доступ к архивным документам, содержащим сведения, составляющие государственную и иную охраняемую законодательством Российской Федерации тайну, осуществляется в соответствии с законодательством Российской Федерации.

Ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, устанавливается на срок 75 лет со дня создания указанных документов.

Доступ пользователя к подлинникам особо ценных документов, в том числе уникальных документов, к документам Архивного фонда Российской Федерации, находящимся в неудовлетворительном физическом состоянии, осуществляется в исключительных случаях (в том числе для проведения работ по изучению палеографических особенностей текстов архивных документов) с письменного разрешения руководителя архива. Пользователю предоставляются копии указанных документов (фонд пользования) или документальные публикации, содержащие данные документы.

Архив не вправе ограничивать или определять пользователю условия использования информации, полученной им в результате самостоятельного поиска или предоставленной ему в порядке оказания архивом платных услуг, за исключением случаев, предусмотренных законодательством РФ или оговоренных в договоре архива с пользователем по информационному обслуживанию.

1. 11 Лекция № 11 (2 часа).

Тема: «Организация управления доступом и защиты ресурсов ОС»

1.11.1 Вопросы лекции:

1. Основы защиты ОС.
2. Практические методы защиты.

1.11.2 Краткое описание проводимого занятия:

1. Основы защиты ОС.

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.

2. Практические методы защиты.

Есть несколько простых правил, соблюдая которые, можно не беспокоиться о своей безопасности:

Скачивать программы можно ТОЛЬКО из надежных источников и как можно меньше со всяческих якобы "хакерских" сайтов... Львиная доля Троянов приходится именно на файлы с этих серверов.

Если скачали какую-то программу - ОБЯЗАТЕЛЬНО необходимо проверить ее на наличие вирусов и других вредоносных программ.

Никогда не надо запускать программы, пришедшие по E-MAIL.

В качестве паролей надо всегда использовать замысловатые наборы символов, типа Jqp2FQs, и по возможности стараться их вводить в окне терминала вручную - это обезоружит Троянов, отсылающих пароли на чей-то E-MAIL адрес.

Следует ограничить число посторонних, имеющих доступ к компьютеру, поскольку достаточно большое число троянов и вирусов переносится на внешних носителях (дискетах и дисках). Также рекомендуется периодически менять пароли на особо важные аккаунты.

Те троянские программы, которые постоянно обеспечивают доступ к зараженной ЭВМ, а, следовательно, держат на ней открытый порт какого-либо транспортного протокола, можно обнаруживать с помощью утилит контроля за сетевыми портами. Например, для операционных систем клона Microsoft Windows такой утилитой является программа NetStat. Запуск ее с ключом "netstat - a" выведет на экран все активные порты ЭВМ. От оператора в этом случае требуется знать порты стандартных сервисов, которые постоянно открыты на ЭВМ, и тогда, любая новая запись на мониторе должна привлечь его внимание. На сегодняшний день существует уже несколько программных продуктов, производящих подобный контроль автоматически.

Ещё один способ обнаружить троянцев - посмотреть открытые порты компьютера и процессы, которые их открыли. Обычно троянская программа использует порты >1000 (например, 30003,47891,6666,31337). Список портов, использующихся троянскими программами - Приложение 1.

В Windows XP Professional SP2 есть встроенное средство защиты - брандмауэр Windows.

Брандмауэр (межсетевой экран или фаервол) - комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Брандмауэры бывают двух видов, программные и аппаратные.

Брандмауэр используется для защиты компьютера от несанкционированного доступа через сеть или Интернет. Брандмауэр Windows встроен в Windows XP и включен автоматически для защиты компьютера от вирусов и других угроз безопасности. Брандмауэр отличается от антивирусного программного обеспечения, однако их совместная работа обеспечивает надежную защиту компьютера. Можно сказать, что

брандмауэр охраняет окна и двери от проникновения неизвестных и нежелательных программ, в то время как антивирусное программное обеспечение предотвращает появление вирусов или других угроз безопасности, которые стремятся пробраться через парадный вход. В Microsoft Windows XP (SP2) брандмауэр Windows включен по умолчанию. Необязательно использовать именно брандмауэр Windows - можно установить и включить любой брандмауэр по выбору.

1. 12 Лекция № 12 (2 часа).

Тема: «Разработка защищенных приложений. Программное управление файловыми ресурсами и сессиями»

1.12.1 Вопросы лекции:

1. Разработка защищенных приложений.
2. Методы зашиты.

1.12.2 Краткое содержание вопросов:

1. Разработка защищенных приложений.

Основная часть уязвимостей появляется на ранних стадиях создания программного обеспечения. Поэтому, наибольшей эффективностью обладает подход, который устраняет проблемы безопасности на начальной стадии разработки приложений, нежели стандартный метод их исправления по необходимости. Консультанты моделируют потенциальные угрозы безопасности еще до создания программного продукта, что позволяет закрыть всевозможные бреши на стадии его разработки.

Глубокие знания процесса разработки прикладных приложений, позволяют им устранять существующие бреши в программном обеспечении, а также избежать потенциальных уязвимостей при создании собственного продукта.

Специалисты регулярно проводят проверку безопасности:

- сайтов интернет торговли, банков, финансовых и других учреждений;
- программного продукта для разработчиков, интернет-порталов и настольных систем.

Наша компания предлагает полный объем услуг по обеспечению информационной безопасности бизнес проектов, включая:

- оценка уязвимости встроенных систем;
- устранение брешей в системе предварительно записанных голосовых сообщений IVR;
- обнаружение «дыр» в настольных и мобильных приложениях, оценка величины рисков, практические рекомендации по их снижению;
- моделирование потенциальных угроз безопасности приложений, а также обнаружение и устранение их на ранней стадии разработки;
- определение уязвимостей, рисков, прочих угроз безопасности в инфраструктуре веб-подразделений организации;

- повышения уровня безопасности установленных приложений, проверка скриптов и исходного программного кода, устранение выявленных ошибок;
- оценка потенциальных способов проникновения хакеров в веб-приложение, обнаружение уязвимостей рабочих версий веб-порталов, определение степени коммерческих рисков и проведение консультаций по их снижению.

2. Методы зашиты.

Методы обеспечения безопасности информации в ИС:

- препятствие;
- управление доступом;
- механизмы шифрования;
- противодействие атакам вредоносных программ;
- регламентация;
- принуждение;
- побуждение.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Управление доступом включает следующие функции зашиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

Принуждение – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на *аппаратные* и *физические*.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Как отмечалось, многие из них слиты с ПО самой ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем первого руководителя.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения (которые традиционно сложились ранее), складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например честность) либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения. Характерным примером таких предписаний является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

1. 13 Лекция № 13 (2 часа).

Тема: «Анализ симптома атаки и методы защиты»

1.13.1 Вопросы лекции:

1. Симптомы атаки.
2. Виды атак.
3. Методы предотвращения.

1.13.2 Краткое содержание вопросов:

1. Симптомы атаки.

Существует ряд признаков, свидетельствующих о заражении компьютера. Если вы замечаете, что с компьютером происходят "странные" вещи, а именно:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- неожиданно открывается и закрывается лоток CD-ROM-устройства;
- произвольно, без Вашего участия, на вашем компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя Вы никак не инициировали такое ее поведение,

то, с большой степенью вероятности, можно предположить, что ваш компьютер поражен вирусом.

Кроме того, есть некоторые характерные признаки поражения вирусом через почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера. Существуют также косвенные признаки заражения компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- Microsoft Internet Explorer "зависает" или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуем вам:

2. Виды атак.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие может осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятельность. Для оценки типов атак необходимо знать некоторые ограничения, изначально присущие протоколу TPC/IP. Сеть Интернет создавалась для связи между государственными учреждениями и университетами в помощь учебному процессу и научным исследованиям. Создатели этой сети не подозревали, насколько широко она распространится. В результате, в спецификациях ранних версий интернет-протокола (IP) отсутствовали требования безопасности. Именно поэтому многие реализации IP являются изначально уязвимыми. Через много лет, получив множество рекламаций (RFC - Request for Comments), мы, наконец, стали внедрять средства безопасности для IP. Однако ввиду того, что изначально средства защиты для протокола IP не разрабатывались, все его реализации стали дополняться разнообразными сетевыми процедурами, услугами и продуктами, снижающими риски, присущие этому протоколу. Далее мы кратко обсудим типы атак, которые обычно применяются против сетей IP, и перечислим способы борьбы с ними.

Снифферы пакетов

Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты,

полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом снифер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью снифера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам. Хакеры слишком хорошо знают и используют наши человеческие слабости (методы атак часто базируются на методах социальной инженерии). Они прекрасно знают, что мы пользуемся одним и тем же паролем для доступа к множеству ресурсов, и поэтому им часто удается, узнав наш пароль, получить доступ к важной информации. В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в сеть и к ее ресурсам.

IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример - атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения.

DoS, без всякого сомнения, является наиболее известной формой хакерских атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту. Даже среди хакеров атаки DoS считаются тривиальными, а их применение вызывает презрительные усмешки, потому что для организации DoS требуется минимум знаний и умений. Тем не менее, именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность. Если вы хотите побольше узнать об атаках DoS, вам следует рассмотреть их наиболее известные разновидности, а именно:

3. Методы предотвращения

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS)) — программное или аппаратное средство, предназначенное для выявления фактов

неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть.

IDS всё чаще становятся необходимым дополнением инфраструктуры сетевой безопасности. В дополнение к межсетевым экранам (firewall), работа которых происходит на основе политики безопасности, IDS служат механизмами мониторинга и наблюдения подозрительной активности. Они могут обнаружить атакующих, которые обошли Firewall, и выдать отчет об этом администратору, который, в свою очередь, предпримет дальнейшие шаги по предотвращению атаки. Технологии обнаружения проникновений не делают систему абсолютно безопасной. Тем не менее практическая польза от IDS существует и не маленькая.

Использование IDS помогает достичь нескольких целей:

- Обнаружить вторжение или сетевую атаку;
- Спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития. Атакующий обычно выполняет ряд предварительных действий, таких как, например, сетевое зондирование (сканирование) или другое тестирование для обнаружения уязвимостей целевой системы;
- Выполнить документирование существующих угроз;
- Обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;
- Получить полезную информацию о проникновениях, которые имели место, для восстановления и корректирования вызвавших проникновение факторов;
- Определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

Обычно IDS включает:

- Сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;
- Подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;
- Хранилище, в котором накапливаются первичные события и результаты анализа;
- Консоль управления, позволяющая конфигурировать IDS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты.

По способам мониторинга IDS системы подразделяются на *network-based (NIDS)* и *host-based (HIDS)*.

Основными коммерческими IDS являются *network-based*. Эти IDS определяют атаки, захватывая и анализируя сетевые пакеты. Слушая сетевой сегмент, NIDS может просматривать сетевой трафик от нескольких хостов, которые присоединены к сетевому сегменту, и таким образом защищать эти хосты.

1. 14 Лекция № 14 (2 часа).

Тема: «Анализ установок безопасности системы»

1.14.1 Вопросы лекции:

1. Основные параметры защиты.

2. Характеристики установок безопасности.

1.14.2 Краткое описание проводимого занятия:

1. Основные параметры защиты.

К процедурному уровню относятся меры безопасности, реализуемые сотрудниками предприятия. Выделяются следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

В рамках управления персоналом для каждой должности должны существовать квалификационные требования по информационной безопасности. В должностные инструкции должны входить разделы, касающиеся защиты информации. Каждого сотрудника предприятия необходимо обучить мерам обеспечения информационной безопасности теоретически и отработать выполнение этих мер практически.
Информационная безопасность ИС предприятия зависит от окружения, в котором она работает. Необходимо принять меры для обеспечения физической защиты зданий и прилегающей территории, поддерживающей инфраструктуры и самих компьютеров.
При разработке проекта СОИБ предполагается адекватная реализация мер физической защиты офисных зданий и других помещений, принадлежащих предприятию, по следующим направлениям:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры.

Предполагается также адекватная реализация следующих направлений поддержания работоспособности:

- поддержка пользователей ИС;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Программа информационной безопасности должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.
Реакция на нарушения режима информационной безопасности преследует две главные цели:

- блокирование нарушителя и уменьшение наносимого вреда;
- недопущение повторных нарушений.

На предприятии должен быть выделен сотрудник, доступный 24 часа в сутки, отвечающий за реакцию на нарушения. Все пользователи ИС должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В случае невозможности связи с данным сотрудником, должны быть разработаны и внедрены процедуры первичной реакции на информационный инцидент.
Планирование восстановительных работ позволяет подготовиться к авариям ИС, уменьшить ущерб от них и сохранить способность к функционированию, хотя бы в минимальном объеме.

Механизмы контроля, существенные для предприятия с юридической точки зрения, включают в себя:

- Защиту данных и тайну персональной информации;
- Охрану документов организации;
- Права на интеллектуальную собственность.

В соответствии с международным стандартом ISO 17799, а также руководящими документами ФСТЭК, ключевыми также являются следующие механизмы контроля:

- Политика информационной безопасности;
- Распределение ролей и ответственности за обеспечение информационной безопасности;
- Обучение и тренинги по информационной безопасности;
- Информирование об инцидентах безопасности;
- Управление непрерывностью бизнеса.

Меры обеспечения информационной безопасности программно-технического уровня

Программно-технические средства защиты располагаются на следующих рубежах:

- Защита внешнего периметра КСПД;
- Защита внутренних сетевых сервисов и информационных обменов;
- Защита серверов и рабочих станций;
- Защита системных ресурсов и локальных приложений на серверах и рабочих станциях;
- Защита выделенного сегмента руководства компании.

На программно-техническом уровне выполнение защитных функций ИС осуществляется следующими служебными сервисами обеспечения информационной безопасности:

- идентификация/аутентификация пользователей ИС;
- разграничение доступа объектов и субъектов информационного обмена;
- протоколирование/аудит действий легальных пользователей;
- экранирование информационных потоков и ресурсов КСПД;
- туннелирование информационных потоков;
- шифрование информационных потоков, критической информации;
- контроль целостности;
- контроль защищенности;
- управление СОИБ.

На внешнем рубеже информационного обмена располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они, вместе со средствами поддержки виртуальных частных сетей, объединяемых с межсетевыми экранами, образуют внешний периметр информационной безопасности, отделяющий информационную систему предприятия от внешнего мира.

Сервис активного аудита СОИБ (как и управление) должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить атаку, даже, если по каким-либо причинам, она окажется успешной.

Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу пользователя к ИС предприятия должна предшествовать идентификация и аутентификация субъектов информационного обмена (пользователей и процессов).

Средства шифрования и контроля целостности информации, передаваемой по каналам связи, целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование.

Последний рубеж образуют средства пассивного аудита, помогающие оценить последствия реализации угроз информационной безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов.

2.Характеристики установок безопасности

Установки безопасности ОС:

- препятствие;
- управление доступом;
- механизмы шифрования;
- противодействие атакам вредоносных программ;
- регламентация;
- принуждение;
- побуждение.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Управление доступом включает следующие функции зашиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

Принуждение – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на *аппаратные* и *физические*.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Как отмечалось, многие из них слиты с ПО самой ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем первого руководителя.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения (которые традиционно сложились ранее), складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например честность) либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения. Характерным примером таких предписаний является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

1. 15 Лекция № 15 (2 часа).

Тема: «Основные механизмы безопасности: средства и методы аутентификации в ОС»

1.15.1 Вопросы лекции:

1. Мотивации, как функция управления.
2. Необходимость контроля. Этапы контроля.
3. Правовые аспекты безопасности.

1.15.2 Краткое содержание вопросов:

1. Мотивации, как функция управления.

Природа мотивации. Для достижения целей организации руководству необходимо обеспечить эффективные действия персонала. Для этого нужно не только обеспечить функциональную загрузку работников и создать им необходимые условия, но и вызвать у них желание энергично совершать именно те действия, которые приближают организации

к достижению поставленных целей. В связи с этим руководство организации должно выполнять весьма важную функцию - создание условий для мотивации работников и осуществление ее на практике.

Мотивация как функция управления — это процесс, с помощью которого руководство организации побуждает работников действовать так, как было ранее запланировано и организовано, поскольку успех организации в определенной мере зависит от того, насколько эффективно действуют участники производственного процесса. Таким образом, *мотивацию в организации* можно трактовать как *побуждение членов организации к действию.* При этом мотивация представляет собой, с одной стороны, побуждение, навязанное индивидам извне, а с другой — это самопобуждение.

Чтобы разобраться в этой двойственной природе мотивации, важно понять, что поведение человека в трудовом процессе определяется взаимодействием различных внешних и внутренних побудительных сил, среди которых следует прежде всего выделить стимулы и мотивы. Стимул понимается как внешняя причина, побуждающая людей к деятельности, а мотив выступает как внутренняя побудительная сила. Если стимул заметен, его можно заранее спланировать или отменить, то мотив скрыт, его действие часто бывает неожиданным для наблюдателей, так как он зависит от инстинктивных импульсов, влечений, потребностей.

Вместе с тем стимулы и мотивы самым тесным образом связаны между собой. Процесс стимулирования деятельности члена организации — это такое воздействие на его поведение, которое включает в свою сферу все потребности, интересы, цели, стремления, мотивы. Следовательно, основу стимулирования составляет взаимодействие внешних условий и внутренней структуры личности члена организации. Стимулирование реализуется через создание условий, изменяющих трудовую ситуацию, чтобы у работника возникало желание, стремление к эффективной деятельности. Однако для успешного стимулирования необходимо знать внутренние мотивы, которые можно приобрести, только изучая социологию и психологию личности.

Обращение к изучению поведения людей в организации обусловлено тем, что не всякое целевое, направленное воздействие на поведение человека активизирует его деятельность, а лишь то, которое становится личностно значимым для данного конкретного человека, соответствует его внутренним устремлениям. Только в этом случае возникает заинтересованность работника в своей деятельности, психологическая предрасположенность по отношению к выполнению ролевых требований и, как следствие этого, побуждение к качественному выполнению работы. Стимулирование включает в себя не только создание внешней ситуации выбора определенной (наиболее привлекательной) формы поведения, но и ее соответствие структуре личности работника. Вместе с внешней стимуляцией эта внутренняя структура (в случае ее активизации) формирует непосредственный мотив действий.

2. Необходимость контроля. Этапы контроля.

Контроль – это процесс, при помощи которого руководство организации определяет, правильные ли его решения и не нуждаются ли они в корректировке. Контроль – это процесс обеспечения достижения организацией своих целей.

Функция контроля – это такая характеристика управления, которая позволяет выявить

проблемы и скорректировать деятельность организации до того, как эти проблемы перерастут в кризис. Сущность контроля заключается в трех основных элементах:

установление контролируемых стандартов деятельности;

измерение и анализ результатов деятельности, информация о которых получена с помощью контроля;

корректировка технологических, хозяйственных и иных процессов в соответствии со сделанными выводами и принятыми решениями.

Без надежной системы контроля ни одна организация не может успешно функционировать. Его задачи следующие.

Во-первых, контроль позволяет обнаружить во внешней или внутренней среде организации факторы, которые могут оказать существенное влияние на ее функционирование и развитие, и своевременно на них отреагировать.

Во-вторых, контроль помогает вскрыть неизбежные в деятельности любой организации нарушения, изъяны, ошибки и оперативно принять меры к их устранению.

В-третьих, результаты контроля служат основой для оценки работы организации и ее персонала за определенный период, эффективности и надежности системы управления ею.

Различают два основных вида контроля: финансовый и административный.

Различают три стадии управленческого контроля: предварительный, текущий и итоговый.

Предварительный контроль осуществляется до фактического начала работ в области человеческих ресурсы (анализ качеств, необходимых для выполнения работ), материальных ресурсов (стандарты качества, контроль за поступающими материалами), финансовых ресурсов (разработка бюджета, установление предельных значений затрат)

Текущий контроль осуществляется непосредственно в ходе выполнения работ, для этого необходим механизм обратной связи, который позволяет выявить непредвиденные проблемы и скорректировать линию поведения.

Оперативный контроль ориентирован на текущую производственную и хозяйственную деятельность, в частности на движение продукции в рамках технологического процесса (соблюдение последовательности операций, норм времени на их выполнение, качество труда); загрузку техники и оборудования; соблюдение общего графика работы.
Итоговый (заключительный) контроль связан с оценкой выполнения организацией планов и составлением новых; он предполагает всесторонний анализ не только конкретных результатов деятельности за текущий период, но и сильных и слабых ее сторон.
Заключительный контроль используется после выполнения работ и имеет две функции: дает информацию для планирования аналогичной продукции в будущем, способствует мотивации на основе измерения полученных результатов и определения степени вознаграждения.

Причины необходимости контроля.

1. Неопределенность - изменение законов, технологий, условий конкуренции приводят к необходимости к постоянной корректировки планов через систему обратной связи, которую обеспечивает контроль.

2. Предупреждение кризисных ситуаций - одно из главных назначений контроля - выявить проблемы и скорректировать деятельность организации до того, как эти проблемы перерастут в кризис

3. Правовые аспекты безопасности.

Прежде чем попытаться рассмотреть весь комплекс нормативных правовых актов, регламентирующих сферу обеспечения безопасности в Российской Федерации, стоит сказать, что общее количество законных и подзаконных актов, подходящих под данные требования таково, что окинуть взглядом и рассмотреть их в пределах одной курсовой работы попросту не представляется возможным. Даже поверхностный обзор данных документов займет более чем значительное количество печатных листов. В этом свете вполне понятно желание некоторых авторов каким-либо образом систематизировать и поделить вышеназванные нормативные акты, по каким-либо основаниям, дабы не углубляясь в изучение тонн печатной продукции окинуть взглядом всю правовую систему обеспечения информационной безопасности Российской Федерации. Мне наиболее понятной и целесообразной показалась скомпилированная из нескольких система четырех уровней правовой основы защиты информации, приведенная в учебнике Боера, занимающегося освещением вопросов информационного права, которая приведена далее.

Правовые основы защиты информации - это законодательный орган защиты информации, в котором можно выделить до 4 уровней правового обеспечения информационной безопасности информации и информационной безопасности предприятия.

Первый уровень правовой основы защиты информации

Первый уровень правовой охраны и защиты информации состоит из международных договоров о защите информации и государственной тайны, к которым присоединилась и Российская Федерация с целью обеспечения надежной информационной безопасности РФ. Кроме того, существует доктрина информационной безопасности РФ, поддерживающая правовое обеспечение информационной безопасности нашей страны.

Правовое обеспечение информационной безопасности РФ:

Международные конвенции об охране информационной собственности, промышленной собственности и авторском праве защиты информации в Интернете;

Конституция РФ (ст.23 определяет право граждан на тайну переписки, телефонных, телеграфных и иных сообщений);

Гражданский кодекс РФ (в ст.139 устанавливается право на возмещение убытков от утечки с помощью незаконных методов информации, относящейся к служебной и коммерческой тайне);

Уголовный кодекс РФ (ст.272 устанавливает ответственность за неправомерный доступ к компьютерной информации, ст.273 - за создание, использование и распространение вредоносных программ для ЭВМ, ст.274 - за нарушение правил эксплуатации ЭВМ, систем и сетей);

Федеральный закон "Об информации, информатизации и защите информации" от 20.02.95 № 24-ФЗ (ст.10 устанавливает разнесение информационных ресурсов по категориям доступа: открытая информация, государственная тайна, конфиденциальная информация, ст.21 определяет порядок защиты информации);

Федеральный закон "О государственной тайне" от 21.07.93 № 5485-1 (ст.5 устанавливает перечень сведений, составляющих государственную тайну; ст.8 - степени секретности сведений и грифы секретности их носителей: "особой важности", "совершенно секретно" и "секретно"; ст.20 - органы по защите государственной тайны, межведомственную комиссию по защите государственной тайны для координации деятельности этих органов; ст.28 - порядок сертификации средств защиты информации, относящейся к государственной тайне); Защита информации курсовая работа.

Федеральные законы "О лицензировании отдельных видов деятельности" от 08.08.2001 № 128-ФЗ, "О связи" от 16.02.95 № 15-ФЗ, "Об электронной цифровой подписи" от 10.01.02 № 1-ФЗ, "Об авторском праве и смежных правах" от 09.07.93 № 5351-1, "О правовой охране программ для электронных вычислительных машин и баз данных" от 23.09.92 № 3523-1 (ст.4 определяет условие при знания авторского права - знак © с указанием правообладателя и года первого выпуска продукта в свет; ст.18 - защиту прав на программы для ЭВМ и базы данных путем выплаты компенсации в размере от 5000 до 50 000 минимальных размеров оплаты труда при нарушении этих прав с целью извлечения прибыли или путем возмещения причиненных убытков, в сумму которых включаются полученные нарушителем доходы).

Таким образом, правовое обеспечение информационной безопасности весьма на высоком уровне, и многие компании могут рассчитывать на полную экономическую информационную безопасность и правовую охрану информации, и защиту, благодаря ФЗ о защите информации.

Второй уровень правовой защиты информации
На втором уровне правовой охраны информации и защиты (ФЗ о защите информации) - это подзаконные акты: указы Президента РФ и постановления Правительства, письма Высшего Арбитражного Суда и постановления пленумов ВС РФ. [16]

Третий уровень правового обеспечения системы защиты экономической информации

К данному уровню обеспечения правовой защиты информации относятся ГОСТы безопасности информационных технологий и обеспечения безопасности информационных систем.

Также на третьем уровне безопасности информационных технологий присутствуют руководящие документы, нормы, методы информационной безопасности и классификаторы, разрабатывающиеся государственными органами.

Четвертый уровень стандарта информационной безопасности

Четвертый уровень стандарта информационной безопасности защиты конфиденциальной информации образуют локальные нормативные акты, инструкции, положения и методы информационной безопасности и документация по комплексной правовой защите информации рефераты по которым часто пишут студенты, изучающие технологии защиты информации, компьютерную безопасность и правовую защиту информации

1. 16 Лекция № 16 (2 часа).

Тема: «Аудит. Реализация политики аудита»

1.16.1 Вопросы лекции:

1. Возможности систем Windows.
2. Возможности систем UNIX

1.16.2 Краткое описание проводимого занятия:

1. Возможности систем Windows.

Практически повсеместно существуют проектные отделы, бухгалтерия, разработчики и другие категории сотрудников, совместно работающие над группами документов, хранящихся в общедоступной (Shared) папке на файловом сервере или на одной из рабочих станций. Может случиться так, что кто-то удалит важный документ или директорию из этой папки, в результате чего труд целого коллектива может быть потерян. В таком случае, перед системным администратором возникает несколько вопросов:

- Когда и во сколько произошла проблема?
- Из какой наиболее близкой к этому времени резервной копии следует восстановить данные?
- Это случилось непреднамеренно, или же кто-то действовал с умыслом?
- Может, имел место системный сбой, который может повториться ещё раз?

В Windows имеется система **Аудита,** позволяющая отслеживать и журналировать информацию о том, когда, кем и с помощью какой программы были удалены документы. По умолчанию, Аудит не задействован — слежение само по себе требует определённый процент мощности системы, а если записывать всё подряд, то нагрузка станет слишком большой. Тем более, далеко не все действия пользователей могут нас интересовать, поэтому политики Аудита позволяют включить отслеживание только тех событий, что для нас действительно важны.

Система Аудита встроена во все операционные системы **Microsoft Windows NT:** Windows XP/Vista/7, Windows Server 2000/2003/2008. К сожалению, в системах серии Windows Home аудит спрятан глубоко, и его настраивать слишком сложно.

Эта функция зачастую используется при обычной работе программ — например, исполненяя команду **Save (Сохранить),** программы пакета **MicrosoftOffice** сначала создают новый временный файл, сохраняют в него документ, после чего удаляют предыдущую версию файла. Аналогично, многие приложения баз данных при запуске сначала создают временный файл блокировок **(.lck),** затем удаляют его при выходе из программы.

Например, конфликтный сотрудник некоей компании при увольнении с места работы решил уничтожить все результаты своего труда, удалив файлы и папки, к которым он имел отношение. События такого рода хорошо заметны — они генерируют десятки, сотни записей в секунду в журнале безопасности. Конечно, восстановление документов из **Shadow Copies (Теневых Копий)** или ежесуточно автоматически создаваемого архива не составляет особого труда, но при этом я мог ответить на вопросы «Кто это сделал?» и «Когда это произошло?».

2. Возможности систем UNIX

Одним из инструментов, позволяющих повысить уровень безопасности в Linux, является подсистема аудита. С её помощью можно получить подробную информацию обо всех системных событиях.
Она не обеспечивает никакой дополнительной защиты, но предоставляет подробную информацию о нарушениях безопасности, на основании которой можно принять конкретные меры. Особенности работы с подсистемой аудита мы рассмотрим в этой статье.

Подсистема аудита: архитектура и принцип работы

Подсистема аудита была добавлена в ядро Linux начиная с версии 2.6. Она предназначена для отслеживания критичных с точки зрения безопасности системных событий.
В качестве примеров таких событий можно привести следующие (список далеко не полный):

- запуск и завершение работы системы;
- чтение, запись и изменение прав доступа к файлам;
- инициация сетевых соединений;
- попытки неудачной авторизации в системе;
- изменение сетевых настроек;
- изменение информации о пользователях и группах;
- запуск и остановка приложений;
- выполнение системных вызовов.

Ни одно из названных событий не может произойти без использования системных вызовов ядра. Чтобы их отслеживать, достаточно просто перехватывать соответствующие системные вызовы. Именно это и делает подсистема аудита:

Получив вызов от приложения в пространстве пользователя, подсистема аудита пропускает его через один из следующих фильтров: user, task или exit (более подробно о них речь пойдёт ниже). После этого вызов пропускается через фильтр exclude, который исходя из правил аудита передаёт его демону auditd для дальнейшей обработки.

Такая простая схема позволяет вполне эффективно отслеживать любой аспект работы ОС, а в случае компрометации системы выявлять подозрительные действия и определять их причину.

1. 17 Лекция № 17 (2 часа).

Тема: «Модели разграничения доступа»

1.17.1 Вопросы лекции:

1.Природа процесса принятия решений.
2. Рациональное решение проблем.

3. Уровни доступа.

1.17.2 Краткое содержание вопросов:

1.Природа процесса принятия решений.

Одним из наиболее мощных инструментов в руках менеджера является **информация.** *Эффективное управление* невозможно без сбора информации и ее обработки различными методами с целью подготовки и принятия управленческих решений. Методы получения информации многообразны и не являются предметом рассмотрения в данной работе. Методы обработки и анализа экономической информации составляют суть эконометрики. Для целевого распределения информации по адресатам необходима интегрированная**информационная система**, направленная на решение задач, стоящих перед предприятием, и являющаяся отражением протекающих бизнес процессов.

Современный *менеджер* должен обладать незаурядными аналитическими способностями, которые позволяли бы ему адекватно оценивать текущую и специально собранную информацию, касающуюся всей гаммы внешних и внутренних факторов. Это необходимо для того, чтобы ставить реальные цели, разрабатывать, принимать и реализовывать соответствующие управленческие решения. Важно постоянно контролировать выполнение принятых решений, вовремя корректировать цели и, как следствие, корректировать средства их достижения.

Другими словами, стратегическое управление является фундаментом общего подхода к управлению всей компанией. Говорят, что исполнительный директор одной из компаний удачно сформулировал важную мысль: "В основном наши конкуренты знают те же самые фундаментальные концепции, методы и подходы, что и мы, и они также имеют все возможности для скрупулезного следования им, как и мы. Зачастую разница достигнутого ими и нами успеха заключается в относительной тщательности и дисциплинированности, с которой они и мы разрабатываем и исполняем свои стратегии на будущее".

Преимуществами стратегического подхода к управлению (в противоположность свободной импровизации, интуиции или бездеятельности) на основе интенсивного использования информационных систем являются:

- обеспечение направленности идей организации на ключевой вопрос стратегии "что мы собираемся делать и чего добиваемся?"
- необходимость для менеджеров более четко реагировать на появляющиеся перемены, новые возможности и угрожающие тенденции;
- возможность для менеджеров оценивать альтернативные варианты капитальных вложений и расширения персонала, т.е. разумно переносить ресурсы в стратегически обоснованные и высокоэффективные проекты;
- возможность объединить решения руководителей всех уровней управления, связанных со стратегией.

Итак, можно сделать следующий *вывод*: стратегический *менеджмент* представляет собой современный вариант системного подхода к управлению промышленным предприятием или иной организацией.

2. Рациональное решение проблем.

Процесс принятия решений очень непрост. Научный подход рассматривает принятие управленческого решения как целостный процесс, который позволяет всесторонне изучить возникшую проблему, проанализировать возможные варианты ее решения и выбрать наиболее эффективный из них. Научный подход обеспечивает принятие рациональных решений. *Рациональное решение базируется на объективном и глубоком анализе проблемы и учитывает определенные формально-логические требования.* В каждой организации практика разработки и принятия управленческих решений имеет свои особенности. Они определяются характером и спецификой деятельности организации, ее структурой, внутренней культурой и т.д. Тем не менее, есть общая для любого процесса принятия решений технология. Она используется в любой организации и сводится к трем стадиям:

1) подготовка решения;

2) принятие решения;

3) реализация решения.

На *стадии подготовки управленческого решения* проводится экономический анализ ситуации на микро - и макроуровне, включающий поиск, сбор и обработку информации, а также выявляются и формулируются проблемы, требующие решения.

На *стадии принятия решения* осуществляется разработка и оценка альтернативных решений и курсов действий, проводимых на основе многовариантных расчетов; отбор критериев выбора оптимального решения; выбор и принятие наилучшего решения.

На *стадии реализации решения* принимаются меры для конкретизации решения и доведении его до исполнителей, осуществляется контроль за ходом его выполнения, вносятся необходимые коррективы и дается оценка полученного результата от выполнения решения.

Способы представления процесса принятия решений различны. В их основе - различные подходы к управлению: системный, количественный, ситуационный и т.д. В определенном смысле универсальным является ситуационный подход. Он наиболее полно отражает проблемы, возникающие при управленческой деятельности, а подготовка, принятие и реализация решения осуществляются на основе всей совокупности информации о ситуации, ее тщательного анализа и оценок.

Процесс принятия рационального решения может быть представлен следующей схемой.

1. Диагностика проблемы

2. Формулирование ограничений и критериев для принятия решения

3. Оценка альтернатив

4. Реализация принятого решения

5. Окончательный выбор

3. Уровни доступа.

1) Информация без ограничения права доступа. К такого рода информации, например, относится:

• информация общего пользования, Предоставляемая пользователям бесплатно (сюда не относится возможность скачать фильмы бесплатно);
• информация о состоянии окружающей природной среды, ее загрязнении - сведения (данные), полученные в результате мониторинга окружающей природной среды, ее загрязнения (Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия»);
• информация в области работ по хранению, перевозке, уничтожению химического оружия - сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по хранению химического оружия и объектов по уничтожению химического оружия, мероприятиях по обеспечению химической, санитарно-гигиенической, экологической и пожарной безопасности при проведении работ по хранению, перевозке и уничтожению химического оружия, а также о мерах по предотвращению возникновения чрезвычайных ситуаций и ликвидации их последствий при выполнении указанных работ, предоставляемые по запросам граждан и юридических лиц, в том числе общественных объединений (Федеральный закон от 2 мая 1997 г. № 76-ФЗ «Об уничтожении химического оружия», статья 1.2).

Информация, содержащая сведения об обстоятельствах и фактах, представляющих угрозу жизни, здоровью граждан, не подлежит засекречиванию, не может быть отнесена к тайне.

2) Информация с ограниченным доступом - государственная тайна, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна и персональные данные как институт охраны права неприкосновенности частной жизни.

3) Информация, распространение которой наносит вред интересам общества, законным интересам и правам граждан, - порнография; информация, разжигающая национальную, расовую и другую рознь; пропаганда(в т.ч. печать листовок) и призывы к войне, ложная реклама, реклама со скрытыми вставками и т.п. - так называемая «вредная» информация.

4) Объекты интеллектуальной собственности (то, что не может быть отнесено к информации с ограниченным доступом, но охраняется особым порядком через институты интеллектуальной собственности - авторское право, патентное право, средства индивидуализации и т. п. Исключение составляют ноу-хау, которые охраняются в режиме коммерческой тайны).

5) Иная общедоступная информация, среди которой ученые выделяют более 20 видов открытой общедоступной информации.

К ограничениям и запретам следует отнести следующие перечни:

1. Перечень оснований для ограничения информационных прав:

• защита основ конституционного строя;
• защита нравственности, здоровья, прав, законных интересов других лиц;
• обеспечение обороны страны и безопасности государства;
• обеспечение общественного спокойствия в целях предотвращения беспорядков и борьбы с преступностью;

• предотвращение разглашения конфиденциальной информации;
• обеспечение авторитета и беспристрастности правосудия;
• условия чрезвычайного положения, установленные по закону (на определенный период).

2. Перечень случаев прямого ограничения информационных прав:

• использование прав в целях насильственного изменения конституционного строя;
• пропаганда социальной ненависти, социального, расового, национального, религиозного, языкового превосходства, насилия и войны;
• нарушение права на неприкосновенность частной жизни (на личную, семейную тайну), неприкосновенность жилища, права на уважение и защиту чести, достоинства и репутации, тайны переписки, телефонных переговоров, телеграфных и иных сообщений;
• нарушение права на государственную, служебную, профессиональную, коммерческую и банковскую тайну;
• право на отказ от свидетельствования против себя самого, своего супруга и близких родственников.

3. Перечень видов информации с ограниченным доступом:

• государственная тайна;
• служебная тайна;
• коммерческая тайна;
• банковская тайна;
• профессиональная тайна;
• персональные данные.

4. Перечень сведений, доступ к которым не может быть ограничен.

1. 18 Лекция № 18 (2 часа).

Тема: «Симметричное шифрование и формирование ключа на основе пароля»

1.18.1 Вопросы лекции:

1. Общие сведения о симметричном шифровании.
2. Формирование ключа на основе пароля.
3. Дешифровка.

1.18.2 Краткое содержание вопросов:

1.Общие сведения о симметричном шифровании

Симметричное шифрование предусматривает использование одного и того же ключа и для зашифрования, и для расшифрования. К симметричным алгоритмам применяются два основных требования: полная утрата всех статистических закономерностей в объекте шифрования и отсутствие линейности. Принято разделять симметричные системы на блочные и поточные. В блочных системах происходит разбиение исходных данных на блоки с последующим преобразованием с помощью ключа.

В поточных системах вырабатывается некая последовательность (выходная гамма), которая в последующем накладывается на само сообщение, и шифрование данных происходит потоком по мере генерирования гаммы. Схема связи с использованием симметричной криптосистемы представлена на рисунке.

Схема связи с использованием симметричной криптосистемы, где M - открытый текст, K - секретный ключ, передаваемый по закрытому каналу, En(M) - операция зашифрования, а Dk(M) - операция расшифрования

Обычно при симметричном шифровании используется сложная и многоступенчатая комбинация подстановок и перестановок исходных данных, причем ступеней (проходов) может быть множество, при этом каждой из них должен соответствовать «ключ прохода». Операция подстановки выполняет первое требование, предъявляемое к симметричному шифру, избавляясь от любых статистических данных путем перемешивания битов сообщения по определенному заданному закону. Перестановка необходима для выполнения второго требования – придания алгоритму нелинейности. Достигается это за счет замены определенной части сообщения заданного объема на стандартное значение путем обращения к исходному массиву.

Симметричные системы имеют как свои преимущества, так и недостатки перед асимметричными. К преимуществам симметричных шифров относят высокую скорость шифрования, меньшую необходимую длину ключа при аналогичной стойкости, большую изученность и простоту реализации. Недостатками симметричных алгоритмов считают в первую очередь сложность обмена ключами ввиду большой вероятности нарушения секретности ключа при обмене, который необходим, и сложность управления ключами в большой сети.

2.Формирование ключа на основе пароля.

Существует тип протоколов, который последнее время набирает все большую популярность, но все еще не является широко известным — протоколы выработки общего ключа с аутентификацией на основе пароля. К таким протоколам относится российский протокол SESPAKE (Security Evaluated Standardized Password Authenticated Key Exchange), с появлением которого в России и возникла необходимость в рассмотрении особенностей протоколов подобного типа. Целью данной статьи является скорее не дать очередное формальное описание нового протокола, а помочь читателю уловить его основную идею и особенности и понять, почему в нём присутствуют те или иные шаги, почему они важны и чем подобный класс протоколов отличается от всего, что было известно ранее.

PBKDF2 (англ. Password-Based Key Derivation Function) — стандарт формирования ключа на основе пароля. Является частью PKCS #5 v2.0 (RFC 2898). Заменил PBKDF1, который ограничивал длину порождаемого ключа 160 битами.

PBKDF2 использует псевдослучайную функцию для получения ключей. Длина генерируемого ключа не ограничивается (хотя эффективная мощность пространства ключей может быть ограничена особенностями применяемой псевдослучайной функции). Использование PBKDF2 рекомендовано для новых программ и продуктов. В качестве псевдослучайной может быть выбрана криптографическая хеш-функция, шифр, HMAC.

3.Дешифровка.

То есть, было необходимо разработать программу, которая позволит не просто хранить данные на сервере, но и предоставит возможность работы с ними через web-интерфейс и при этом обеспечит их бесполезность для злоумышленников в случае кражи, что достигается шифрованием/дешифрованием исключительно на стороне клиента.
Для типичного сценария использования возможна работа с тремя типами данных:

- обычный текст, вводимый в поля ввода формы и хранящийся на сервере в базе данных в зашифрованном виде
- файлы, которые хранятся на сервере в зашифрованном виде, и при необходимости пользователь может их скачать
- изображения, хранящиеся на сервере как зашифрованные файлы, но при необходимости они расшифровываются на стороне клиента и вставляются на web-страницу как обычные картинки.

Тот факт, что обработка данных должна производиться исключительно на стороне клиента, ограничивал выбор средств для реализации. На начальной стадии разработки была опробована связка «Java-апплет – Java-сервлет», но через какое-то время пришлось искать другой способ, потому что были трудности в отладке и передаче данных между апплетом и сервлетом.
Я остановился на использовании возможностей HTML5 и JavaScript-объекта «XmlHttpRequest Level 2» в частности, потому что они позволили с меньшими усилиями реализовать необходимый функционал.

Работа с текстом

Алгоритм шифрования:

- вносим текст в поле формы на web-странице
- шифруем текст с помощью функций Java Script
- отправляем зашифрованный текст на сервер, где сохраняем в базу данных.

Обратный процесс:

- получаем зашифрованные данные из базы данных с сервера
- дешифруем их с помощью функций Java Script
- выводим расшифрованный текст в нужное место на web-странице.

Работа с файлами

Процесс шифрования/дешифрования файлов происходит немного другим образом.

Алгоритм шифрования:

- выбираем файл с компьютера пользователя
- получаем содержимое файла в объект Java Script, используя XmlHttpRequest Level 2 и возможности HTML 5
- шифруем его с помощью функций Java Script
- отправляем зашифрованные данные на сервер, где сохраняем как файл.

Обратный процесс:

- получаем содержимое зашифрованного файла с сервера
- записываем его в объект Java Script, используя XmlHttpRequest Level 2 и возможности HTML 5
- дешифруем с помощью функций Java Script
- передаём расшифрованные данные в Java-апплет, чтобы дать пользователю возможность указать путь и имя для сохраняемого файла, т. к. на данный момент развития технологий в браузерах нельзя штатно вызывать диалог сохранения файла в произвольное место на компьютере пользователя, только в ограниченную «песочницу», что нам не подходит. Если по каким-либо причинам использование Java-апплета не подходит, эту часть можно заменить на Flash с аналогичным функционалом.

Работа с изображениями

Алгоритм шифрования:

- выбираем файл с изображением с компьютера пользователя
- записываем его содержимое в объект Java Script, используя XmlHttpRequest Level 2 и возможности HTML 5
- кодируем в формат Base64
- шифруем с помощью функций Java Script
- отправляем зашифрованные данные на сервер, где сохраняем в файл.

Обратный процесс:

- получаем содержимое зашифрованного изображения с сервера
- записываем его в объект Java Script, используя XmlHttpRequest Level 2 и возможности HTML 5
- дешифруем с помощью функций Java Script. На этом этапе получаем изображение, закодированное в формате Base64
- вставляем содержимое в тег на web-странице (браузеры по умолчанию поддерживают вставку изображений в формате Base64).

1. 19-22 Лекция № 19-22 (8 часов).

Тема: «Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС»

1.19-22.1 Вопросы лекции:

1. Задачи и принципы сопровождения системного программного обеспечения.

2. Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС

1.19-22.2 Краткое содержание вопросов:

1. Задачи и принципы сопровождения системного программного обеспечения.

Организация эффективной и надежной защиты операционной системы невозможна с помощью одних только программно-аппаратных средств. Эти средства обязательно должны, дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже самая надежная программно-аппаратная защита оборачивается фикцией.

Основные административные меры защиты.

1. Постоянный контроль корректности функционирования операционной системы, особенно ее подсистемы защиты. Такой контроль наиболее удобно организовать, если операционная система поддерживает регистрацию событий (event logging). В этом случае операционная система автоматически регистрирует в специальном журнале (или нескольких журналах) наиболее важные события, произошедшие в процессе функционирования системы.
2. Организация и поддержание адекватной политики безопасности. Политика безопасности должна постоянно корректироваться, оперативно реагируя на изменения в конфигурации операционной системы, установку, удаление и изменение конфигурации прикладных программных продуктов и расширений операционной системы, попытки злоумышленников преодолеть защиту операционной системы и т.д.
3. Инструктирование пользователей операционной системы о необходимости соблюдения мер безопасности при работе с операционной системой и контроль за соблюдением этих мер.
4. Регулярное создание и обновление резервных копий программ и данных операционной системы.

Постоянный контроль изменений в конфигурационных данных и политике безопасности операционной системы.

Основные принципы администрирования ОС.

- Непрерывность;
- Комплексность;
- Актуальность;
- Адекватность;
- Непротиворечивость. (разграничение доступа, настроек процессов);
- Формальный подход. Применение методик (инструкций, положений, приказов, РД и прочих рекомендательных документов) и четких концептуальных принципов при постановке задач администрирования и их реализации;
- Подконтрольность.

Задачи и принципы управления безопасностью.

Отдельные средства ИБ не обеспечивают эффективного функционирования и требуют объединения в единую и централизованно управляемую и постоянно действующую *систему информационной безопасности* Система ИБ обычно должна решать следующие задачи:

- ввод в систему списка имен пользователей и терминалов, допущенных к информации ИС;
- подготовку и ввод в систему, запись паролей пользователей на носители;

• ввод в систему назначенных полномочий пользователей и терминалов;
• раздачу пользователям носителей с паролями и значений паролей, запоминаемых и вводимых пользователями вручную с клавиатуры;
• сбор сигналов несовпадения паролей и нарушения полномочий пользователей;
• установление времени, места и причины НСД;
• анализ ситуации, принятие адекватных мер и восстановление нормального функционирования ИС
• контроль конфигурации системы;
• сбор сигналов вскрытия аппаратуры и контроль ввода (вывода) аппаратуры в (из) ремонт (а) и на (из) профилактику(и);
• контроль журнала регистрации доступа к информации ИС и периодический вызов справок из него;
• взаимодействие со службой функционального контроля ИС;
• контроль функционирования системы защиты;
• подготовку ключей, контроль и обеспечение функционирования средств шифрования информации;
• контроль стирания и уничтожения остатков секретной информации на машинных и бумажных носителях;
• регистрацию, учет и разграничение доступа к носителям информации и ПО;
• ведение статистики и прогнозирование НСД.

И удовлетворять следующим принципом:
■ непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;
■ плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);
■ целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;
■ конкретной. Защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
■ активной. Защищать информацию необходимо с достаточной степенью настойчивости;
■ надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;
■ универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;
■ комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что защита — это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообусловливающих друг друга сторон, свойств, тенденц

2. Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС

Безопасность – одна из наиболее актуальных проблем в области ИТ в настоящее время, ввиду сильной зависимости повседневной деятельности и бизнеса от компьютерных

технологий и ввиду резко возрастающего числа сетевых атак (киберпреступности). Особенно важна безопасность для операционных систем и сетей как основных объектов атак. В лекции рассмотрены следующие вопросы:

- Проблема безопасности
- Аутентификация
- Программные угрозы (атаки)
- Системные угрозы (атаки)
- Защита систем
- Обнаружение взлома
- Криптография
- Безопасность в Windows NT / 2000 / XP / 2003 / Vista, в.NET
- Инициатива Trustworthy Computing Initiative корпорации Microsoft.

Проблема безопасности

Безопасность (security) – это защита от внешних атак. В настоящее время наблюдается значительный рост числа самых разнообразных атак хакеров, угрожающих целостности информации, работоспособности компьютерных систем и зависящих от них компаний, благосостоянию и личной безопасности людей. Для защиты от атак необходимы специальные меры безопасности, компьютерные технологии и инструменты.
В любой компьютерной системе должна быть реализована подсистема безопасности, которая должна проверять внешнее окружение системы и защищать ее от:

- Несанкционированного доступа
- Злонамеренной модификации или разрушения
- Случайного ввода неверной информации.

Практика показывает, что легче защитить от случайной, чем от злонамеренной порчи информации.

Аутентификация

Одной из наиболее широко используемых мер безопасности является аутентификация (authentication) – идентификация пользователейпри входе в систему. Такая идентификация пользователей наиболее часто реализуется через логины – зарегистрированные имена пользователей для входа в систему – и пароли – секретные кодовые слова, ассоциируемые с каждым логином.
Основной принцип использования паролей в том, что они должны сохраняться в секрете. Поэтому одна из традиционных целей атакующихххакеров состоит в том, чтобы любыми способами выведать у пользователя его логин и пароль. Для сохранения секретности паролей предпринимаются следующие меры.

- Частая смена паролей. Аналогичные меры применялись в армии во время войны. Большинство сайтов и других систем (например, сайт партнеров фирмы Microsoft) требуют от пользователей регулярной (например, не реже. чем раз в три месяца) смены паролей, иначе сайт блокируется для доступа. Подобные меры вполне оправданы.
- Использование "не угадываемых" паролей. Практически все системы требуют от пользователя при регистрации устанавливать пароли, не являющиеся легко угадываемыми: например, как правило, пароль должен содержать большие и маленькие буквы и цифры, специальные символы и иметь длину не менее 7-8 символов. Используются также автоматические генераторы не угадываемых паролей. Поэтому

использование в качестве паролей легко угадываемых слов – например, имени любимой собаки или общеупотребительного понятия – не рекомендуется.

- Сохранение всех неверных попыток доступа. Во многих системах реализован системный журнал, в котором фиксируются все неверные попытки ввода логинов и паролей. Обычно дается фиксированное число таких попыток (например, три).

Пароли также могут быть закриптованы или разрешены для доступа лишь один раз, после чего от пользователя требуется смена пароля.

Программные угрозы (атаки)

Рассмотрим некоторые типичные виды угроз и атак, используемые хакерами.
Троянская программа (Trojan Horse) – атакующая программа, которая "подделывается" под некоторую полезную программу, но при своем запуске не по назначению (злонамеренно) использует свое окружение, например, получает и использует конфиденциальную информацию. Троянские программы используют системные механизмы для того, чтобы программы, написанные одними пользователями, могли исполняться другими пользователями.
Вход в ловушку (Trap Door) - использование логина или пароля, который позволяет избежать проверок, связанных с безопасностью.
Переполнение стека и буфера (Stack and Buffer Overflow) - использование ошибки в программе (переполнение стека или буферов в памяти) для обращения к памяти другого пользователя или процесса с целью нарушения ее целостности.

Системные угрозы (атаки)

Рассмотрим также некоторые типичные атаки, использующие уязвимости (vulnerabilities) в системных программах – ошибки и недочеты, дающие возможность организации атак.
Черви (Worms) – злонамеренные программы, использующие механизмы самовоспроизведения (размножения). Например, один из Интернет-червей использует сетевые возможности UNIX (удаленный доступ) и ошибки в программах finger и sendmail. Принцип его действия следующий: некоторая постоянно используемая в сети системная программа распространяет главную программу червя.
Вирусы – фрагменты кода, встраивающиеся в обычные программы с целью нарушения работоспособности этих программ и всей компьютерной системы. В основном вирусы действуют на микрокомпьютерные системы. Вирусы скачиваются с публично доступных сайтов или с дисков, содержащих "инфекцию". Для предотвращения заражения компьютерными вирусами необходимо соблюдать принципы безопасности при использовании компьютеров (safe computing) – использовать антивирусы, guards – программы, постоянно находящиеся в памяти и проверяющие на вирусы каждый открываемый файл - .exe, doc, и т.д.
Отказ в обслуживании (Denial of Service – DoS) – одна из распространенных разновидностей атак на сервер, заключающаяся в создании искусственной перегрузки сервера с целью препятствовать его нормальной работе. Например, для Web-сервера такая атака может заключаться в том, чтобы искусственно сгенерировать миллион запросов "GET". Если сервер реализован не вполне надежно, подобная атакачаще всего приводит к переполнению памяти на сервере и необходимости его перезапуска.

Типы сетевых атак

Рассмотрим некоторые типы современных сетевых атак, которых необходимо постоянно остерегаться пользователям.
Phishing – попытка украсть конфиденциальную информацию пользователя путем ее обманного получения от самого пользователя. Даже само слово phishing – искаженное слово fishing (рыбная ловля), т.е. хакер с помощью этого приема как бы пытается поймать чересчур наивного пользователя "на удочку". Например, напугав в своем сообщении пользователя, что его логин и пароль, кредитная карта или банковский счет под угрозой, хакер пытается добиться от пользователя в ответ ввода и отправки некоторой конфиденциальной информации. Обычно phishing-сообщение по электронной почте приходит как бы от имени банка и подделывается под цвета, логотипы и т.д., используемые на сайте банка. Однако для его разоблачения обычно достаточно подвести курсор мыши (не кликая ее) к приведенной web-ссылке или email-адресу (при этом она высвечивается) и убедиться в том, что адрес указывает отнюдь не на банк, а на совершенно посторонний сайт или email. Поэтому пользователям не следует быть слишком наивными. Другая действенная мера, если phishingпроисходит регулярно с одних и тех же email-адресов, - включить эти адреса в черный список на email-сервере. Тогда подобные сообщения вообще не будут доходить до входного почтового ящика пользователя.
Pharming – перенаправление пользователя на злонамеренный Web-сайт (обычно с целью phishing). Меры предотвращения со стороны пользователя мы уже рассмотрели. В современные web-браузеры встроены программы антифишингового контроля, которые запускаются автоматически при обращении к сайту. Хотя это отнимает у пользователя некоторое время, подобные меры помогают предотвратить многие атаки.
Tampering with data – злонамеренное искажение или порча данных. Действенной мерой по борьбе с подобными атаками являетсякриптование информации.
Spoofing – " подделка" под определенного пользователя (злонамеренное применение его логина, пароля и полномочий). Логин и парольпри этом либо получены от пользователя обманным путем (например, в результате phishing), либо извлечены из "взломанного" хакерской программой системного файла.
Elevation of privilege – попытка расширить полномочия (например, до полномочий системного администратора) с целью злонамеренных действий. Поэтому наиболее секретная информация в любой компьютерной системе – пароль системного администратора, который необходимо защищать особенно тщательно.

1. 23-27 Лекция № 23-26 (8 часов).

Тема: «Цифровая подпись. Процедура оформления подписи и проверка»

1.23-27.1 Вопросы лекции:

1. Основы формирования цифровой подписи.
2. Методы передачи цифровой подписи.

1.23-27.2 Краткое содержание вопросов:

1. Основы формирования цифровой подписи.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом

связана с такой информацией и которая используется для определения лица, подписывающего информацию;

[Электронная] цифровая подпись (digital signature): Строка бит, полученная в результате процесса формирования подписи. Данная строка имеет внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

Общая суть электронной подписи заключается в следующем. С помощью криптографической хэш-функции на основании документа вычисляется относительно короткая строка символов фиксированной длины (хэш). Затем этот хэш шифруется закрытым ключом владельца — результатом является подпись документа. Подпись прикладывается к документу, таким образом получается подписанный документ. Лицо, желающее установить подлинность документа, расшифровывает подпись открытым ключом владельца, а также вычисляет хэш документа. Документ считается подлинным, если вычисленный по документу хэш совпадает с расшифрованным из подписи, в противном случае документ является подделанным.
Принципы использования электронной подписи:
Принципами использования электронной подписи являются:

- право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;
- возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования Федерального закона №63 «Об электронной подписи» применительно к использованию конкретных видов электронных подписей;
- недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Виды электронных подписей:
Видами электронных подписей, отношения в области использования которых регулируются Федеральным законом №63 «Об электронной подписи», являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

1. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
2. Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

3. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом №63 «Об электронной подписи».

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью:

1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.
2. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны соответствовать требованиям статьи 9 настоящего Федерального закона.
3. Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.
4. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

2. Методы передачи цифровой подписи.

Шифрование передаваемых через Интернет данных позволяет защитить их от посторонних лиц. Однако для полной безопасности должна быть уверенность в том, что второй участник транзакции является тем лицом, за которое он себя выдает. В бизнесе наиболее важным идентификатором личности заказчика является его подпись. В электронной коммерции применяется электронный эквивалент традиционной подписи — цифровая подпись . С ее помощью можно доказать не только то, что транзакция была инициирована определенным источником, но и то, что информация не была испорчена во время передачи.

Как и в шифровании, технология электронной подписи использует либо секретный ключ (в этом случае оба участника сделки применяют один и тот же ключ), либо открытый ключ (при этом требуется пара ключей — открытый и личный). И в данном случае более просты в использовании и более популярны методы с открытым ключом (такие, как RSA)

Хэш-функции являются одним из важных элементов криптосистем на основе ключей и используются для обнаружения факта модификации сообщения, то есть для электронной подписи. Их относительно легко вычислить, но почти невозможно расшифровать. Хэш-функция имеет исходные данные переменной длины и возвращает строку (иногда называемую дайджестом сообщения — MD) фиксированного размера, обычно 128 бит.

Существует несколько защищенных хэш-функций: Message Digest 5 (MD-5), Secure Hash Algorithm (SHA) и др. Они гарантируют, что разные документы будут иметь разные электронные подписи, и что даже самые незначительные изменения документа вызовут изменение его дайджеста.

Рассмотрим, как работает технология цифровой подписи, использующая алгоритм RSA. Предположим, вы хотите послать сообщение. В этом случае порядок работы следующий:
1. При помощи хеш-функции вы получаете дайджест — уникальным образом сжатый вариант исходного текста.
2. Получив дайджест сообщения, вы шифруете его с помощью личного ключа RSA, и дайджест превращается в цифровую подпись.
3. Вы посылаете вместе с самим сообщением цифровую подпись.
4. Получив послание, получатель расшифровывает цифровую подпись с помощью вашего открытого ключа и извлекает дайджест сообщения.
5. Получатель, применяя для сообщения ту же хэш-функцию, что и вы, получает свой сжатый вариант текста и сравнивает его с дайджестом, восстановленным из подписи. Если они совпадают, то это значит, что подпись правильная и сообщение действительно поступило от вас. В противном случае сообщение либо отправлено из другого источника, либо было изменено после создания подписи.

При аутентификации личности отправителя открытый и личный ключи играют роли, противоположные тем, что они выполняли при шифровании. Так, в технологии шифрования открытый ключ используется для зашифровки, а личный — для расшифровки. При аутентификации с помощью подписи все наоборот. Кроме того, подпись гарантирует только целостность и подлинность сообщения, но не его защиту от посторонних глаз. Для этого предназначены алгоритмы шифрования. Например, стандартная технология проверки подлинности электронных документов DSS (Digital Signature Standard) применяется в США компаниями, работающими с государственными учреждениями. Однако у технологии RSA более широкие возможности в силу того, что она служит как для генерации подписи, так и для шифрования самого сообщения. Цифровая подпись позволяет проверить подлинность личности отправителя: она основана

на использовании личного ключа автора сообщения и обеспечивает самый высокий уровень сохранности информации.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

2.1 Лабораторная работа № 1 (2 часа).

Тема: «Функции операционных систем. Поколения операционных систем»

2.1.1 Цель работы: Познакомится с основными функциями операционных систем, а также с их поколениями.

2.1.2 Задание для работы:

1. Функции операционных систем.
2. Поколения операционных систем.

2.1.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.1.4 Описание (ход) работы:

Операционная система (operating system) – комплекс программ, предоставляющий пользователю удобную среду для работы с компьютерным оборудованием.

Операционная система позволяет запускать пользовательские программы; управляет всеми ресурсами компьютерной системы – процессором (процессорами), оперативной памятью, устройствами ввода вывода; обеспечивает долговременное хранение данных в виде файлов на устройствах внешней памяти; предоставляет доступ к компьютерным сетям.

Все компоненты можно разделить на два больших класса – программы или программное обеспечение (ПО, software) и оборудование илиаппаратное обеспечение (hardware). Программное обеспечение делится на прикладное, инструментальное и системное. Рассмотрим кратко каждый вид ПО.

Цель создания вычислительной системы – решение задач пользователя. Для решения определенного круга задач создается прикладнаяпрограмма (приложение, application). Примерами прикладных программ являются текстовые редакторы и процессоры (Блокнот, MicrosoftWord), графические редакторы (Paint, Microsoft Visio), электронные таблицы (Microsoft Excel), системы управления базами данных (Microsoft Access, Microsoft SQL Server), браузеры (Internet Explorer) и т. п. Все множество прикладных программ называется прикладным программным обеспечением (application software).

Создается программное обеспечение при помощи разнообразных средств программирования (среды разработки, компиляторы, отладчики и т. д.), совокупность которых называется инструментальным программным обеспечением. Представителем инструментального ПО являетсясреда разработки Microsoft Visual Studio.

Основным видом системного программного обеспечения являются операционные системы. Их основная задача – обеспечить интерфейс(способ взаимодействия) между пользователем и приложениями с одной стороны, и аппаратным обеспечением с другой. К системному ПОотносятся также системные утилиты – программы, которые выполняют строго определенную функцию по обслуживанию вычислительной системы, например,

диагностируют состояние системы, выполняют дефрагментацию файлов на диске, осуществляют сжатие (архивирование) данных. Утилиты могут входить в состав операционной системы.

Взаимодействие всех программ с операционной системой осуществляется при помощи системных вызовов (system calls) – запросов программ на выполнение операционной системой необходимых действий. Набор системных вызовов образует API – Application Programming Interface(интерфейс прикладного программирования).

Далее рассмотрим, какие функции должны выполнять современные операционные системы.

К основным функциям, выполняемым операционными системами, можно отнести:

- обеспечение выполнения программ – загрузка программ в память, предоставление программам процессорного времени, обработка системных вызовов;
- управление оперативной памятью – эффективное выделение памяти программам, учет свободной и занятой памяти;
- управление внешней памятью – поддержка различных файловых систем;
- управление вводом-выводом – обеспечение работы с различными периферийными устройствами;
- предоставление пользовательского интерфейса;
- обеспечение безопасности – защита информации и других ресурсов системы от несанкционированного использования;
- организация сетевого взаимодействия.

Поколения операционных систем.

40-е годы XX века.

Первые ЭВМ были построены на основе электронных ламп. Они не были предназначены для практических целей. Одни и те же люди проектировали эти машины, писали для них программы и их эксплуатировали. Первые электронные ЭВМ не имели ОС. Функции ОС включались в состав прикладных программ.

Первое поколение ОС.

50-е годы XXв.

Первое поколение ОС было создано для ЭВМ, построенных на полупроводниковых транзисторах. Такие ЭВМ могли работать более длительное время без ошибок и сбоев. Машинное время их стоило очень дорого, поэтому одной из основных функций первых

ОС была организация пакетного режима работы. Этот режим позволял сокращать время простоя при переходе от решения одной задачи к другой.

Второе поколение ОС.

Середина 60-х г.

Это поколение ОС было связано с ЭВМ, построенными на основе модулей и первых интегральных схем. Стали появляться ЭВМ с несколькими CPU. ОС для таких машин должны были обладать способностями управлять работой нескольких процессоров, иметь многозадачный режим работы, а так же, обладать возможностью работы с несколькими пользователями. Это были системы коллективного пользования.

На многопроцессорной ЭВМ задача разбивалась на несколько частей, и эти часть параллельно выполнялись на отдельных процессорах, что позволяло резко увеличить вычислительную мощность. Мультипрограммный режим работы заключался в том, что в память ЭВМ загружалось одновременно несколько задач, ОС при этом выделяла процессор каждой задаче на определенное время, автоматически переключая его между всеми задачами.

Режим коллективного пользования заключался в том, что
к вычислит.машине подключалось несколько терминалов (монитор и клавиатура), за которыми работали отдельные пользователи. ОС с большей скоростью переключала терминалы, и у каждого пользователя создавалось впечатление, что он один работает с ВМ.

ОС реального времени использовались в ВМ, которые управляли какими-либо машинами или устройствами. Как правило, скорость реакции устройства меньше скорости реакции ЭВМ, ОС реального времени искусственно замедляли работу ЭВМ, приближая ее к скорости устройства или машины.

Третье поколение ОС.

70-е годы XXв.

Это поколение ОС предназначалось для ВМ, построенных на основе интегральных схем, как ЭВМ общего пользования. ЭВМ впервые стали использоваться в промышленности, медицине и т.д.

Появилось большое количество различных типов ЭВМ. Наиболее известным компьютером этого поколения был IBM PC 360. ОС третьего поколения должны были работать на разных типах машин, а, кроме того, должны быть многорежимными, т.е., поддерживать пакетный режим, многозадачный, многопроцессорный и т.д. ОС были громоздкими и сложными, часто содержали большое количество ошибок. Для эксплуатации таких ОС нужна была спецподготовка. Оператору ЭВМ приходилось изучать сложные языки управления задачами.

Но именно в этот период были заложены все основные черты современных ОС.

Четвертое поколение ОС.

80-е годы XXв.

Это поколение связано в первую очередь с ЭВМ на основе больших и сверхбольших интегральных микросхем. Основными классами ЭВМ этого поколения являются ЭВМ общего пользования, мини и микро ЭВМ, персональные ЭВМ и суперЭВМ (многопроцессорные).

Это поколение включает в себя все основные черты ОС предыдущих поколений, а так же имеют следующие особенности:

5. Управление работой сетей ЭВМ.
6. Управление работой сложных многопроцессорных вычислительных комплексов.
7. Появление ОС ПК.
8. ОС начали использовать «дружественный» интерфейс, т.е. ОС строятся в расчете на не подготовленных или малоподготовленных пользователей.

2.2 Лабораторная работа № 2 (2 часа).

Тема: «Назначение, возможности систем клона UNIX, систем группы Windows»

2.2.1 Цель работы: Познакомится с назначением и возможностями операционной системы Linux, а также операционными системами семейства Windows.

2.2.2 Задание для работы:

1.Классификация ОС.
2.Общая характеристика ОС Windows, UNIX.

2.2.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.2.4 Описание (ход) работы:

Операционные системы классифицируются по:

- количеству одновременно работающих пользователей: однопользовательские, многопользовательские;
- числу процессов, одновременно выполняемых под управлением системы: однозадачные, многозадачные;
- количеству поддерживаемых процессоров: однопроцессорные, многопроцессорные;
- разрядности кода ОС: 8-разрядные, 16-разрядные, 32-разрядные, 64-разрядные;
- типу интерфейса: командные (текстовые) и объектно-ориентированные (графические);
- типу доступа пользователя к ЭВМ: с пакетной обработкой, с разделением времени, реального времени;
- типу использования ресурсов: сетевые, локальные.

В соответствии с первым признаком классификации многопользовательские операционные системы, в отличие от однопользовательских, поддерживают одновременную работу на ЭВМ нескольких пользователей за различными терминалами.

Второй признак предполагает деление ОС на многозадачные и однозадачные. Понятие многозадачности означает поддержку параллельного выполнения нескольких

программ, существующих в рамках одной вычислительной системы, в один момент времени. Однозадачные ОС поддерживают режим выполнения только одной программы в отдельный момент времени.

В соответствии с третьим признаком многопроцессорные ОС, в отличие от однопроцессорных, поддерживают режим распределения ресурсов нескольких процессоров для решения той или иной задачи.

Четвертый признак подразделяет операционные системы на 8-, 16-, 32- и 64-разрядные. При этом подразумевается, что разрядность операционной системы не может превышать разрядности процессора.

В соответствии с пятым признаком ОС по типу пользовательского интерфейса делятся на объектно-ориентированные (как правило, с графическим интерфейсом) и командные (с текстовым интерфейсом). Согласно шестому признаку ОС подразделяются на системы:

- пакетной обработки, в которых из программ, подлежащих выполнению, формируется пакет (набор) заданий, вводимых в ЭВМ и выполняемых в порядке очередности с возможным учетом приоритетности;
- разделения времени (TSR), обеспечивающих одновременный диалоговый (интерактивный) режим доступа к ЭВМ нескольких пользователей на раз¬ных терминалах, которым по очереди выделяются ресурсы машины, что координируется операционной системой в соответствии с заданной дисциплиной обслуживания;
- реального времени, обеспечивающих определенное гарантированное время ответа машины на запрос пользователя с управлением им какими-либо внешними но отношению к ЭВМ событиями, процессами или объектами.

В соответствии с седьмым признаком классификации ОС делятся на сетевые и локальные. Сетевые ОС предназначены для управления ресурсами компьютеров, объединенных в сеть с целью совместного использования данных, и предоставляют мощные средства разграничения доступа к данным в рамках обеспечения их целостности и сохранности, а также множество сервисных возможностей по использованию сетевых ресурсов.

В большинстве случаев сетевые операционные системы устанавливаются на один или более достаточно мощных компьютеров-серверов, выделяемых исключительно для обслуживания сети и совместно используемых ресурсов. Все остальные ОС будут считаться локальными и могут использоваться на любом персональном компьютере, а также на отдельном компьютере, подключенном к сети в качестве рабочей станции или клиента.

В настоящее время распространены следующие семейства операционных систем: DOS; OS/2; UNIX; Windows; ОС реального времени.

Основные критерии подхода к выбору операционной системы:

В настоящее время имеется большое количество операционных систем, и перед пользователем стоит задача определить, какая операционная система лучше других (по тем или иным критериям). Очевидно, что идеальных систем не бывает, любая из них имеет свои достоинства и недостатки. Выбирая операционную систему, пользователь должен представлять, насколько та или иная ОС обеспечит ему решение его задач.

Чтобы выбрать ту или иную ОС, необходимо знать:

- на каких аппаратных платформах и с какой скоростью работает ОС;
- какое периферийное аппаратное обеспечение ОС поддерживает;
- как полно удовлетворяет ОС потребности пользователя, то есть каковы функции системы;

- каков способ взаимодействия ОС с пользователем, то есть насколько нагляден, удобен, понятен и привычен пользователю интерфейс;
- существуют ли информативные подсказки, встроенные справочники и т. д.;
- какова надежность системы, то есть ее устойчивость к ошибкам пользователя, отказам оборудования и т. д.;
- какие возможности предоставляет ОС для организации сетей;
- обеспечивает ли ОС совместимость с другими операционными системами;
- какие инструментальные средства имеет ОС для разработки прикладных программ;
- осуществляется ли в ОС поддержка различных национальных языков;
- какие известные пакеты прикладных программ можно использовать при работе с данной системой;
- как осуществляется в ОС защита информации и самой системы.

ОС UNIX является удачной реализацией многопользовательской и многозадачной ОС. Она спроектирована как инструменталь-ная система для разработки программного обеспечения. Система UNIX обладает простым, но очень мощным командным языком и независимой от устройств файловой системой. Системы и приложения, выполняющиеся в ней, легко переносимы.

При создании ОС UNIX имелось три цели:
1.) стремление сохранить простоту и обойтись минимальным количеством функций.

2.) использование общих механизмов во множестве случаев, например при обраще-нии к файлам, прерываниях, именовании и др.;

3.) предоставление возможности решать большие задачи, комбинируя более мелкие.

Процесс может выполняться в одном из двух состояний – пользовательском или систем-ном.
В пользовательском состоянии процесс выполняет пользовательскую программу и имеет доступ к пользовательскому сегменту данных.

В системном состоянии процесс выполняет программы ядра и имеет доступ к системному сегменту данных.

В UNIX-системах используется разделение времени, то есть каждому процессу выделяется квант времени. Процесс либо завершается сам до истечения отведенного ему кванта времени, либо он откладывается по истечении кванта. Чем меньше отведенное процессу время – тем выше его приоритет. Все системные процессы имеют более высокие приоритеты по сравнению с пользовательскими и поэтому всегда обслуживаются в первую очередь.

Linux – это современная POSIX-совмести-мая и UNIX-подобная ОС для ПК и рабочих станций.
Изначально Linux создавался как самодель-ная UNIX-подобная реализация для ПК типа IBM PC с процессором i80386. Однако Linux стал настолько популярен и его на сегодня-шний день поддерживает такое большое число компаний, что в настоящее время имеется

реализация этой ОС практически для всех типов процессоров и компьютеров на их основе.
Ядро Linux сразу было создано с учетом возможностей защищенного режима процессоров Intel 80386 и 80486. В частно-сти, Linux использует парадигму описания памяти в защищенном режиме и другие новые свойства процессоров. В настоящее время имеются ядра для этой системы, оптимизированные для работы с процесс-сорами Intel и AMD последнего поколения, хотя основные архитектурные особенности защищенного режима работы изменились мало.

2.3 Лабораторная работа № 3 (2 часа).

Тема: «Управление ресурсами»

2.3.1 Цель работы: Познакомится с основами управления ресурсов, методами и способами их взаимодействия и использования.

2.3.2 Задание для работы:

1. Управление процессорами.
2.Управление памятью.

2.3.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.3.4 Описание (ход) работы:

Основные задачи управления процессором сводятся к решению двух взаимосвязанных проблем:
 Создание условий, при которых каждый процесс и приложение получат достаточную часть рабочего времени процессора, чтобы обеспечивалось их нормальное функционирование

 Использование стольких циклов процессора, сколько возможно для нормальной работы.

Основной единицей программного обеспечения, с которой операционная система работает при планировании работы процессора, является либо процесс, либо поток, в зависимости от операционной системы.

Было бы заманчиво рассматривать процесс как приложение, однако такой подход дает неполную картину того, какая устанавливается взаимосвязь процессов с операционной системой и аппаратными средствами. Видимое пользователем приложение (текстовый редактор, электронная таблица или игра) действительно является процессом, однако это приложение может инициировать запуск некоторых других процессов для решения таких задач, как связь с другими устройствами или компьютерами. Имеется также большое число процессов, которые протекают, не проявляя себя. Например, в Windows XP и UNIX могут быть десятки фоновых процессов, предназначенных для управления сетью, памятью и дисками, проверки на наличие вирусов и т.д.

Таким образом, процесс – это программа, выполняющая определенное действие, и которой можно управлять – силами пользователя, с помощью других приложений или с

помощью операционной системы.

Операционная система осуществляет контроль и планирует выполнение центральным процессором процессов, а не приложений. В однозадачной системе планирование выполнения простое. Операционная система разрешает приложению запуститься, временно приостанавливая его выполнение на достаточно длительное время лишь в случае необходимости обслуживания прерываний и пользовательского ввода данных.

Прерывания – специальные сигналы, отправляемые на центральный процессор аппаратными средствами или программами. Это похоже на то, как если бы во время оживленного собрания какая-то часть компьютера вдруг подняла руку, требуя к себе внимания центрального процессора. Иногда операционная система устанавливает приоритеты процессов таким образом, что прерывания маскируются, то есть операционная система игнорирует прерывания от некоторых источников, чтобы определенная операция была завершена как можно скорее. Существуют некоторые прерывания (например, вызванные состоянием ошибки или проблемами с памятью), которые настолько важны, что их нельзя игнорировать. Эти немаскируемые прерывания (non-maskable interrupts, NMIs) требуют немедленного решения проблемы, несмотря на то, что должны выполняться другие задачи.

Учитывая, что прерывания создают определенные сложности при выполнении процессов даже в однозадачной системе, функционирование операционной системы становится намного более сложным в многозадачной системе. В последнем случае операционная система должна организовать выполнение приложений таким образом, чтобы создавалось впечатление, что определенные события происходят одновременно. Это сложно осуществить, поскольку центральный процессор в каждый момент времени может делать только одну операцию. Современные многоядерные процессоры и многопроцессорные компьютеры могут выполнять по нескольку операций одновременно, однако каждое ядро процессора, как и прежде, в каждый момент времени может делать только одну операцию.

Чтобы создавалось впечатление, что множество событий происходит одновременно, операционная система должна осуществлять переключение между разными процессами тысячи раз в секунду. Это делается следующим образом:

 Процесс занимает определенную часть оперативной памяти. Кроме того, он использует регистры, стеки и очереди в центральном процессоре, а также в пространстве памяти операционной системы.

 Допустим, имеется два многозадачных процесса. Операционная система выделяет на каждую программу по определенному количеству исполнительных циклов.

 После прохождения этого количества циклов операционная система делает копии всех регистров, стеков и очередей, использовавшихся в процессах, и отмечает место, на котором наступила пауза выполнения процесса.

 Затем производится загрузка всех регистров, стеков и очередей, используемых вторым процессом, и этому процессу разрешается прохождение определенного количества циклов центрального компьютера.

 По завершении этих циклов делаются копии всех регистров, стеков и очередей, использовавшихся второй программой, и производится загрузка первой программы. .

Основная (или как ее принято называть в отечественной литературе и документации, оперативная) память всегда была и остается до сих пор наиболее критическим ресурсом компьютеров. Если учесть, что большинство современных компьютеров обеспечивает 32-разрядную адресацию в пользовательских программах, и все большую силу набирает новое поколение 64-разрядных компьютеров, то становится понятным, что практически безнадежно рассчитывать, что когда-нибудь удастся оснастить компьютеры основной памятью такого объема, чтобы ее хватило для выполнения произвольной пользовательской программы, не говоря уже об обеспечении мультипрограммного режима, когда в основной памяти, вообще говоря, могут одновременно содержаться несколько пользовательских программ.

Поэтому всегда первичной функцией всех операционных систем (более точно, операционных систем, обеспечивающих режим мультипрограммирования) было обеспечение разделения основной памяти между конкурирующими пользовательскими процессами. Мы не будем здесь слишком сильно вдаваться в историю этого вопроса. Заметим лишь, что применявшаяся техника распространяется от статического распределения памяти (каждый процесс пользователя должен полностью поместиться в основной памяти, и система принимает к обслуживанию дополнительные пользовательские процессы до тех пор, пока все они одновременно помещаются в основной памяти), с промежуточным решением в виде "простого своппинга" (система по-прежнему располагает каждый процесс в основной памяти целиком, но иногда на основании некоторого критерия целиком сбрасывает образ некоторого процесса из основной памяти во внешнюю память и заменяет его в основной памяти образом некоторого другого процесса), до смешанных стратегий, основанных на использовании "страничной подкачки по требованию" и развитых механизмов своппинга.

Операционная система UNIX начинала свое существование с применения очень простых методов управления памятью (простой своппинг), но в современных вариантах системы для управления памятью применяется весьма изощренная техника.

Поэтому в таких случаях используется техника копирования страниц при попытке записи. Несмотря на то, что в сегмент запись разрешена, для каждой его страницы устанавливается блокировка записи. Тем самым, во время попытки выполнения записи возникает прерывание, и ОС на основе анализа статуса соответствующего сегмента принимает решение о выделении новой страницы, копировании на нее содержимого оригинальной страницы и о включении этой новой страницы на место старой в виртуальную память либо процесса-предка, либо процесса-потомка (в зависимости от того, кто из них пытался писать).

На этом мы заканчиваем краткое описание механизма управления виртуальной памятью в ОС UNIX. Еще раз подчеркнем, что мы опустили множество важных технических деталей, стремясь продемонстрировать наиболее важные принципиальные решения.

2.4 Лабораторная работа № 4 (2 часа).

Тема: «Доменная политика конфигураций безопасности. Конфигурирование безопасности в Windows NT»

2.4.1 Цель работы: Познакомится с понятиями и особенностями доменной политики безопасности и конфигурированием безопасности в Windows NT.

2.4.2 Задание для работы:

1. Доменная политика конфигураций безопасности.
2. Основы безопасности в Windows NT

2.4.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.4.4 Описание (ход) работы:

Подробные политики паролей можно использовать для определения нескольких политик паролей в одном домене. С помощью подробных политик паролей можно применять различные ограничения политик паролей и блокировки учетных записей к разным группам пользователей в домене.
Например, можно применить более строгие параметры к привилегированным учетным записям и менее строгие – к учетным записям других пользователей. Может также возникнуть необходимость применения особой политики паролей к тем учетным записям, пароли которых синхронизируются с другими источниками данных.

Подробные политики паролей применимы только к объектам пользователей (или объектам inetOrgPerson, если они используются вместо объектов пользователей) и глобальным группам безопасности. По умолчанию задавать подробные политики паролей могут только члены группы администраторов домена. Однако возможность задавать эти политики можно также делегировать другим пользователям. Домен должен работать в режиме Windows Server 2008.
Подробную политику паролей нельзя применить непосредственно к подразделению. Для применения подробной политики паролей к пользователям из подразделения можно использовать теневую группу.
Теневая группа – это глобальная группа безопасности, которая логически сопоставляется с подразделением для принудительного применения подробной политики паролей. После добавления пользователей подразделения в созданную теневую группу к ней можно применить подробную политику паролей. Для других подразделений можно по мере необходимости создавать дополнительные теневые группы. При перемещении пользователя из одного подразделения в другое необходимо обновлять его членство в соответствующих теневых группах.
В одном домене допускается использование подробных политик паролей одновременно с настраиваемыми фильтрами паролей. Если на контроллерах домена с Windows 2000 или Windows Server 2003 развернуты настраиваемые фильтры паролей, их можно использовать и в дальнейшем в целях обеспечения дополнительных ограничений для паролей.

Объекту пользователя или группы может быть привязано несколько объектов параметров паролей. Такая ситуация имеет место в случае, если этот объект является членом

нескольких групп, к которым привязаны различные объекты параметров паролей, либо в случае, когда несколько объектов параметров паролей привязаны к этому объекту напрямую. Однако только один объект параметров паролей может быть применен в качестве действующей политики паролей. Только параметры этого объекта параметров паролей будут оказывать влияние на пользователя или группу. Слияние с параметрами других объектов параметров паролей, привязанных к этому пользователю или группе, невозможно.
Результирующая политика может быть определена только для объекта пользователя. Объект параметров паролей может быть применен к объекту пользователя двумя способами, указанными ниже.

3. Непосредственно: объект параметров паролей связывается с пользователем.

4. Косвенно: объект параметров паролей связывается с группами, членом которых является пользователь.

По умолчанию объекты параметров паролей могут создавать только члены группы администраторов домена. Только члены этой группы имеют разрешения "Создать дочерний" и "Удалить дочерний" на объект контейнера параметров паролей. Кроме того, только члены группы "Администраторы домена" по умолчанию имеют разрешение "Записать свойство" на объект параметров паролей. Поэтому только члены данной группы могут привязать объект параметров паролей к группе или пользователю. Это разрешение можно делегировать другим группам или пользователям.
Чтобы применить объект параметров паролей к объекту пользователя или группы, разрешения на работу с ними не требуются. Разрешения на запись объекта пользователя или группы не позволяют связать объект параметров паролей с пользователем или группой. Владелец группы не имеет разрешений на связывание объекта параметров паролей с группой, поскольку прямая ссылка содержится в объекте параметров паролей. Возможность связывания объекта параметров паролей с группой или пользователем имеется у владельца объекта параметров паролей.
Параметры объекта параметров паролей можно считать конфиденциальными; таким образом, по умолчанию пользователи, прошедшие проверку подлинности, не имеют разрешений "Чтение свойства" для объекта параметров паролей. По умолчанию только члены группы администраторов домена имеют эти разрешения для используемого по умолчанию дескриптора безопасности объекта параметров паролей в схеме.

Модель безопасности Windows NT базируется на концепции пользовательских бюджетов (user accounts). Можно создать неограниченное количество пользовательских бюджетов и сгруппировать их наиболее удобным методом. После этого для каждого бюджета или группы можно представить или ограничить доступ к любому из ресурсов компьютера.

В операционную систему Windows NT встроена возможность аудита. Это позволяет отслеживать, какие пользовательские бюджеты использовались для доступа в систему, и какого типа доступ к файлам и другим объектам был получен пользователями. Кроме того, аудит может использоваться для отслеживания попыток входа в систему, остановки и перезапуска системы и прочих аналогичных событий.

Модель безопасности Windows NT содержит следующие компоненты:

- Процессы входа в систему (Logon processes), принимающие от пользователей на регистрацию в системе. Сюда относятся начальный интерактивный процесс регистрации, отображающий диалоговое окно входа в систему, и процесс удаленной регистрации,

позволяющий удаленным пользователям получить доступ к серверу Windows NT.

- Распорядитель локальной безопасности (Local Security Authority, LSA), гарантирующий, что каждый пользователь, регистрирующийся в системе, имеет право доступа к ней. Этот компонент является центральным для всей подсистемы безопасности Windows NT. Он создает маркеры безопасного доступа, управляет локальной политикой безопасности и обеспечивает интерактивный сервис аутентификации пользователей. Кроме того, LSA управляет политикой аудита и регистрирует сообщения аудита, генерируемые монитором безопасности (Security Reference Monitor).

- Диспетчер бюджетов безопасности (Security Accounts Monitor, SAM). Этот компонент поддерживает базу данных пользовательских бюджетов. База данных SAM содержит информацию обо всех пользовательских и групповых бюджетах. SAM обеспечивает сервис валидизации пользовательских паролей, используемый LSA. База данных SAM известна также под названием базы данных каталога (Directory Database).

- Монитор безопасности (Security Reference Monitor) - компонент системы безопасности, ответственный за проверку наличия у пользователей прав доступа к объектам и осуществления действий, которые они пытаются выполнить. Монитор безопасности принудительным образом устанавливает проверку прав доступа к объектам и устанавливает политику аудита заданную LSA. Монитор безопасности предоставляет сервис процессам, которые работают как в режиме ядра, так и в режиме пользователя. Это гарантирует, что все пользователи и процессы, пытающиеся получить доступ к объекту и выполнить над ним некоторые действия, обладают соответствующими правами доступа. Кроме того, монитор безопасности генерирует сообщения аудита в тех случаях, когда это необходимо.

Ключевой особенностью системы безопасности Windows NT является управление доступом к объектам. Модель безопасности поддерживает информацию защиты для каждого пользователя, группы и объекта. Она может идентифицировать попытки доступа, осуществленные непосредственно пользователем, а также способна выявлять непрямые попытки доступа, предпринятые не самим пользователем, а программой или иным процессом, действующими от лица пользователя. Windows NT отслеживает все попытки доступа и позволяет управлять доступом как к объектам, которые пользователи могут просматривать с помощью пользовательского интерфейса (например, файлам и принтерам), так и к абстрактным объектам, которые с помощью пользовательского интерфейса просмотреть нельзя (к ним относятся, например, процессы и именованные каналы).

Администратор системы присваивает пользователям и группам права доступа (permissions), с помощью которых можно предоставить или отклонить пользовательский доступ к объектам. Возможность избирательного присвоения прав доступа по усмотрению владельца объекта (или пользователя, уполномоченного изменять права доступа), называется избирательным контролем доступа (discretionary access control).

Система безопасности идентифицирует пользователей с помощью идентификатора безопасности (security ID, SID). Уникальность идентификаторов безопасности гарантирована, и существование двух идентичных SID полностью исключено. Когда пользователь регистрируется в системе, Windows NT создает маркер безопасности доступа (security access token). В состав маркера безопасного доступа входят SID пользователя, SID всех групп, к которым этот пользователь принадлежит, а также дополнительная информация о пользователе и его группах. Кроме того, любой процесс,

работающий от имени пользователя, получает копию его маркера безопасного доступа. Когда пользователь пытается получить доступ к объекту, Windows NT ссылается на содержащийся в маркере безопасного доступа SID. Идентификаторы безопасности (SID) сравниваются со списком контроля доступа к объекту, чтобы гарантировать, что пользователь имеет достаточные права.

Диапазон средств защиты файлов можно установить как на базе подхода "по файлам", так и на базе подхода "по каталогам". Чтобы воспользоваться всей властью над отдельными файлами, их следует расположить на томах с NTFS. Windows NT поддерживает для совместимости с MS DOS работу с FAT, но эта файловая система была разработана без учета требований безопасности. Чтобы воспользоваться всеми преимуществами защиты Windows NT, необходимо использовать файловую систему NTFS.

Системные принтеры можно защитить, не позволяя конкретным пользователям отправлять на них задания (постоянно или только в течение указанного времени суток).

2.5 Лабораторная работа № 5 (2 часа).

Тема: «Организация управления доступом и защиты ресурсов ОС»

2.5.1 Цель работы: Изучить элементы организации управления доступом к различным разделам операционной системы, а также изучить основные аспекты защиты операционной системы .

2.5.2 Задание для работы:

1. Основы защиты ОС.
2. Практические методы защиты.

2.5.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.5.4 Описание (ход) работы:

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.

Есть несколько простых правил, соблюдая которые, можно не беспокоиться о своей безопасности:

Скачивать программы можно ТОЛЬКО из надежных источников и как можно меньше со всяческих якобы "хакерских" сайтов... Львиная доля Троянов приходится именно на файлы с этих серверов.

Если скачали какую-то программу - ОБЯЗАТЕЛЬНО необходимо проверить ее на наличие вирусов и других вредоносных программ.

Никогда не надо запускать программы, пришедшие по E-MAIL.

В качестве паролей надо всегда использовать замысловатые наборы символов, типа Jqp2FQs, и по возможности стараться их вводить в окне терминала вручную - это обезоружит Троянов, отсылающих пароли на чей-то E-MAIL адрес.

Следует ограничить число посторонних, имеющих доступ к компьютеру, поскольку достаточно большое число троянов и вирусов переносится на внешних носителях (дискетах и дисках). Также рекомендуется периодически менять пароли на особо важные аккаунты.

Те троянские программы, которые постоянно обеспечивают доступ к зараженной ЭВМ, а, следовательно, держат на ней открытый порт какого-либо транспортного протокола, можно обнаруживать с помощью утилит контроля за сетевыми портами. Например, для операционных систем клона Microsoft Windows такой утилитой является программа NetStat. Запуск ее с ключом "netstat - a" выведет на экран все активные порты ЭВМ. От оператора в этом случае требуется знать порты стандартных сервисов, которые постоянно открыты на ЭВМ, и тогда, любая новая запись на мониторе должна привлечь его внимание. На сегодняшний день существует уже несколько программных продуктов, производящих подобный контроль автоматически.

Ещё один способ обнаружить троянцев - посмотреть открытые порты компьютера и процессы, которые их открыли. Обычно троянская программа использует порты >1000 (например, 30003,47891,6666,31337). Список портов, использующихся троянскими программами - Приложение 1.

В Windows XP Professional SP2 есть встроенное средство защиты - брандмауэр Windows.

Брандмауэр (межсетевой экран или фаервол) - комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Брандмауэры бывают двух видов, программные и аппаратные.

Брандмауэр используется для защиты компьютера от несанкционированного доступа через сеть или Интернет. Брандмауэр Windows встроен в Windows XP и включен автоматически для защиты компьютера от вирусов и других угроз безопасности. Брандмауэр отличается от антивирусного программного обеспечения, однако их совместная работа обеспечивает надежную защиту компьютера. Можно сказать, что брандмауэр охраняет окна и двери от проникновения неизвестных и нежелательных программ, в то время как антивирусное программное обеспечение предотвращает появление вирусов или других угроз безопасности, которые стремятся пробраться через парадный вход. В Microsoft Windows XP (SP2) брандмауэр Windows включен по умолчанию. Необязательно использовать именно брандмауэр Windows - можно установить и включить любой брандмауэр по выбору.

2.6 Лабораторная работа № 6 (2 часа).

Тема: «Разработка защищенных приложений. Программное управление файловыми ресурсами и сессиями»

2.6.1 Цель работы: Изучить теоретическую и практическую часть создания защищенных приложений, а также научиться грамотно управлять файловыми ресурсами и сессиями..

2.6.2 Задание для работы:

1. Методы разработки защищенных приложений.
2. Области применения.

2.6.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.6.4 Описание (ход) работы:

Основная часть уязвимостей появляется на ранних стадиях создания программного обеспечения. Поэтому, наибольшей эффективностью обладает подход, который устраняет проблемы безопасности на начальной стадии разработки приложений, нежели стандартный метод их исправления по необходимости. Консультанты моделируют потенциальные угрозы безопасности еще до создания программного продукта, что позволяет закрыть всевозможные бреши на стадии его разработки.

Глубокие знания процесса разработки прикладных приложений, позволяют им устранять существующие бреши в программном обеспечении, а также избежать потенциальных уязвимостей при создании собственного продукта.

Специалисты регулярно проводят проверку безопасности:

- сайтов интернет торговли, банков, финансовых и других учреждений;
- программного продукта для разработчиков, интернет-порталов и настольных систем.

Наша компания предлагает полный объем услуг по обеспечению информационной безопасности бизнес проектов, включая:

- оценка уязвимости встроенных систем;
- устранение брешей в системе предварительно записанных голосовых сообщений IVR;
- обнаружение «дыр» в настольных и мобильных приложениях, оценка величины рисков, практические рекомендации по их снижению;
- моделирование потенциальных угроз безопасности приложений, а также обнаружение и устранение их на ранней стадии разработки;
- определение уязвимостей, рисков, прочих угроз безопасности в инфраструктуре веб-подразделений организации;
- повышения уровня безопасности установленных приложений, проверка скриптов и исходного программного кода, устранение выявленных ошибок;
- оценка потенциальных способов проникновения хакеров в веб-приложение, обнаружение уязвимостей рабочих версий веб-порталов, определение степени коммерческих рисков и проведение консультаций по их снижению.

Как правило, при развертывании Web-приложения прежде всего требуется обеспечить, чтобы анонимные клиенты не могли обращаться к ценным ресурсам через интернет. Если приложение работает в интрасети, то для аутентификации клиентов обычно применяются средства Windows (подробнее об управлении доступом я расскажу чуть позже), а приложение защищается от внешнего доступа межсетевым экраном (брандмауэром). С интернет-приложениями дело обстоит сложнее, поскольку нужен хотя бы минимальный уровень доступа для анонимных пользователей, обращающихся через интернет. Если не принимать в расчет эти различия, можно руководствоваться следующими принципами, в равной мере применимыми к защите интернет-приложений и приложений интрасети. Идеальный вариант — в Web-пространстве имен вашего приложения не должно быть никаких файлов, которые не планируется передавать клиентам. То есть все такие файлы надо удалить из физической структуры каталогов, начинающейся с самого верхнего каталога, помеченного в конфигурации IIS как Web-приложение или виртуальный каталог. Если файл не принадлежит Web-пространству имен, он не будет доступен при запросах к этому пространству, если только ваше приложение не выполнит явные операции по открытию этого файла и передаче его содержимого. Если ваше приложение

программно обращается к данным или вспомогательным файлам, размещайте их вне Web-пространства имен.

Сферы применения:

- Установление защищенного удаленного доступа к внутренним информационным ресурсам организации: электронной почте, календарям сотрудников, адресной книге организации, внутренним порталам, библиотекам файлов и документов, системам управления совещаниями, спискам задач и др.
- Обеспечение юридически значимого электронного документооборота с применением сертифицированных средств криптографической защиты информации.
- Взаимодействие с площадками электронных торгов и аукционов, b2b услуг, госуслуг.
- Обеспечение конфиденциальности электронных почтовых сообщений.
- Обеспечение конфиденциальности информации, хранимой на мобильном устройстве.

2.7 Лабораторная работа № 7 (2 часа).

Тема: «Анализ симптома атаки и методы защиты»

2.7.1 Цель работы: Научиться анализировать ситуации, связанные с атаками на информацию, научиться противостоять этим атакам, а также предотвращать их в дальнейшем.

2.7.2 Задание для работы:

1. Симптомы атаки.
2. Виды атак.
3. Методы предотвращения.

2.7.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.7.4 Описание (ход) работы:

Существует ряд признаков, свидетельствующих о заражении компьютера. Если вы замечаете, что с компьютером происходят "странные" вещи, а именно:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- неожиданно открывается и закрывается лоток CD-ROM-устройства;
- произвольно, без Вашего участия, на вашем компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя Вы никак не инициировали такое ее поведение,

то, с большой степенью вероятности, можно предположить, что ваш компьютер поражен вирусом.

Кроме того, есть некоторые характерные признаки поражения вирусом через почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера. Существуют также косвенные признаки заражения компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- Microsoft Internet Explorer "зависает" или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуем вам:

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие может осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятельность. Для оценки типов атак необходимо знать некоторые ограничения, изначально присущие протоколу TPC/IP. Сеть Интернет создавалась для связи между государственными учреждениями и университетами в помощь учебному процессу и научным исследованиям. Создатели этой сети не подозревали, насколько широко она распространится. В результате, в спецификациях ранних версий интернет-протокола (IP) отсутствовали требования безопасности. Именно поэтому многие реализации IP являются изначально уязвимыми. Через много лет, получив множество рекламаций (RFC - Request for Comments), мы, наконец, стали внедрять средства безопасности для IP. Однако ввиду того, что изначально средства защиты для протокола IP не разрабатывались, все его реализации стали дополняться разнообразными сетевыми процедурами, услугами и продуктами, снижающими риски, присущие этому протоколу. Далее мы кратко обсудим типы атак, которые обычно применяются против сетей IP, и перечислим способы борьбы с ними.

Снифферы пакетов

Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним

ресурсам. Хакеры слишком хорошо знают и используют наши человеческие слабости (методы атак часто базируются на методах социальной инженерии). Они прекрасно знают, что мы пользуемся одним и тем же паролем для доступа к множеству ресурсов, и поэтому им часто удается, узнав наш пароль, получить доступ к важной информации. В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в сеть и к ее ресурсам.

IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример - атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения.

DoS, без всякого сомнения, является наиболее известной формой хакерских атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту. Даже среди хакеров атаки DoS считаются тривиальными, а их применение вызывает презрительные усмешки, потому что для организации DoS требуется минимум знаний и умений. Тем не менее, именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность. Если вы хотите побольше узнать об атаках DoS, вам следует рассмотреть их наиболее известные разновидности, а именно:

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS)) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть.

IDS всё чаще становятся необходимым дополнением инфраструктуры сетевой безопасности. В дополнение к межсетевым экранам (firewall), работа которых происходит на основе политики безопасности, IDS служат механизмами мониторинга и наблюдения подозрительной активности. Они могут обнаружить атакующих, которые обошли Firewall, и выдать отчет об этом администратору, который, в свою очередь, предпримет дальнейшие шаги по предотвращению атаки. Технологии обнаружения проникновений не делают систему абсолютно безопасной. Тем не менее практическая польза от IDS существует и не маленькая.

Использование IDS помогает достичь нескольких целей:

- Обнаружить вторжение или сетевую атаку;
- Спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития. Атакующий обычно выполняет ряд

предварительных действий, таких как, например, сетевое зондирование (сканирование) или другое тестирование для обнаружения уязвимостей целевой системы;

- Выполнить документирование существующих угроз;
- Обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;
- Получить полезную информацию о проникновениях, которые имели место, для восстановления и корректирования вызвавших проникновение факторов;
- Определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

Обычно IDS включает:

- Сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;
- Подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;
- Хранилище, в котором накапливаются первичные события и результаты анализа;
- Консоль управления, позволяющая конфигурировать IDS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты.

По способам мониторинга IDS системы подразделяются на *network-based (NIDS)* и *host-based (HIDS)*.

Основными коммерческими IDS являются *network-based*. Эти IDS определяют атаки, захватывая и анализируя сетевые пакеты. Слушая сетевой сегмент, NIDS может просматривать сетевой трафик от нескольких хостов, которые присоединены к сетевому сегменту, и таким образом защищать эти хосты.

2.8 Лабораторная работа № 8 (2 часа).

Тема: «Анализ установок безопасности системы»

2.8.1 Цель работы: Научиться анализировать стандартные установки безопасности системы, находить их недостатки и использовать преимущества.

2.8.2 Задание для работы:

1. Основные параметры защиты.
2. Характеристики установок безопасности.

2.8.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.8.4 Описание (ход) работы:

К процедурному уровню относятся меры безопасности, реализуемые сотрудниками предприятия. Выделяются следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;

- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

В рамках управления персоналом для каждой должности должны существовать квалификационные требования по информационной безопасности. В должностные инструкции должны входить разделы, касающиеся защиты информации. Каждого сотрудника предприятия необходимо обучить мерам обеспечения информационной безопасности теоретически и отработать выполнение этих мер практически.
Информационная безопасность ИС предприятия зависит от окружения, в котором она работает. Необходимо принять меры для обеспечения физической защиты зданий и прилегающей территории, поддерживающей инфраструктуры и самих компьютеров.
При разработке проекта СОИБ предполагается адекватная реализация мер физической защиты офисных зданий и других помещений, принадлежащих предприятию, по следующим направлениям:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры.

Предполагается также адекватная реализация следующих направлений поддержания работоспособности:

- поддержка пользователей ИС;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Программа информационной безопасности должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.
Реакция на нарушения режима информационной безопасности преследует две главные цели:

- блокирование нарушителя и уменьшение наносимого вреда;
- недопущение повторных нарушений.

На предприятии должен быть выделен сотрудник, доступный 24 часа в сутки, отвечающий за реакцию на нарушения. Все пользователи ИС должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В случае невозможности связи с данным сотрудником, должны быть разработаны и внедрены процедуры первичной реакции на информационный инцидент.
Планирование восстановительных работ позволяет подготовиться к авариям ИС, уменьшить ущерб от них и сохранить способность к функционированию, хотя бы в минимальном объеме.
Механизмы контроля, существенные для предприятия с юридической точки зрения, включают в себя:

- Защиту данных и тайну персональной информации;
- Охрану документов организации;
- Права на интеллектуальную собственность.

В соответствии с международным стандартом ISO 17799, а также руководящими документами ФСТЭК, ключевыми также являются следующие механизмы контроля:

- Политика информационной безопасности;
- Распределение ролей и ответственности за обеспечение информационной безопасности;
- Обучение и тренинги по информационной безопасности;

- Информирование об инцидентах безопасности;
- Управление непрерывностью бизнеса.

Меры обеспечения информационной безопасности программно-технического уровня
Программно-технические средства защиты располагаются на следующих рубежах:

- Защита внешнего периметра КСПД;
- Защита внутренних сетевых сервисов и информационных обменов;
- Защита серверов и рабочих станций;
- Защита системных ресурсов и локальных приложений на серверах и рабочих станциях;
- Защита выделенного сегмента руководства компании.

На программно-техническом уровне выполнение защитных функций ИС осуществляется следующими служебными сервисами обеспечения информационной безопасности:

- идентификация/аутентификация пользователей ИС;
- разграничение доступа объектов и субъектов информационного обмена;
- протоколирование/аудит действий легальных пользователей;
- экранирование информационных потоков и ресурсов КСПД;
- туннелирование информационных потоков;
- шифрование информационных потоков, критической информации;
- контроль целостности;
- контроль защищенности;
- управление СОИБ.

На внешнем рубеже информационного обмена располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они, вместе со средствами поддержки виртуальных частных сетей, объединяемых с межсетевыми экранами, образуют внешний периметр информационной безопасности, отделяющий информационную систему предприятия от внешнего мира.
Сервис активного аудита СОИБ (как и управление) должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить атаку, даже, если по каким-либо причинам, она окажется успешной.
Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу пользователя к ИС предприятия должна предшествовать идентификация и аутентификация субъектов информационного обмена (пользователей и процессов).
Средства шифрования и контроля целостности информации, передаваемой по каналам связи, целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование.
Последний рубеж образуют средства пассивного аудита, помогающие оценить последствия реализации угроз информационной безопасности, найти виновного, выяснить, почему успех атаки стал возможным.
Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов.

Установки безопасности ОС:

- препятствие;
- управление доступом;
- механизмы шифрования;
- противодействие атакам вредоносных программ;
- регламентация;
- принуждение;
- побуждение.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Управление доступом включает следующие функции зашиты:

· идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

· опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

· проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

· разрешение и создание условий работы в пределах установленного регламента;

· регистрацию (протоколирование) обращений к защищаемым ресурсам;

· реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

Принуждение – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на *аппаратные* и *физические*.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Как отмечалось, многие из них слиты с ПО самой ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем первого руководителя.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения (которые традиционно сложились ранее), складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например честность) либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения. Характерным примером таких предписаний является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

2.9 Лабораторная работа № 9 (2 часа).

Тема: «Основные механизмы безопасности: средства и методы аутентификации в ОС»

2.9.1 Цель работы: Изучить механизмы безопасности на основе средств и методов аутентификации в операционной системе.

2.9.2 Задание для работы:

1. Мотивации, как функция управления.
2. Необходимость контроля. Этапы контроля.

2.9.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.9.4 Описание (ход) работы:

Природа мотивации. Для достижения целей организации руководству необходимо обеспечить эффективные действия персонала. Для этого нужно не только обеспечить функциональную загрузку работников и создать им необходимые условия, но и вызвать у них желание энергично совершать именно те действия, которые приближают организации к достижению поставленных целей. В связи с этим руководство организации должно выполнять весьма важную функцию - создание условий для мотивации работников и осуществление ее на практике.

Мотивация как функция управления — это процесс, с помощью которого руководство организации побуждает работников действовать так, как было ранее запланировано и

организовано, поскольку успех организации в определенной мере зависит от того, насколько эффективно действуют участники производственного процесса. Таким образом, *мотивацию в организации* можно трактовать как *побуждение членов организации к действию.* При этом мотивация представляет собой, с одной стороны, побуждение, навязанное индивидам извне, а с другой — это самопобуждение.

Чтобы разобраться в этой двойственной природе мотивации, важно понять, что поведение человека в трудовом процессе определяется взаимодействием различных внешних и внутренних побудительных сил, среди которых следует прежде всего выделить стимулы и мотивы. Стимул понимается как внешняя причина, побуждающая людей к деятельности, а мотив выступает как внутренняя побудительная сила. Если стимул заметен, его можно заранее спланировать или отменить, то мотив скрыт, его действие часто бывает неожиданным для наблюдателей, так как он зависит от инстинктивных импульсов, влечений, потребностей.

Вместе с тем стимулы и мотивы самым тесным образом связаны между собой. Процесс стимулирования деятельности члена организации — это такое воздействие на его поведение, которое включает в свою сферу все потребности, интересы, цели, стремления, мотивы. Следовательно, основу стимулирования составляет взаимодействие внешних условий и внутренней структуры личности члена организации. Стимулирование реализуется через создание условий, изменяющих трудовую ситуацию, чтобы у работника возникало желание, стремление к эффективной деятельности. Однако для успешного стимулирования необходимо знать внутренние мотивы, которые можно приобрести, только изучая социологию и психологию личности.

Обращение к изучению поведения людей в организации обусловлено тем, что не всякое целевое, направленное воздействие на поведение человека активизирует его деятельность, а лишь то, которое становится личностно значимым для данного конкретного человека, соответствует его внутренним устремлениям. Только в этом случае возникает заинтересованность работника в своей деятельности, психологическая предрасположенность по отношению к выполнению ролевых требований и, как следствие этого, побуждение к качественному выполнению работы. Стимулирование включает в себя не только создание внешней ситуации выбора определенной (наиболее привлекательной) формы поведения, но и ее соответствие структуре личности работника. Вместе с внешней стимуляцией эта внутренняя структура (в случае ее активизации) формирует непосредственный мотив действий.

Контроль – это процесс, при помощи которого руководство организации определяет, правильные ли его решения и не нуждаются ли они в корректировке. Контроль – это процесс обеспечения достижения организацией своих целей.

Функция контроля – это такая характеристика управления, которая позволяет выявить проблемы и скорректировать деятельность организации до того, как эти проблемы перерастут в кризис. Сущность контроля заключается в трех основных элементах:

установление контролируемых стандартов деятельности;

измерение и анализ результатов деятельности, информация о которых получена с помощью контроля;

корректировка технологических, хозяйственных и иных процессов в соответствии со сделанными выводами и принятыми решениями.

Без надежной системы контроля ни одна организация не может успешно функционировать. Его задачи следующие.

Во-первых, контроль позволяет обнаружить во внешней или внутренней среде организации факторы, которые могут оказать существенное влияние на ее функционирование и развитие, и своевременно на них отреагировать.

Во-вторых, контроль помогает вскрыть неизбежные в деятельности любой организации нарушения, изъяны, ошибки и оперативно принять меры к их устранению.

В-третьих, результаты контроля служат основой для оценки работы организации и ее персонала за определенный период, эффективности и надежности системы управления ею.

Различают два основных вида контроля: финансовый и административный.

Различают три стадии управленческого контроля: предварительный, текущий и итоговый.

Предварительный контроль осуществляется до фактического начала работ в области человеческих ресурсы (анализ качеств, необходимых для выполнения работ), материальных ресурсов (стандарты качества, контроль за поступающими материалами), финансовых ресурсов (разработка бюджета, установление предельных значений затрат)

Текущий контроль осуществляется непосредственно в ходе выполнения работ, для этого необходим механизм обратной связи, который позволяет выявить непредвиденные проблемы и скорректировать линию поведения.

Оперативный контроль ориентирован на текущую производственную и хозяйственную деятельность, в частности на движение продукции в рамках технологического процесса (соблюдение последовательности операций, норм времени на их выполнение, качество труда); загрузку техники и оборудования; соблюдение общего графика работы.
Итоговый (заключительный) контроль связан с оценкой выполнения организацией планов и составлением новых; он предполагает всесторонний анализ не только конкретных результатов деятельности за текущий период, но и сильных и слабых ее сторон.
Заключительный контроль используется после выполнения работ и имеет две функции: дает информацию для планирования аналогичной продукции в будущем, способствует мотивации на основе измерения полученных результатов и определения степени вознаграждения.
Причины необходимости контроля.
1. Неопределенность - изменение законов, технологий, условий конкуренции приводят к необходимости к постоянной корректировки планов через систему обратной связи, которую обеспечивает контроль.
2. Предупреждение кризисных ситуаций - одно из главных назначений контроля - выявить проблемы и скорректировать деятельность организации до того, как эти проблемы перерастут в кризис

2.10 Лабораторная работа № 10 (2 часа).

Тема: «Назначение, возможности систем клона UNIX, систем группы Windows»

2.10.1 Цель работы: Познакомится с назначением и возможностями операционной системы Linux, а также операционными системами семейства Windows.

2.10.2 Задание для работы:

1.Классификация ОС.
2.Общая характеристика ОС Windows, UNIX.

2.10.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.10.4 Описание (ход) работы:

Операционные системы классифицируются по:

- количеству одновременно работающих пользователей: однопользовательские, многопользовательские;
- числу процессов, одновременно выполняемых под управлением системы: однозадачные, многозадачные;
- количеству поддерживаемых процессоров: однопроцессорные, многопроцессорные;
- разрядности кода ОС: 8-разрядные, 16-разрядные, 32-разрядные, 64-разрядные;
- типу интерфейса: командные (текстовые) и объектно-ориентированные (графические);
- типу доступа пользователя к ЭВМ: с пакетной обработкой, с разделением времени, реального времени;
- типу использования ресурсов: сетевые, локальные.

В соответствии с первым признаком классификации многопользовательские операционные системы, в отличие от однопользовательских, поддерживают одновременную работу на ЭВМ нескольких пользователей за различными терминалами.

Второй признак предполагает деление ОС на многозадачные и однозадачные. Понятие многозадачности означает поддержку параллельного выполнения нескольких программ, существующих в рамках одной вычислительной системы, в один момент времени. Однозадачные ОС поддерживают режим выполнения только одной программы в отдельный момент времени.

В соответствии с третьим признаком многопроцессорные ОС, в отличие от однопроцессорных, поддерживают режим распределения ресурсов нескольких процессоров для решения той или иной задачи.

Четвертый признак подразделяет операционные системы на 8-, 16-, 32- и 64-разрядные. При этом подразумевается, что разрядность операционной системы не может превышать разрядности процессора.

В соответствии с пятым признаком ОС по типу пользовательского интерфейса делятся на объектно-ориентированные (как правило, с графическим интерфейсом) и командные (с текстовым интерфейсом). Согласно шестому признаку ОС подразделяются на системы:

- пакетной обработки, в которых из программ, подлежащих выполнению, формируется пакет (набор) заданий, вводимых в ЭВМ и выполняемых в порядке очередности с возможным учетом приоритетности;
- разделения времени (TSR), обеспечивающих одновременный диалоговый (интерактивный) режим доступа к ЭВМ нескольких пользователей на раз¬ных

терминалах, которым по очереди выделяются ресурсы машины, что координируется операционной системой в соответствии с заданной дисциплиной обслуживания;

- реального времени, обеспечивающих определенное гарантированное время ответа машины на запрос пользователя с управлением им какими-либо внешними но отношению к ЭВМ событиями, процессами или объектами.

В соответствии с седьмым признаком классификации ОС делятся на сетевые и локальные. Сетевые ОС предназначены для управления ресурсами компьютеров, объединенных в сеть с целью совместного использования данных, и предоставляют мощные средства разграничения доступа к данным в рамках обеспечения их целостности и сохранности, а также множество сервисных возможностей по использованию сетевых ресурсов.

В большинстве случаев сетевые операционные системы устанавливаются на один или более достаточно мощных компьютеров-серверов, выделяемых исключительно для обслуживания сети и совместно используемых ресурсов. Все остальные ОС будут считаться локальными и могут использоваться на любом персональном компьютере, а также на отдельном компьютере, подключенном к сети в качестве рабочей станции или клиента.

В настоящее время распространены следующие семейства операционных систем: DOS; OS/2; UNIX; Windows; ОС реального времени.

Основные критерии подхода к выбору операционной системы:

В настоящее время имеется большое количество операционных систем, и перед пользователем стоит задача определить, какая операционная система лучше других (по тем или иным критериям). Очевидно, что идеальных систем не бывает, любая из них имеет свои достоинства и недостатки. Выбирая операционную систему, пользователь должен представлять, насколько та или иная ОС обеспечит ему решение его задач.

Чтобы выбрать ту или иную ОС, необходимо знать:

- на каких аппаратных платформах и с какой скоростью работает ОС;
- какое периферийное аппаратное обеспечение ОС поддерживает;
- как полно удовлетворяет ОС потребности пользователя, то есть каковы функции системы;
- каков способ взаимодействия ОС с пользователем, то есть насколько нагляден, удобен, понятен и привычен пользователю интерфейс;
- существуют ли информативные подсказки, встроенные справочники и т. д.;
- какова надежность системы, то есть ее устойчивость к ошибкам пользователя, отказам оборудования и т. д.;
- какие возможности предоставляет ОС для организации сетей;
- обеспечивает ли ОС совместимость с другими операционными системами;
- какие инструментальные средства имеет ОС для разработки прикладных программ;
- осуществляется ли в ОС поддержка различных национальных языков;
- какие известные пакеты прикладных программ можно использовать при работе с данной системой;
- как осуществляется в ОС защита информации и самой системы.

ОС UNIX является удачной реализацией многопользовательской и многозадачной ОС. Она спроектирована как инструменталь-ная система для разработки программного обеспечения. Система UNIX обладает простым, но очень мощным командным языком и независимой от устройств файловой системой. Системы и приложения, выполняющиеся в ней, легко переносимы.

При создании ОС UNIX имелось три цели:
1.) стремление сохранить простоту и обойтись минимальным количеством функций.

2.) использование общих механизмов во множестве случаев, например при обраще-нии к файлам, прерываниях, именовании и др.;

3.) предоставление возможности решать большие задачи, комбинируя более мелкие.

Процесс может выполняться в одном из двух состояний – пользовательском или систем-ном.
В пользовательском состоянии процесс выполняет пользовательскую программу и имеет доступ к пользовательскому сегменту данных.

В системном состоянии процесс выполняет программы ядра и имеет доступ к системному сегменту данных.

В UNIX-системах используется разделение времени, то есть каждому процессу выделяется квант времени. Процесс либо завершается сам до истечения отведенного ему кванта времени, либо он откладывается по истечении кванта. Чем меньше отведенное процессу время – тем выше его приоритет. Все системные процессы имеют более высокие приоритеты по сравнению с пользовательскими и поэтому всегда обслуживаются в первую очередь.

Linux – это современная POSIX-совмести-мая и UNIX-подобная ОС для ПК и рабочих станций.
Изначально Linux создавался как самодель-ная UNIX-подобная реализация для ПК типа IBM PC с процессором i80386. Однако Linux стал настолько популярен и его на сегодня-шний день поддерживает такое большое число компаний, что в настоящее время имеется реализация этой ОС практически для всех типов процессоров и компьютеров на их основе.
Ядро Linux сразу было создано с учетом возможностей защищенного режима процессоров Intel 80386 и 80486. В частно-сти, Linux использует парадигму описания памяти в защищенном режиме и другие новые свойства процессоров. В настоящее время имеются ядра для этой системы, оптимизированные для работы с процесс-сорами Intel и AMD последнего поколения, хотя основные архитектурные особенности защищенного режима работы изменились мало.

2.11 Лабораторная работа № 11 (2 часа).

Тема: «Аудит. Реализация политики аудита»

2.11.1 Цель работы: Познакомится с понятием аудита, причина его проведения, правовыми документами аудита а также положительными моментами его проведения.

2.11.2 Задание для работы:

1. Возможности систем Windows.
2. Возможности систем UNIX

2.11.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.11.4 Описание (ход) работы:

Практически повсеместно существуют проектные отделы, бухгалтерия, разработчики и другие категории сотрудников, совместно работающие над группами документов, хранящихся в общедоступной (Shared) папке на файловом сервере или на одной из рабочих станций. Может случиться так, что кто-то удалит важный документ или директорию из этой папки, в результате чего труд целого коллектива может быть потерян. В таком случае, перед системным администратором возникает несколько вопросов:

- Когда и во сколько произошла проблема?
- Из какой наиболее близкой к этому времени резервной копии следует восстановить данные?
- Это случилось непреднамеренно, или же кто-то действовал с умыслом?
- Может, имел место системный сбой, который может повториться ещё раз?

В Windows имеется система **Аудита,** позволяющая отслеживать и журналировать информацию о том, когда, кем и с помощью какой программы были удалены документы. По умолчанию, Аудит не задействован — слежение само по себе требует определённый процент мощности системы, а если записывать всё подряд, то нагрузка станет слишком большой. Тем более, далеко не все действия пользователей могут нас интересовать, поэтому политики Аудита позволяют включить отслеживание только тех событий, что для нас действительно важны.

Система Аудита встроена во все операционные системы **Microsoft Windows NT:** Windows XP/Vista/7, Windows Server 2000/2003/2008. К сожалению, в системах серии Windows Home аудит спрятан глубоко, и его настраивать слишком сложно.

Эта функция зачастую используется при обычной работе программ — например, исполненяя команду **Save (Сохранить),** программы пакета **MicrosoftOffice** сначала создают новый временный файл, сохраняют в него документ, после чего удаляют предыдущую версию файла. Аналогично, многие приложения баз данных при запуске сначала создают временный файл блокировок **(.lck),** затем удаляют его при выходе из программы.

Например, конфликтный сотрудник некоей компании при увольнении с места работы решил уничтожить все результаты своего труда, удалив файлы и папки, к которым он имел отношение. События такого рода хорошо заметны — они генерируют десятки, сотни записей в секунду в журнале безопасности. Конечно, восстановление документов из **Shadow Copies (Теневых Копий)** или ежесуточно автоматически создаваемого архива не составляет особого труда, но при этом я мог ответить на вопросы «Кто это сделал?» и «Когда это произошло?».

Одним из инструментов, позволяющих повысить уровень безопасности в Linux, является подсистема аудита. С её помощью можно получить подробную информацию обо всех системных событиях.

Она не обеспечивает никакой дополнительной защиты, но предоставляет подробную информацию о нарушениях безопасности, на основании которой можно принять

конкретные меры. Особенности работы с подсистемой аудита мы рассмотрим в этой статье.

Подсистема аудита: архитектура и принцип работы

Подсистема аудита была добавлена в ядро Linux начиная с версии 2.6. Она предназначена для отслеживания критичных с точки зрения безопасности системных событий.
В качестве примеров таких событий можно привести следующие (список далеко не полный):

- запуск и завершение работы системы;
- чтение, запись и изменение прав доступа к файлам;
- инициация сетевых соединений;
- попытки неудачной авторизации в системе;
- изменение сетевых настроек;
- изменение информации о пользователях и группах;
- запуск и остановка приложений;
- выполнение системных вызовов.

Ни одно из названных событий не может произойти без использования системных вызовов ядра. Чтобы их отслеживать, достаточно просто перехватывать соответствующие системные вызовы. Именно это и делает подсистема аудита:

Получив вызов от приложения в пространстве пользователя, подсистема аудита пропускает его через один из следующих фильтров: user, task или exit (более подробно о них речь пойдёт ниже). После этого вызов пропускается через фильтр exclude, который исходя из правил аудита передаёт его демону auditd для дальнейшей обработки.

Такая простая схема позволяет вполне эффективно отслеживать любой аспект работы ОС, а в случае компрометации системы выявлять подозрительные действия и определять их причину.

2.12 Лабораторная работа № 12-13 (4 часа).

Тема: «Симметричное шифрование и формирование ключа на основе пароля»

2.12.1 Цель работы: Ознакомиться с криптографическими методами шифрования, в особенности симметричное шифрование. Изучить основы формирования ключа на основе пароля.

2.12.2 Задание для работы:

1. Общие сведения о симметричном шифровании.
2. Формирование ключа на основе пароля.

2.12.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.12.4 Описание (ход) работы:

Симметричное шифрование предусматривает использование одного и того же ключа и для зашифрования, и для расшифрования. К симметричным алгоритмам применяются два основных требования: полная утрата всех статистических закономерностей в объекте шифрования и отсутствие линейности. Принято разделять симметричные системы на блочные и поточные. В блочных системах происходит разбиение исходных данных на блоки с последующим преобразованием с помощью ключа.

В поточных системах вырабатывается некая последовательность (выходная гамма), которая в последующем накладывается на само сообщение, и шифрование данных происходит потоком по мере генерирования гаммы. Схема связи с использованием симметричной криптосистемы представлена на рисунке.

Схема связи с использованием симметричной криптосистемы, где M - открытый текст, K - секретный ключ, передаваемый по закрытому каналу, En(M) - операция зашифрования, а Dk(M) - операция расшифрования

Обычно при симметричном шифровании используется сложная и многоступенчатая комбинация подстановок и перестановок исходных данных, причем ступеней (проходов) может быть множество, при этом каждой из них должен соответствовать «ключ прохода». Операция подстановки выполняет первое требование, предъявляемое к симметричному шифру, избавляясь от любых статистических данных путем перемешивания битов сообщения по определенному заданному закону. Перестановка необходима для выполнения второго требования – придания алгоритму нелинейности. Достигается это за счет замены определенной части сообщения заданного объема на стандартное значение путем обращения к исходному массиву.

Симметричные системы имеют как свои преимущества, так и недостатки перед асимметричными. К преимуществам симметричных шифров относят высокую скорость шифрования, меньшую необходимую длину ключа при аналогичной стойкости, большую изученность и простоту реализации. Недостатками симметричных алгоритмов считают в первую очередь сложность обмена ключами ввиду большой вероятности нарушения секретности ключа при обмене, который необходим, и сложность управления ключами в большой сети.

Существует тип протоколов, который последнее время набирает все большую популярность, но все еще не является широко известным — протоколы выработки общего ключа с аутентификацией на основе пароля. К таким протоколам относится российский протокол SESPAKE (Security Evaluated Standardized Password Authenticated Key Exchange), с появлением которого в России и возникла необходимость в рассмотрении особенностей протоколов подобного типа. Целью данной статьи является скорее не дать очередное формальное описание нового протокола, а помочь читателю уловить его основную идею и особенности и понять, почему в нём присутствуют те или иные шаги, почему они важны и чем подобный класс протоколов отличается от всего, что было известно ранее.

PBKDF2 (англ. Password-Based Key Derivation Function) — стандарт формирования ключа на основе пароля. Является частью PKCS #5 v2.0 (RFC 2898). Заменил PBKDF1, который ограничивал длину порождаемого ключа 160 битами.

PBKDF2 использует псевдослучайную функцию для получения ключей. Длина генерируемого ключа не ограничивается (хотя эффективная мощность пространства ключей может быть ограничена особенностями применяемой псевдослучайной функции). Использование PBKDF2 рекомендовано для новых программ и продуктов. В качестве псевдослучайной может быть выбрана криптографическая хеш-функция, шифр, HMAC.

2.13 Лабораторная работа № 14-15 (4 часа).

Тема: «Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС»

2.13.1 Цель работы: Изучить основы генерации, настройки и измерения производительности. Также проводится изучение возможностей модификации систем управления операционной системы для повышения качества безопасности.

2.13.2 Задание для работы:

1. Задачи и принципы сопровождения системного программного обеспечения.
2. Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС

2.13.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2.13.4 Описание (ход) работы:

Организация эффективной и надежной защиты операционной системы невозможна с помощью одних только программно-аппаратных средств. Эти средства обязательно должны, дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже самая надежная программно-аппаратная защита оборачивается фикцией.

Основные административные меры защиты.

1. Постоянный контроль корректности функционирования операционной системы, особенно ее подсистемы защиты. Такой контроль наиболее удобно организовать, если операционная система поддерживает регистрацию событий (event logging). В этом случае операционная система автоматически регистрирует в специальном журнале (или нескольких журналах) наиболее важные события, произошедшие в процессе функционирования системы.
2. Организация и поддержание адекватной политики безопасности. Политика безопасности должна постоянно корректироваться, оперативно реагируя на изменения в конфигурации операционной системы, установку, удаление и изменение конфигурации прикладных программных продуктов и расширений операционной системы, попытки злоумышленников преодолеть защиту операционной системы и т.д.

3. Инструктирование пользователей операционной системы о необходимости соблюдения мер безопасности при работе с операционной системой и контроль за соблюдением этих мер.

4. Регулярное создание и обновление резервных копий программ и данных операционной системы.

Постоянный контроль изменений в конфигурационных данных и политике безопасности операционной системы.

Основные принципы администрирования ОС.

- Непрерывность;
- Комплексность;
- Актуальность;
- Адекватность;
- Непротиворечивость. (разграничение доступа, настроек процессов);
- Формальный подход. Применение методик (инструкций, положений, приказов, РД и прочих рекомендательных документов) и четких концептуальных принципов при постановке задач администрирования и их реализации;
- Подконтрольность.

Задачи и принципы управления безопасностью.

Отдельные средства ИБ не обеспечивают эффективного функционирования и требуют объединения в единую и централизованно управляемую и постоянно действующую *систему информационной безопасности* Система ИБ обычно должна решать следующие задачи:

• ввод в систему списка имен пользователей и терминалов, допущенных к информации ИС;
• подготовку и ввод в систему, запись паролей пользователей на носители;
• ввод в систему назначенных полномочий пользователей и терминалов;
• раздачу пользователям носителей с паролями и значений паролей, запоминаемых и вводимых пользователями вручную с клавиатуры;
• сбор сигналов несовпадения паролей и нарушения полномочий пользователей;
• установление времени, места и причины НСД;
• анализ ситуации, принятие адекватных мер и восстановление нормального функционирования ИС
• контроль конфигурации системы;
• сбор сигналов вскрытия аппаратуры и контроль ввода (вывода) аппаратуры в (из) ремонт (а) и на (из) профилактику(и);
• контроль журнала регистрации доступа к информации ИС и периодический вызов справок из него;
• взаимодействие со службой функционального контроля ИС;
• контроль функционирования системы защиты;
• подготовку ключей, контроль и обеспечение функционирования средств шифрования информации;
• контроль стирания и уничтожения остатков секретной информации на машинных и бумажных носителях;
• регистрацию, учет и разграничение доступа к носителям информации и ПО;
• ведение статистики и прогнозирование НСД.

И удовлетворять следующим принципом:

■ непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;

■ плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);
■ целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;
■ конкретной. Защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
■ активной. Защищать информацию необходимо с достаточной степенью настойчивости;
■ надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;
■ универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;
■ комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что защита — это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообусловливающих друг друга сторон, свойств, тенденц

Безопасность – одна из наиболее актуальных проблем в области ИТ в настоящее время, ввиду сильной зависимости повседневной деятельности и бизнеса от компьютерных технологий и ввиду резко возрастающего числа сетевых атак (киберпреступности). Особенно важна безопасность для операционных систем и сетей как основных объектов атак. В лекции рассмотрены следующие вопросы:

- Проблема безопасности
- Аутентификация
- Программные угрозы (атаки)
- Системные угрозы (атаки)
- Защита систем
- Обнаружение взлома
- Криптография
- Безопасность в Windows NT / 2000 / XP / 2003 / Vista, в.NET
- Инициатива Trustworthy Computing Initiative корпорации Microsoft.

Проблема безопасности

Безопасность (security) – это защита от внешних атак. В настоящее время наблюдается значительный рост числа самых разнообразных атак хакеров, угрожающих целостности информации, работоспособности компьютерных систем и зависящих от них компаний, благосостоянию и личной безопасности людей. Для защиты от атак необходимы специальные меры безопасности, компьютерные технологии и инструменты.
В любой компьютерной системе должна быть реализована подсистема безопасности, которая должна проверять внешнее окружение системы и защищать ее от:

- Несанкционированного доступа
- Злонамеренной модификации или разрушения
- Случайного ввода неверной информации.

Практика показывает, что легче защитить от случайной, чем от злонамеренной порчи информации.

Аутентификация

Одной из наиболее широко используемых мер безопасности является аутентификация (authentication) – идентификация пользователейпри входе в систему. Такая идентификация пользователей наиболее часто реализуется через логины – зарегистрированные имена пользователей для входа в систему – и пароли – секретные кодовые слова, ассоциируемые с каждым логином.
Основной принцип использования паролей в том, что они должны сохраняться в секрете. Поэтому одна из традиционных целей атакующихххакеров состоит в том, чтобы любыми способами выведать у пользователя его логин и пароль. Для сохранения секретности паролей предпринимаются следующие меры.

- Частая смена паролей. Аналогичные меры применялись в армии во время войны. Большинство сайтов и других систем (например, сайт партнеров фирмы Microsoft) требуют от пользователей регулярной (например, не реже. чем раз в три месяца) смены паролей, иначе сайт блокируется для доступа. Подобные меры вполне оправданы.
- Использование "не угадываемых" паролей. Практически все системы требуют от пользователя при регистрации устанавливать пароли, не являющиеся легко угадываемыми: например, как правило, пароль должен содержать большие и маленькие буквы и цифры, специальные символы и иметь длину не менее 7-8 символов. Используются также автоматические генераторы не угадываемых паролей. Поэтому использование в качестве паролей легко угадываемых слов – например, имени любимой собаки или общеупотребительного понятия – не рекомендуется.
- Сохранение всех неверных попыток доступа. Во многих системах реализован системный журнал, в котором фиксируются все неверные попытки ввода логинов и паролей. Обычно дается фиксированное число таких попыток (например, три).

Пароли также могут быть закриптованы или разрешены для доступа лишь один раз, после чего от пользователя требуется смена пароля.

Программные угрозы (атаки)

Рассмотрим некоторые типичные виды угроз и атак, используемые хакерами.
Троянская программа (Trojan Horse) – атакующая программа, которая "подделывается" под некоторую полезную программу, но при своем запуске не по назначению (злонамеренно) использует свое окружение, например, получает и использует конфиденциальную информацию. Троянские программы используют системные механизмы для того, чтобы программы, написанные одними пользователями, могли исполняться другими пользователями.
Вход в ловушку (Trap Door) - использование логина или пароля, который позволяет избежать проверок, связанных с безопасностью.
Переполнение стека и буфера (Stack and Buffer Overflow) - использование ошибки в программе (переполнение стека или буферов в памяти) для обращения к памяти другого пользователя или процесса с целью нарушения ее целостности.

Системные угрозы (атаки)

Рассмотрим также некоторые типичные атаки, использующие уязвимости (vulnerabilities) в системных программах – ошибки и недочеты, дающие возможность организации атак.
Черви (Worms) – злонамеренные программы, использующие механизмы самовоспроизведения (размножения). Например, один из Интернет-червей использует сетевые возможности UNIX (удаленный доступ) и ошибки в программах finger и sendmail. Принцип его действия следующий: некоторая постоянно используемая в сети системная программа распространяет главную программу червя.
Вирусы – фрагменты кода, встраивающиеся в обычные программы с целью нарушения работоспособности этих программ и всей компьютерной системы. В основном вирусы действуют на микрокомпьютерные системы. Вирусы скачиваются с публично доступных сайтов или с дисков, содержащих "инфекцию". Для предотвращения заражения компьютерными вирусами необходимо соблюдать принципы безопасности при использовании компьютеров (safe computing) – использовать антивирусы, guards – программы, постоянно находящиеся в памяти и проверяющие на вирусы каждый открываемый файл - .exe, doc, и т.д.
Отказ в обслуживании (Denial of Service – DoS) – одна из распространенных разновидностей атак на сервер, заключающаяся в создании искусственной перегрузки сервера с целью препятствовать его нормальной работе. Например, для Web-сервера такая атака может заключаться в том, чтобы искусственно сгенерировать миллион запросов "GET". Если сервер реализован не вполне надежно, подобная атакачаще всего приводит к переполнению памяти на сервере и необходимости его перезапуска.

Типы сетевых атак

Рассмотрим некоторые типы современных сетевых атак, которых необходимо постоянно остерегаться пользователям.
Phishing – попытка украсть конфиденциальную информацию пользователя путем ее обманного получения от самого пользователя. Даже само слово phishing – искаженное слово fishing (рыбная ловля), т.е. хакер с помощью этого приема как бы пытается поймать чересчур наивного пользователя "на удочку". Например, напугав в своем сообщении пользователя, что его логин и пароль, кредитная карта или банковский счет под угрозой, хакер пытается добиться от пользователя в ответ ввода и отправки некоторой конфиденциальной информации. Обычно phishing-сообщение по электронной почте приходит как бы от имени банка и подделывается под цвета, логотипы и т.д., используемые на сайте банка. Однако для его разоблачения обычно достаточно подвести курсор мыши (не кликая ее) к приведенной web-ссылке или email-адресу (при этом она высвечивается) и убедиться в том, что адрес указывает отнюдь не на банк, а на совершенно посторонний сайт или email. Поэтому пользователям не следует быть слишком наивными. Другая действенная мера, если phishingпроисходит регулярно с одних и тех же email-адресов, - включить эти адреса в черный список на email-сервере. Тогда подобные сообщения вообще не будут доходить до входного почтового ящика пользователя.
Pharming – перенаправление пользователя на злонамеренный Web-сайт (обычно с целью phishing). Меры предотвращения со стороны пользователя мы уже рассмотрели. В современные web-браузеры встроены программы антифишингового контроля, которые запускаются автоматически при обращении к сайту. Хотя это отнимает у пользователя некоторое время, подобные меры помогают предотвратить многие атаки.
Tampering with data – злонамеренное искажение или порча данных. Действенной мерой по борьбе с подобными атаками являетсякриптование информации.

Spoofing – " подделка" под определенного пользователя (злонамеренное применение его логина, пароля и полномочий). Логин и парольпри этом либо получены от пользователя обманным путем (например, в результате phishing), либо извлечены из "взломанного" хакерской программой системного файла.
Elevation of privilege – попытка расширить полномочия (например, до полномочий системного администратора) с целью злонамеренных действий. Поэтому наиболее секретная информация в любой компьютерной системе – пароль системного администратора, который необходимо защищать особенно тщательно.

2.14 Лабораторная работа № 16-17 (4 часа).

Тема: «Цифровая подпись. Процедура оформления подписи и проверка»

2. 14.2 Цель работы: Изучить понятие цифровая подпись и ее применение в современном мире. Также изучаются аспекты и процедуры получения подписи и проверки ее на подлинность.

2. 14.2 Задание для работы:

1. Основы формирования цифровой подписи.
2. Методы передачи цифровой подписи.

2. 14.3 Перечень приборов, материалов, используемых в лабораторной работе:

1.Персональный компьютер с установленным специальным ПО.

2. Мультимедийное оборудование

2. 14.4 Описание (ход) работы:

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

[Электронная] цифровая подпись (digital signature): Строка бит, полученная в результате процесса формирования подписи. Данная строка имеет внутреннюю структуру, зависящую от конкретного механизма формирования подписи.

Общая суть электронной подписи заключается в следующем. С помощью криптографической хэш-функции на основании документа вычисляется относительно короткая строка символов фиксированной длины (хэш). Затем этот хэш шифруется закрытым ключом владельца — результатом является подпись документа. Подпись прикладывается к документу, таким образом получается подписанный документ. Лицо, желающее установить подлинность документа, расшифровывает подпись открытым ключом владельца, а также вычисляет хэш документа. Документ считается подлинным, если вычисленный по документу хэш совпадает с расшифрованным из подписи, в противном случае документ является подделанным.
Принципы использования электронной подписи:
Принципами использования электронной подписи являются:
- право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено

федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

- возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования Федерального закона №63 «Об электронной подписи» применительно к использованию конкретных видов электронных подписей;
- недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Виды электронных подписей:

Видами электронных подписей, отношения в области использования которых регулируются Федеральным законом №63 «Об электронной подписи», являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

1. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
2. Неквалифицированной электронной подписью является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

3. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом №63 «Об электронной подписи».

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью:

1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.
2. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом,

равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны соответствовать требованиям статьи 9 настоящего Федерального закона.

3. Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

4. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

Шифрование передаваемых через Интернет данных позволяет защитить их от посторонних лиц. Однако для полной безопасности должна быть уверенность в том, что второй участник транзакции является тем лицом, за которое он себя выдает. В бизнесе наиболее важным идентификатором личности заказчика является его подпись. В электронной коммерции применяется электронный эквивалент традиционной подписи — цифровая подпись . С ее помощью можно доказать не только то, что транзакция была инициирована определенным источником, но и то, что информация не была испорчена во время передачи.

Как и в шифровании, технология электронной подписи использует либо секретный ключ (в этом случае оба участника сделки применяют один и тот же ключ), либо открытый ключ (при этом требуется пара ключей — открытый и личный). И в данном случае более просты в использовании и более популярны методы с открытым ключом (такие, как RSA)

Хэш-функции являются одним из важных элементов криптосистем на основе ключей и используются для обнаружения факта модификации сообщения, то есть для электронной подписи. Их относительно легко вычислить, но почти невозможно расшифровать. Хэш-функция имеет исходные данные переменной длины и возвращает строку (иногда называемую дайджестом сообщения — MD) фиксированного размера, обычно 128 бит.

Существует несколько защищенных хэш-функций: Message Digest 5 (MD-5), Secure Hash Algorithm (SHA) и др. Они гарантируют, что разные документы будут иметь разные

электронные подписи, и что даже самые незначительные изменения документа вызовут изменение его дайджеста.

Рассмотрим, как работает технология цифровой подписи, использующая алгоритм RSA. Предположим, вы хотите послать сообщение. В этом случае порядок работы следующий:
1. При помощи хеш-функции вы получаете дайджест — уникальным образом сжатый вариант исходного текста.
2. Получив дайджест сообщения, вы шифруете его с помощью личного ключа RSA, и дайджест превращается в цифровую подпись.
3. Вы посылаете вместе с самим сообщением цифровую подпись.
4. Получив послание, получатель расшифровывает цифровую подпись с помощью вашего открытого ключа и извлекает дайджест сообщения.
5. Получатель, применяя для сообщения ту же хэш-функцию, что и вы, получает свой сжатый вариант текста и сравнивает его с дайджестом, восстановленным из подписи. Если они совпадают, то это значит, что подпись правильная и сообщение действительно поступило от вас. В противном случае сообщение либо отправлено из другого источника, либо было изменено после создания подписи.

При аутентификации личности отправителя открытый и личный ключи играют роли, противоположные тем, что они выполняли при шифровании. Так, в технологии шифрования открытый ключ используется для зашифровки, а личный — для расшифровки. При аутентификации с помощью подписи все наоборот. Кроме того, подпись гарантирует только целостность и подлинность сообщения, но не его защиту от посторонних глаз. Для этого предназначены алгоритмы шифрования. Например, стандартная технология проверки подлинности электронных документов DSS (Digital Signature Standard) применяется в США компаниями, работающими с государственными учреждениями. Однако у технологии RSA более широкие возможности в силу того, что она служит как для генерации подписи, так и для шифрования самого сообщения. Цифровая подпись позволяет проверить подлинность личности отправителя: она основана на использовании личного ключа автора сообщения и обеспечивает самый высокий уровень сохранности информации.

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

3.1 Практическое занятие № 2 (2 часа).

Тема: «Элементы безопасности системы. Учетные записи пользователей и групп в ОС Windows NT»

3.1.1 Задание для работы:

1. Элементы безопасности системы.
2. Учетные записи пользователей и групп в ОС Windows NT.

3.1.2 Краткое описание проводимого занятия:

1. Элементы безопасности системы.

Система обеспечения информационной безопасности Российской Федерации предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;
- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;
- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;

- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

- Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

2. Учетные записи пользователей и групп в ОС Windows NT.

Учетные записи пользователей и учетные записи компьютеров представляют собой такие же физические объекты, как компьютер или пользователь. Учетные записи пользователей также могут использоваться как записи выделенных служб для некоторых приложений. Учетные записи пользователей и компьютеров (а также группы) называются участниками безопасности. Участники безопасности являются объектами каталогов, которым автоматически назначаются коды безопасности (SID) для доступа к ресурсам домена. Учетная запись пользователя или компьютера используется для следующих целей.

- Проверка подлинности пользователя или компьютера.

  Учетная запись пользователя дает право войти в компьютеры и в домен с подлинностью, проверяемой доменом.. Каждый входящий в сеть пользователь должен иметь собственную учетную запись и пароль. Для обеспечения максимальной безопасности следует запретить пользователям использовать одну и ту же учетную запись.

- Разрешение или запрещение доступа к ресурсам домена.

  Как только проверка подлинности пользователя завершена, он получает или не получает доступ к ресурсам домена в соответствии с явными разрешениями, назначенными данному пользователю на ресурсе.

- Аудит действий, выполняемых с использованием учетной записи пользователя или компьютера.

  Аудит помогает при наблюдении за безопасностью учетных записей.

Если права и разрешения встроенной учетной записи не были изменены или отключены администратором сети, они могут использоваться злоумышленниками (или службой) для нелегального проникновения в домен с применением учетной записи администратора или гостя. Для обеспечения достаточной защиты эти учетные записи переименовывают или отключают. Поскольку коды безопасности (SID) учетных записей сохраняются,

переименованная учетная запись сохраняет все остальные свойства, в том числе описание, пароль, принадлежность к группам, профиль пользователя, учетную информацию, а также любые разрешения и права пользователя.
Для обеспечения безопасности проверки подлинности пользователя следует создавать отдельные учетные записи для каждого пользователя сети. Каждая учетная запись пользователя (включая учетные записи администратора и гостя) может быть добавлена в группу для управления правами и разрешениями, назначенными этой учетной записи. Использование соответствующих этой сети учетных записей и групп позволяет проверить подлинность входящего в сеть пользователя и возможность предоставления ему разрешенных ресурсов.
Повысить защиту домена от атак можно с помощью надежных паролей и политики блокировки учетных записей. Использование надежных паролей снижает риск угадывания и подбора вариантов паролей.

3.1.3 Результаты и выводы:

В результате практической работы, студент изучил основы безопасность операционной системы, а также основные положения и принципы создания и управления учетными записями пользователей и групп.

3.2 Практическое занятие № 2 (2 часа).

Тема: «Домены Windows NT. Локальная политика безопасности»

3.2.1 Задание для работы:

3. Домены Windows NT.
4. Локальная политика безопасности.

3.2.2 Краткое описание проводимого занятия:

2. Домены Windows NT.

Домен - это основная единица администрирования и обеспечения безопасности в Windows NT. Для домена существует общая база данных учетной информации пользователей домена (user accounts) и ресурсов домена - компьютеров (computer accounts) и принтеров (printer accounts). Пользователь домена выполняет один логический вход в домен и получает доступ сразу ко всем разрешенным ресурсам этого домена.

Членами домена являются как пользователи, так и компьютеры. При отсутствии доменной организации каждый компьютер Windows NT Workstation и Windows NT Server хранит собственную базу учетных данных пользователей - SAM (Security Access Manager). В этой базе хранится вся необходимая системе информация о пользователе - имя, пароль (в зашифрованном виде) и так называемый SID - Security Identifier. Идентификатор SID играет ключевую роль в процессе предоставления пользователю доступа к защищенным ресурсам системы - файлам, принтерам и т.п. В списке прав доступа ресурса ACL хранится информация о конкретных номерах SID, которым разрешен тот или иной вид доступа. Каждый SID является уникальным числом. При изменении имени пользователя его SID не изменяется.

Компьютер домена также характеризуется именем и идентификатором SID, между которыми имеется такое же соотношение, как и между именем и идентификатором SID пользователя.

В домене обязательно есть сервер Windows NT Server, выполняющий роль первичного контроллера домена - Primary Domain Controller, PDC. Этот контроллер хранит первичную копию базы данных учетной информации пользователей домена - SAM PD. Все изменения учетной информации сначала производятся именно в этой копии. Основной контроллер домена всегда существует в единственном экземпляре.

Кроме основного контроллера, в домене могут существовать несколько резервных контроллеров - Backup Domain Controllers, BDC. Эти контроллеры хранят реплики базы учетных данных. Все резервные контроллеры в дополнение к основному могут обрабатывать запросы пользователей на логический вход в домен. База данных SAM BD всегда является копией (с точностью до интервала синхронизации) базы SAM PD.

Резервный контроллер домена решает две задачи:

3. Он становится основным контроллером при отказе последнего.
4. Уменьшает нагрузку на основной контроллер по обработке запросов на логический вход пользователей.

Если сеть состоит из нескольких сетей, соединенных глобальными связями, то в каждой из составляющих сетей должен быть по крайней мере один резервный контроллер домена.

Членами домена могут быть также компьютеры, на которых установлены Windows NT Server, не назначенные на роль PDC или BDC. Такие серверы называются *отдельно стоящими серверами (Stand-alone servers)* или серверами - членами доменами *(Member servers)*. На таких компьютерах, освобожденных от функций аутентификации пользователей и ведения справочной базы данных, могут более производительно выполняться ответственные приложения или файл- и принт-сервисы. Stand-alone серверы не могут быть оперативно переконфигурированы в PDC или BDC, для этого требуется переинсталляция.

Рабочая станция Windows NT Workstation и сервер Windows NT Server, не выполняющий роль PDC или BDC, могут динамически изменять свое членство в домене, а серверы PDC и BDC - только при инсталляции системы. Поэтому при инсталляции очень важно правильно выбрать принадлежность компьютера, назначенного на роль контроллера домена, тому или иному домену.

2.Локальная политика безопасности.

Локальная политика безопасности – это оснастка консоли управления, позволяющая устанавливать различные системные параметры безопасности. Данная оснастка также является частью групповой политики.
Для запуска этой оснастки откройте Панель управления, в категории Система и безопасность щелкните на ссылке Администрирование, после этого дважды щелкните на значке Локальная политика безопасности и подтвердите ваши действия в окне UAC (если оно появится)
Наиболее актуальные параметры безопасности собраны в разделе Локальные политики.

• Политика аудита. Здесь вы можете определить, какие события будут записываться в журнал безопасности. Для включения аудита дважды щелкните на нужном событии и в появившемся окне установите нужные флажки: Успех – для занесения в журнал удачных попыток, Отказ – для фиксации неудачных попыток выбранного действия.
• Назначение прав пользователя. В этой категории имеется довольно обширный список параметров, определяющих, что можно и что нельзя делать на компьютере отдельным пользователям и группам. Например, вы можете указать, каким пользователям разрешить локальный вход, а каким – доступ по сети, кто может выполнять завершение работы или изменять системное время.
• Параметры безопасности. Здесь собраны различные административные параметры, определяющие поведение системы при входе в нее, доступе к компьютеру из сети, работе с устройствами и др.

3.2.3 Результаты и выводы:

В ходе практической работы, студент знакомится с понятием домена как такового и понятием домена в Windows NT, также изучается локальная политика безопасности.

3.3 Практическое занятие № 3 (2 часа).

Тема: «Управление ресурсами»

3.3.1 Задание для работы:

1.Управление процессорами.
2.Управление памятью.

3.3.2 Краткое описание проводимого занятия:

1.Управление процессорами. .
Основные задачи управления процессором сводятся к решению двух взаимосвязанных проблем:
 Создание условий, при которых каждый процесс и приложение получат достаточную часть рабочего времени процессора, чтобы обеспечивалось их нормальное функционирование

 Использование стольких циклов процессора, сколько возможно для нормальной работы.

Основной единицей программного обеспечения, с которой операционная система работает при планировании работы процессора, является либо процесс, либо поток, в зависимости от операционной системы.

Было бы заманчиво рассматривать процесс как приложение, однако такой подход дает неполную картину того, какая устанавливается взаимосвязь процессов с операционной системой и аппаратными средствами. Видимое пользователем приложение (текстовый редактор, электронная таблица или игра) действительно является процессом, однако это приложение может инициировать запуск некоторых других процессов для решения таких задач, как связь с другими устройствами или компьютерами. Имеется также большое

число процессов, которые протекают, не проявляя себя. Например, в Windows XP и UNIX могут быть десятки фоновых процессов, предназначенных для управления сетью, памятью и дисками, проверки на наличие вирусов и т.д.

Таким образом, процесс – это программа, выполняющая определенное действие, и которой можно управлять – силами пользователя, с помощью других приложений или с помощью операционной системы.

Операционная система осуществляет контроль и планирует выполнение центральным процессором процессов, а не приложений. В однозадачной системе планирование выполнения простое. Операционная система разрешает приложению запуститься, временно приостанавливая его выполнение на достаточно длительное время лишь в случае необходимости обслуживания прерываний и пользовательского ввода данных.

Прерывания – специальные сигналы, отправляемые на центральный процессор аппаратными средствами или программами. Это похоже на то, как если бы во время оживленного собрания какая-то часть компьютера вдруг подняла руку, требуя к себе внимания центрального процессора. Иногда операционная система устанавливает приоритеты процессов таким образом, что прерывания маскируются, то есть операционная система игнорирует прерывания от некоторых источников, чтобы определенная операция была завершена как можно скорее. Существуют некоторые прерывания (например, вызванные состоянием ошибки или проблемами с памятью), которые настолько важны, что их нельзя игнорировать. Эти немаскируемые прерывания (non-maskable interrupts, NMIs) требуют немедленного решения проблемы, несмотря на то, что должны выполняться другие задачи.

Учитывая, что прерывания создают определенные сложности при выполнении процессов даже в однозадачной системе, функционирование операционной системы становится намного более сложным в многозадачной системе. В последнем случае операционная система должна организовать выполнение приложений таким образом, чтобы создавалось впечатление, что определенные события происходят одновременно. Это сложно осуществить, поскольку центральный процессор в каждый момент времени может делать только одну операцию. Современные многоядерные процессоры и многопроцессорные компьютеры могут выполнять по нескольку операций одновременно, однако каждое ядро процессора, как и прежде, в каждый момент времени может делать только одну операцию.

Чтобы создавалось впечатление, что множество событий происходит одновременно, операционная система должна осуществлять переключение между разными процессами тысячи раз в секунду. Это делается следующим образом:

 Процесс занимает определенную часть оперативной памяти. Кроме того, он использует регистры, стеки и очереди в центральном процессоре, а также в пространстве памяти операционной системы.

 Допустим, имеется два многозадачных процесса. Операционная система выделяет на каждую программу по определенному количеству исполнительных циклов.

 После прохождения этого количества циклов операционная система делает копии всех регистров, стеков и очередей, использовавшихся в процессах, и отмечает место, на

котором наступила пауза выполнения процесса.

 Затем производится загрузка всех регистров, стеков и очередей, используемых вторым процессом, и этому процессу разрешается прохождение определенного количества циклов центрального компьютера.

 По завершении этих циклов делаются копии всех регистров, стеков и очередей, использовавшихся второй программой, и производится загрузка первой программы.

2. Управление памятью.

Основная (или как ее принято называть в отечественной литературе и документации, оперативная) память всегда была и остается до сих пор наиболее критическим ресурсом компьютеров. Если учесть, что большинство современных компьютеров обеспечивает 32-разрядную адресацию в пользовательских программах, и все большую силу набирает новое поколение 64-разрядных компьютеров, то становится понятным, что практически безнадежно рассчитывать, что когда-нибудь удастся оснастить компьютеры основной памятью такого объема, чтобы ее хватило для выполнения произвольной пользовательской программы, не говоря уже об обеспечении мультипрограммного режима, когда в основной памяти, вообще говоря, могут одновременно содержаться несколько пользовательских программ.

Поэтому всегда первичной функцией всех операционных систем (более точно, операционных систем, обеспечивающих режим мультипрограммирования) было обеспечение разделения основной памяти между конкурирующими пользовательскими процессами. Мы не будем здесь слишком сильно вдаваться в историю этого вопроса. Заметим лишь, что применявшаяся техника распространяется от статического распределения памяти (каждый процесс пользователя должен полностью поместиться в основной памяти, и система принимает к обслуживанию дополнительные пользовательские процессы до тех пор, пока все они одновременно помещаются в основной памяти), с промежуточным решением в виде "простого своппинга" (система по-прежнему располагает каждый процесс в основной памяти целиком, но иногда на основании некоторого критерия целиком сбрасывает образ некоторого процесса из основной памяти во внешнюю память и заменяет его в основной памяти образом некоторого другого процесса), до смешанных стратегий, основанных на использовании "страничной подкачки по требованию" и развитых механизмов своппинга.

Операционная система UNIX начинала свое существование с применения очень простых методов управления памятью (простой своппинг), но в современных вариантах системы для управления памятью применяется весьма изощренная техника.

Поэтому в таких случаях используется техника копирования страниц при попытке записи. Несмотря на то, что в сегмент запись разрешена, для каждой его страницы устанавливается блокировка записи. Тем самым, во время попытки выполнения записи возникает прерывание, и ОС на основе анализа статуса соответствующего сегмента принимает решение о выделении новой страницы, копировании на нее содержимого оригинальной страницы и о включении этой новой страницы на место старой в виртуальную память либо процесса-предка, либо процесса-потомка (в зависимости от того, кто из них пытался писать).

На этом мы заканчиваем краткое описание механизма управления виртуальной памятью в ОС UNIX. Еще раз подчеркнем, что мы опустили множество важных технических деталей, стремясь продемонстрировать наиболее важные принципиальные решения.

3.3.3 Результаты и выводы:

В ходе практической работы, студент учится управлению процессорами определённых типов, а также основам управления памяти.

3.4 Практическое занятие № 4 (2 часа).

Тема: «Доменная политика конфигураций безопасности. Конфигурирование безопасности в Windows NT**»**

3.4.1 Задание для работы:

1. Доменная политика конфигураций безопасности.
2. Основы безопасности в Windows NT

3.4.2 Краткое описание проводимого занятия:

3. Доменная политика конфигураций безопасности.

Подробные политики паролей можно использовать для определения нескольких политик паролей в одном домене. С помощью подробных политик паролей можно применять различные ограничения политик паролей и блокировки учетных записей к разным группам пользователей в домене.
Например, можно применить более строгие параметры к привилегированным учетным записям и менее строгие – к учетным записям других пользователей. Может также возникнуть необходимость применения особой политики паролей к тем учетным записям, пароли которых синхронизируются с другими источниками данных.

Подробные политики паролей применимы только к объектам пользователей (или объектам inetOrgPerson, если они используются вместо объектов пользователей) и глобальным группам безопасности. По умолчанию задавать подробные политики паролей могут только члены группы администраторов домена. Однако возможность задавать эти политики можно также делегировать другим пользователям. Домен должен работать в режиме Windows Server 2008.
Подробную политику паролей нельзя применить непосредственно к подразделению. Для применения подробной политики паролей к пользователям из подразделения можно использовать теневую группу.
Теневая группа – это глобальная группа безопасности, которая логически сопоставляется с подразделением для принудительного применения подробной политики паролей. После добавления пользователей подразделения в созданную теневую группу к ней можно применить подробную политику паролей. Для других подразделений можно по мере необходимости создавать дополнительные теневые группы. При перемещении пользователя из одного подразделения в другое необходимо обновлять его членство в соответствующих теневых группах.
В одном домене допускается использование подробных политик паролей одновременно с настраиваемыми фильтрами паролей. Если на контроллерах домена с Windows 2000 или

Windows Server 2003 развернуты настраиваемые фильтры паролей, их можно использовать и в дальнейшем в целях обеспечения дополнительных ограничений для паролей.

Объекту пользователя или группы может быть привязано несколько объектов параметров паролей. Такая ситуация имеет место в случае, если этот объект является членом нескольких групп, к которым привязаны различные объекты параметров паролей, либо в случае, когда несколько объектов параметров паролей привязаны к этому объекту напрямую. Однако только один объект параметров паролей может быть применен в качестве действующей политики паролей. Только параметры этого объекта параметров паролей будут оказывать влияние на пользователя или группу. Слияние с параметрами других объектов параметров паролей, привязанных к этому пользователю или группе, невозможно.
Результирующая политика может быть определена только для объекта пользователя. Объект параметров паролей может быть применен к объекту пользователя двумя способами, указанными ниже.

5. Непосредственно: объект параметров паролей связывается с пользователем.

6. Косвенно: объект параметров паролей связывается с группами, членом которых является пользователь.

По умолчанию объекты параметров паролей могут создавать только члены группы администраторов домена. Только члены этой группы имеют разрешения "Создать дочерний" и "Удалить дочерний" на объект контейнера параметров паролей. Кроме того, только члены группы "Администраторы домена" по умолчанию имеют разрешение "Записать свойство" на объект параметров паролей. Поэтому только члены данной группы могут привязать объект параметров паролей к группе или пользователю. Это разрешение можно делегировать другим группам или пользователям.
Чтобы применить объект параметров паролей к объекту пользователя или группы, разрешения на работу с ними не требуются. Разрешения на запись объекта пользователя или группы не позволяют связать объект параметров паролей с пользователем или группой. Владелец группы не имеет разрешений на связывание объекта параметров паролей с группой, поскольку прямая ссылка содержится в объекте параметров паролей. Возможность связывания объекта параметров паролей с группой или пользователем имеется у владельца объекта параметров паролей.
Параметры объекта параметров паролей можно считать конфиденциальными; таким образом, по умолчанию пользователи, прошедшие проверку подлинности, не имеют разрешений "Чтение свойства" для объекта параметров паролей. По умолчанию только члены группы администраторов домена имеют эти разрешения для используемого по умолчанию дескриптора безопасности объекта параметров паролей в схеме.

4. Основы безопасности в Windows NT

Модель безопасности Windows NT базируется на концепции пользовательских бюджетов (user accounts). Можно создать неограниченное количество пользовательских бюджетов и сгруппировать их наиболее удобным методом. После этого для каждого бюджета или группы можно представить или ограничить доступ к любому из ресурсов компьютера.

В операционную систему Windows NT встроена возможность аудита. Это позволяет отслеживать, какие пользовательские бюджеты использовались для доступа в систему, и какого типа доступ к файлам и другим объектам был получен пользователями. Кроме того, аудит может использоваться для отслеживания попыток входа в систему, остановки

и перезапуска системы и прочих аналогичных событий.

Модель безопасности Windows NT содержит следующие компоненты:

- Процессы входа в систему (Logon processes), принимающие от пользователей на регистрацию в системе. Сюда относятся начальный интерактивный процесс регистрации, отображающий диалоговое окно входа в систему, и процесс удаленной регистрации, позволяющий удаленным пользователям получить доступ к серверу Windows NT.

- Распорядитель локальной безопасности (Local Security Authority, LSA), гарантирующий, что каждый пользователь, регистрирующийся в системе, имеет право доступа к ней. Этот компонент является центральным для всей подсистемы безопасности Windows NT. Он создает маркеры безопасного доступа, управляет локальной политикой безопасности и обеспечивает интерактивный сервис аутентификации пользователей. Кроме того, LSA управляет политикой аудита и регистрирует сообщения аудита, генерируемые монитором безопасности (Security Reference Monitor).

- Диспетчер бюджетов безопасности (Security Accounts Monitor, SAM). Этот компонент поддерживает базу данных пользовательских бюджетов. База данных SAM содержит информацию обо всех пользовательских и групповых бюджетах. SAM обеспечивает сервис валидизации пользовательских паролей, используемый LSA. База данных SAM известна также под названием базы данных каталога (Directory Database).

- Монитор безопасности (Security Reference Monitor) - компонент системы безопасности, ответственный за проверку наличия у пользователей прав доступа к объектам и осуществления действий, которые они пытаются выполнить. Монитор безопасности принудительным образом устанавливает проверку прав доступа к объектам и устанавливает политику аудита заданную LSA. Монитор безопасности предоставляет сервис процессам, которые работают как в режиме ядра, так и в режиме пользователя. Это гарантирует, что все пользователи и процессы, пытающиеся получить доступ к объекту и выполнить над ним некоторые действия, обладают соответствующими правами доступа. Кроме того, монитор безопасности генерирует сообщения аудита в тех случаях, когда это необходимо.

Ключевой особенностью системы безопасности Windows NT является управление доступом к объектам. Модель безопасности поддерживает информацию защиты для каждого пользователя, группы и объекта. Она может идентифицировать попытки доступа, осуществленные непосредственно пользователем, а также способна выявлять непрямые попытки доступа, предпринятые не самим пользователем, а программой или иным процессом, действующими от лица пользователя. Windows NT отслеживает все попытки доступа и позволяет управлять доступом как к объектам, которые пользователи могут просматривать с помощью пользовательского интерфейса (например, файлам и принтерам), так и к абстрактным объектам, которые с помощью пользовательского интерфейса просмотреть нельзя (к ним относятся, например, процессы и именованные каналы).

Администратор системы присваивает пользователям и группам права доступа (permissions), с помощью которых можно предоставить или отклонить пользовательский доступ к объектам. Возможность избирательного присвоения прав доступа по усмотрению владельца объекта (или пользователя, уполномоченного изменять права доступа), называется избирательным контролем доступа (discretionary access control).

Система безопасности идентифицирует пользователей с помощью идентификатора безопасности (security ID, SID). Уникальность идентификаторов безопасности гарантирована, и существование двух идентичных SID полностью исключено. Когда пользователь регистрируется в системе, Windows NT создает маркер безопасности доступа (security access token). В состав маркера безопасного доступа входят SID пользователя, SID всех групп, к которым этот пользователь принадлежит, а также дополнительная информация о пользователе и его группах. Кроме того, любой процесс, работающий от имени пользователя, получает копию его маркера безопасного доступа. Когда пользователь пытается получить доступ к объекту, Windows NT ссылается на содержащийся в маркере безопасного доступа SID. Идентификаторы безопасности (SID) сравниваются со списком контроля доступа к объекту, чтобы гарантировать, что пользователь имеет достаточные права.

Диапазон средств защиты файлов можно установить как на базе подхода "по файлам", так и на базе подхода "по каталогам". Чтобы воспользоваться всей властью над отдельными файлами, их следует расположить на томах с NTFS. Windows NT поддерживает для совместимости с MS DOS работу с FAT, но эта файловая система была разработана без учета требований безопасности. Чтобы воспользоваться всеми преимуществами защиты Windows NT, необходимо использовать файловую систему NTFS.

Системные принтеры можно защитить, не позволяя конкретным пользователям отправлять на них задания (постоянно или только в течение указанного времени суток).

3.4.3 Результаты и выводы:

В ходе практической работы, студент освоил материал о доменной политике безопасности Windows, а также изучил основы безопасности в Windows NT.

3.5 Практическое занятие № 5 (2 часа).

Тема: «Управление программами»

3.5.1 Задание для работы:

1. Понятие программы.
2. Виртуальные программы.

3.5.2 Краткое описание проводимого занятия:

1. Понятие программы.

Компьютерная программа — это последовательность инструкций, которая предназначена для исполнения вычислительной машиной. Образ программы, чаще всего, хранится в памяти машины (например, на *диске*) как исполняемый модуль (один или несколько файлов). Из образа на диске с помощью специального программного загрузчика может быть построена исполняемая программа уже в оперативной памяти машины.

Термин «*компьютерная программа*» в зависимости от своего контекста, может применяться также к *исходным текстам* (или кодам) программы. Их примеры могут быть просмотрены в специальных каталогах исходников. Вместе с правилами и процедурами, а

также с документацией по функционированию программных систем обработки данных, компьютерные программы составляют понятие программного обеспечения.

В системном программировании имеет место более формальное определение *программы* как машинных кодов и данных, загруженных в оперативную память компьютера, и исполняемых процессором машины для достижения поставленной цели. В этом определении подчеркиваются две особенности компьютерной программы: нахождение ее в памяти и исполнение процессором машины.

Процесс создания компьютерной программы называется «программированием», а люди, занимающиеся этим видом деятельности, называются программистами. При разработке компьютерных программ в них довольно часто возникают ошибки. Считается, что в программе содержатся ошибки, если для каких-то данных программа дает неправильные результаты, сбои или отказы. Если программа выдает правильные результаты обработки для всех возможных входных данных, то можно считать, что она не содержит ошибок.

Процесс поиска ошибок в программах и их исправления называется отладкой программ. Обычно, заранее неизвестно, сколько ошибок содержит программа. По этой причине заранее неизвестна и продолжительность отладки программ.

Запись исходных текстов компьютерных программ при помощи специальных *языков программирования* (*ЯП*) облегчает человеку понимание и редактирование программ. Этому, также, помогают *комментарии*, допускаемые синтаксисом большинства языков программирования. Для выполнения программы на компьютере ее готовый исходный текст преобразуется (*компилируется* или *интерпретируется*) в *машинный код*, исполняемый процессором.

Программы с исходными текстами, доступными для прочтения и изменения любым желающим, называются открытыми программами. Любая компьютерная программа является объектом авторского права. Авторы или собственники программ имеют право ограничивать и даже полностью закрывать доступ к их исходным текстам, которые являются интеллектуальной собственностью правообладателей.

Некоторые языки программирования (интерпретируемые) позволяют обойтись без предварительной компиляции написанных на них программ, и специальные *программы-интерпретаторы*переводят такие программы в машинный код уже во время исполнения программы. Этот процесс называется интерпретированием или динамической компиляцией. Он позволяет улучшить переносимость программ между различными программными и аппаратными платформами. Интерпретируемые программы часто называются сценариями или скриптами.

В большинстве распространенных ЯП исходные тексты программ состоят из списков инструкций, описывающих заложенный в программе алгоритм. Такой подход называется императивным. Но применяются и иные методологии программирования. Так, например, в декларативном программировании описываются исходные и требуемые характеристики обрабатываемых данных, а выбор подходящего алгоритма решения описанной задачи поручается специализированной программе-интерпретатору. Применяются также *логическое* и *функциональное* программирование.

2. Виртуальные программы.

Иногда возникает необходимость получить второй компьютер, на котором можно установить другую операционную систему или безопасно протестировать программы. С этой задачей Вам поможет справиться виртуальная машина.

Виртуальная машина – программа, которая эмулирует реальный (физический) компьютер со всем его компонентами (жёсткий диск, привод, BIOS, сетевые адаптеры и т.д.). На такой виртуальный компьютер можно установить операционную систему, драйверы, программы и т.д. Таким образом, Вы можете запустить на своем реальном компьютере еще несколько виртуальных компьютеров, с такой же или другой операционной системой. Вы можете без проблем осуществить обмен данными между Вашим реальным и виртуальным компьютером.

Зачем нужна виртуальная машина

Не каждому пользователя ПК нужна виртуальная машина, но продвинутые пользователи довольно часто используют ее. Виртуальную машину используют для различных целей и задач:
Установка второй/другой операционной системы;
Тестирование программного обеспечения;
Безопасный запуск подозрительных программ;
Эмуляция компьютерной сети;
Запуск приложений, которые нельзя запустить из Вашей операционной системы.
На Вашем реальном компьютер может быть установлена операционная система Windows 7, а на виртуальную машину можно поставить Windows XP, Windows 8 или Linux.
Если Вам нужно выбрать программу (например, видео плеер) Вам нужно установить несколько подобных программ, и определить какая из них Вам больше нравится. Что бы ни захламлять Ваш компьютер, протестируйте программы на виртуальной машине.

Обзор виртуальных машин
Существует большое количество различных программ для создания и управления виртуальными компьютерами. Сейчас мы рассмотрим 3 самые популярные программы.
Виртуальная машина VirtualBox

VirtualBox – бесплатная виртуальная машина, на которую можно установить все самые популярные операционные системы. VirtualBox поддерживает работу с Windows, Linux, FreeBSD, Mac OS.

Виртуальная машина VMware

VMware – наиболее известная и распространенная виртуальная машина. VMware как правило используют для работы крупные площадки или корпорации.
VMware поставляется в двух видах: Workstation и Player. VMware Workstation отличная, но платная виртуальная машина. VMware Player – бесплатная урезанная версия VMware Workstation.

3.5.3 Результаты и выводы:

В ходе практической работы, студент освоил материал о практическом управлении программами. Также был более глубоко усвоен лекционный материал.

3.6 Практическое занятие № 6 (2 часа).

Тема: «Разработка защищенных приложений. Программное управление учетной записью»

3.6.1 Задание для работы:

1. Методы разработки защищенных приложений.
2. Области применения.

3.6.2 Краткое описание проводимого занятия:

3. Методы разработки защищенных приложений.

Основная часть уязвимостей появляется на ранних стадиях создания программного обеспечения. Поэтому, наибольшей эффективностью обладает подход, который устраняет проблемы безопасности на начальной стадии разработки приложений, нежели стандартный метод их исправления по необходимости. Консультанты моделируют потенциальные угрозы безопасности еще до создания программного продукта, что позволяет закрыть всевозможные бреши на стадии его разработки.

Глубокие знания процесса разработки прикладных приложений, позволяют им устранять существующие бреши в программном обеспечении, а также избежать потенциальных уязвимостей при создании собственного продукта.

Специалисты регулярно проводят проверку безопасности:

- сайтов интернет торговли, банков, финансовых и других учреждений;
- программного продукта для разработчиков, интернет-порталов и настольных систем.

Наша компания предлагает полный объем услуг по обеспечению информационной безопасности бизнес проектов, включая:

- оценка уязвимости встроенных систем;
- устранение брешей в системе предварительно записанных голосовых сообщений IVR;
- обнаружение «дыр» в настольных и мобильных приложениях, оценка величины рисков, практические рекомендации по их снижению;
- моделирование потенциальных угроз безопасности приложений, а также обнаружение и устранение их на ранней стадии разработки;
- определение уязвимостей, рисков, прочих угроз безопасности в инфраструктуре веб-подразделений организации;
- повышения уровня безопасности установленных приложений, проверка скриптов и исходного программного кода, устранение выявленных ошибок;
- оценка потенциальных способов проникновения хакеров в веб-приложение, обнаружение уязвимостей рабочих версий веб-порталов, определение степени коммерческих рисков и проведение консультаций по их снижению.

4. Области применения.

Как правило, при развертывании Web-приложения прежде всего требуется обеспечить, чтобы анонимные клиенты не могли обращаться к ценным ресурсам через интернет. Если приложение работает в интрасети, то для аутентификации клиентов обычно применяются

средства Windows (подробнее об управлении доступом я расскажу чуть позже), а приложение защищается от внешнего доступа межсетевым экраном (брандмауэром). С интернет-приложениями дело обстоит сложнее, поскольку нужен хотя бы минимальный уровень доступа для анонимных пользователей, обращающихся через интернет. Если не принимать в расчет эти различия, можно руководствоваться следующими принципами, в равной мере применимыми к защите интернет-приложений и приложений интрасети. Идеальный вариант — в Web-пространстве имен вашего приложения не должно быть никаких файлов, которые не планируется передавать клиентам. То есть все такие файлы надо удалить из физической структуры каталогов, начинающейся с самого верхнего каталога, помеченного в конфигурации IIS как Web-приложение или виртуальный каталог. Если файл не принадлежит Web-пространству имен, он не будет доступен при запросах к этому пространству, если только ваше приложение не выполнит явные операции по открытию этого файла и передаче его содержимого. Если ваше приложение программно обращается к данным или вспомогательным файлам, размещайте их вне Web-пространства имен.

Сферы применения:

- Установление защищенного удаленного доступа к внутренним информационным ресурсам организации: электронной почте, календарям сотрудников, адресной книге организации, внутренним порталам, библиотекам файлов и документов, системам управления совещаниями, спискам задач и др.
- Обеспечение юридически значимого электронного документооборота с применением сертифицированных средств криптографической защиты информации.
- Взаимодействие с площадками электронных торгов и аукционов, b2b услуг, госуслуг.
- Обеспечение конфиденциальности электронных почтовых сообщений.
- Обеспечение конфиденциальности информации, хранимой на мобильном устройстве.

3.6.3 Результаты и выводы:

В ходе практической работы, студент знакомится с защищенными приложениями и областью их применения.

3.7 Практическое занятие № 7 (2 часа).

Тема: «Управление процессами»

3.7.1 Задание для работы:

1.Понятия процесса и потока.
2.Состояния процессов.

3.7.2 Краткое описание проводимого занятия:

1.Понятия процесса и потока.

Термин «процесс» впервые появился при разработке операционной системы Multix и имеет несколько определений, которые используются в зависимости от контекста, согласно которым **процесс** — это:

4. программа на стадии выполнения
5. «объект», которому выделено процессорное время
6. асинхронная работа

Для описания состояний процессов используется несколько моделей. Самая простая — модель трех состояний. Она определяет следующие состояния процесса:

4. состояния выполнения
5. состояния ожидания
6. состояния готовности

Выполнение — это *активное состояние*, во время которого процесс обладает всеми необходимыми ему ресурсами. В этом состоянии процесс непосредственно выполняется процессором.

Ожидание — это *пассивное состояние*, во время которого процесс заблокирован и не может быть выполнен, потому что ожидает какое-то событие, например, ввода данных или освобождения нужного ему устройства.

Готовность — это тоже пассивное состояние, процесс тоже заблокирован, но в отличие от состояния ожидания, он заблокирован не по внутренним причинам (ведь ожидание ввода данных — это внутренняя, «личная» проблема процесса — он может ведь и не ожидать ввода данных и свободно выполняться — никто ему не мешает), а по внешним, независящим от процесса, причинам.

Потоки

Концепция процесса, пришедшая из мира UNIX, плохо реализуется в многозадачной системе, поскольку процесс имеет тяжелый контекст. Возникает понятие **потока (thread)**, который понимается как подпроцесс, или *легковесный процесс (light-weight process)*, выполняющийся в контексте полноценного процесса.

С помощью процессов можно организовать параллельное выполнение программ. Для этого процессы клонируются вызовами fork() или exec(), а затем между ними организуется взаимодействие средствами IPC. Это довольно дорогостоящий в отношении ресурсов способ.

С другой стороны, для организации параллельного выполнения и взаимодействия процессов можно использовать механизм многопоточности. Основной единицей здесь является **поток**, который представляет собой облегченную версию процесса. Чтобы понять, в чем состоит его особенность, необходимо вспомнить основные характеристики процесса.

3. Процесс располагает определенными ресурсами. Он размещен в некотором виртуальном адресном пространстве, содержащем образ этого процесса. Кроме того, процесс управляет другими ресурсами (файлы, устройства ввода/вывода и т.д.).
4. Процесс подвержен диспетчеризации. Он определяет порядок выполнения одной или нескольких программ, при этом выполнение может перекрываться другими процессами. Каждый процесс имеет состояние выполнения и приоритет диспетчеризации.

Если рассматривать эти характеристики независимо друг от друга (как это принято в современной теории ОС), то:

- владельцу ресурса, обычно называемому процессом или задачей, присущи:
  - виртуальное адресное пространство;
  - индивидуальный доступ к процессору, другим процессам, файлам, и ресурсам ввода — вывода.
- Модулю для диспетчеризации, обычно называемому потоком или облегченным процессом, присущи:
  - состояние выполнения (активное, готовность и т.д.);
  - сохранение контекста потока в неактивном состоянии;
  - стек выполнения и некоторая статическая память для локальных переменных;
  - доступ к пространству памяти и ресурсам своего процесса.

Все потоки процесса разделяют общие ресурсы. Изменения, вызванные одним потоком, становятся немедленно доступны другим.

При корректной реализации потоки имеют определенные преимущества перед процессами. Им требуется:

- меньше времени для создания нового потока, поскольку создаваемый поток использует адресное пространство текущего процесса;
- меньше времени для завершения потока;
- меньше времени для переключения между двумя потоками в пределах процесса;
- меньше коммуникационных расходов, поскольку потоки разделяют все ресурсы, и в частности адресное пространство. Данные, продуцируемые одним из потоков, немедленно становятся доступными всем другим потокам.

.

2.Состояния процессов

Состояние процессов

В многозадачной (многопроцессной) системе процесс может находиться в одном из трех основных состояний:

ВЫПОЛНЕНИЕ - активное состояние процесса, во время которого процесс обладает всеми необходимыми ресурсами и непосредственно выполняется процессором;

ОЖИДАНИЕ - пассивное состояние процесса, процесс заблокирован, он не может выполняться по своим внутренним причинам, он ждет осуществления некоторого события, например, завершения операции ввода-вывода, получения сообщения от другого процесса, освобождения какого-либо необходимого ему ресурса;

ГОТОВНОСТЬ - также пассивное состояние процесса, но в этом случае процесс заблокирован в связи с внешними по отношению к нему обстоятельствами: процесс имеет все требуемые для него ресурсы, он готов выполняться, однако процессор занят выполнением другого процесса.

В ходе жизненного цикла каждый процесс переходит из одного состояния в другое в соответствии с алгоритмом планирования процессов, реализуемым в данной операционной системе. Типичный граф состояний процесса показан на рисунке 2.1.

В состоянии ВЫПОЛНЕНИЕ в однопроцессорной системе может находиться только один процесс, а в каждом из состояний ОЖИДАНИЕ и ГОТОВНОСТЬ - несколько процессов, эти процессы образуют очереди соответственно ожидающих и готовых процессов. Жизненный цикл процесса начинается с состояния ГОТОВНОСТЬ, когда процесс готов к выполнению и ждет своей очереди. При активизации процесс переходит в состояние ВЫПОЛНЕНИЕ и находится в нем до тех пор, пока либо он сам освободит процессор, перейдя в состояние ОЖИДАНИЯ какого-нибудь события, либо будет насильно "вытеснен" из процессора, например, вследствие исчерпания отведенного данному процессу кванта процессорного времени. В последнем случае процесс возвращается в состояние ГОТОВНОСТЬ. В это же состояние процесс переходит из состояния ОЖИДАНИЕ, после того, как ожидаемое событие произойдет.

3.7.3 Результаты и выводы:

В ходе практической работы, студент изучил понятием потока и процесса, различные состояния потоков и процессов.

3.8 Практическое занятие № 8 (2 часа).

Тема: «Политика безопасности. Управление правами и привилегиями пользователей**»**

3.8.1 Задание для работы:

1. Управление правами и привилегиями пользователей.
2. Политика безопасности в РФ.

3.8.2 Краткое описание проводимого занятия:

1. Управление правами и привилегиями пользователей.

Пользовательские права – это настройки для компьютера, контролирующие то, что пользователь (или группа пользователей) может делать с компьютером. Например, если у вас есть право на резервное копирование файлов на каком-то компьютере, это означает, что вы можете сделать копию ЛЮБОГО файла, хранящегося на данном компьютере, даже файлов ОС, файлов для администраторов или любых других файлов. В общем, это относится ко всему компьютеру, а не к отдельным файлам или папкам.

Разрешения – то, что настраивается для контроля доступа к ресурсам. Ресурс – это файл, папка, ключ реестра, принтер или объект Active Directory (на контроллере домена). Разрешения настраиваются в Access Control List (ACL – Список контроля доступа). Разрешения определяют, «кто» и «что» можно делать с ресурсом. Примеры: Read(чтение), Modify(изменение), Delete(удаление) и т.д.

Локальная группа – эти группы хранятся в локальном Security Accounts Manager (SAM) компьютера (или сервера). Локальные группы действуют только в рамках того компьютера, на котором они располагаются. То есть, если пользователь участвует в локальной группе, возможности, обеспечиваемые локальной группой, распространяются только на тот компьютер, где находится группа.

Наименьшие привилегии – это принцип, впервые представленный министерством обороны (Department of Defense – DoD). Смысл его в том, что пользователю даются только минимальные привилегии, необходимые для выполнения задач. Если пользователю требуется запускать ключевое бизнес-приложение с администраторскими правами, они должны быть обеспечены пользователю. Однако, когда этот пользователь запускает Microsoft Word, он должен получать доступ к нему только как стандартный пользователь.

Общая безопасность настольного ПК

Для корпоративных сред общая задача состоит в том, чтобы позволить пользователям запускать приложения, устанавливать нужные программы и драйверы, запускать службы операционной системы, делать то, что приносит компании доход, но при этом выдавать пользователям наименьшие из возможных привилегий.

Часто я слышу от многих администраторов, что они хотят установить ограничения для каждого пользователя, определив, к каким компьютерам у них есть доступ, реализуя таким образом свою модель безопасности. И хотя я считаю, что в таком методе есть смысл, он очень трудоемок, и делает среду очень запутанной в управлении и при решении возникающих проблем.

Если безопасность хорошо проработана для каждого настольного ПК, тогда допуск каждого пользователя к каждому ПК не должен стать проблемой с точки зрения информационной безопасности. При этом правильно настроены должны быть пользовательские права, разрешения, участие в локальных группах и реализация принципа наименьших привилегий для приложений, установок и функций ОС.

Пользовательские права

Пользовательские права – это настройки, контролирующие различные аспекты работы настольного ПК. В сущности, эти права обеспечивают или запрещают наивысший уровень возможностей в отношении ПК. Когда я говорю о наивысшем уровне, я имею в виду уровень всего компьютера, а не отдельных файлов или папок. Когда право определено для ПК, оно включает в себя действие над чем угодно на этом компьютере.

Есть некоторые права пользователя, содержащие более высокую степень риска по сравнению с другими. Например, есть такое право – «Shut down the System»(Завершение работы). Это возможность, которую должен иметь любой пользователь. То есть, нет ничего страшного в том, чтобы дать такое право каждому пользователю. А вот если рассмотреть право «Act as part of the operating system»(Работа в режиме операционной системы), очевидно, что обычному пользователю его выдавать не следует.

2. Политика безопасности в РФ.

Доктрина информационной безопасности Российской Федерации — совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации была утверждена 9 сентября 2000 года Президентом Российской Федерации В.В. Путиным.

Информационная безопасность - это состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Составляющие доктрины:

1) Обязательное соблюдение конституционных прав и свобод человека в области получения информации и пользования ею.
2) Информационное обеспечение государственной политики РФ(доведение до граждан РФ и международной общественности о государственной политике РФ, официальной позиции по значимым событиям в России и в мире) с доступом граждан к открытым государственным ресурсам.
3) Развитие современных ИТ отечественной индустрии (средств информатизации, телекоммуникации и связи). Обеспечение ИТ внутреннего рынка России и выход на мировые рынки.
4) Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Виды угроз:

1. Угрозы, направленные на конституционные права и свободы человека в области информационной деятельности.
2. Угрозы информационному обеспечению государственной политики РФ.
3. Угроза развитию современных ИТ отечественной индустрии, а также выходу на внутренний и мировой рынок.
4. Угрозы безопасности информационных и телекоммуникационных средств и систем.

Методы обеспечения информационной безопасности РФ в доктрине:

Правовые методы
- Разработка нормативных правовых актов, регламентирующих отношения в сфере ИТ
- разработка нормативных методических документов отвечающим по вопросам информационной безопасности РФ

Организационно-технические методы
- создание системы информационной безопасности РФ и её совершенствование
- привлечение лиц к ответственности, совершивших преступления в этой сфере
- создание систем и средств для предотвращения несанкционированного доступа к обрабатываемой информации
- выявление средств и устройств, представляющих опасность для нормального функционирования систем - предотвращение перехвата информации с применением средств криптографической защиты как при передаче информации, так и при её хранении
- контроль за выполнением требований по защите информации
- контроль за действиями персонала, имеющих доступ к информации, подготовка кадров в области обеспечения информационной безопасности РФ
- создание системы мониторинга информационной безопасности РФ

Экономические методы

- разработка программ обеспечения информационной безопасности и их финансирование
- финансирование работ, связанных с обеспечением информационной безопасности РФ

3.8.3 Результаты и выводы:

В ходе практической работы, студент знакомится с политикой безопасности в РФ, а также с правами и привилегиями пользователей.

3.9 Практическое занятие № 9 (2 часа).

Тема: «Организация управления доступом и защиты ресурсов ОС»

3.9.1 Задание для работы:

1. Основы защиты ОС.
2. Практические методы защиты.

3.9.2 Краткое описание проводимого занятия:

3. Основы защиты ОС.

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.

4. Практические методы защиты.

Есть несколько простых правил, соблюдая которые, можно не беспокоиться о своей безопасности:

Скачивать программы можно ТОЛЬКО из надежных источников и как можно меньше со всяческих якобы "хакерских" сайтов... Львиная доля Троянов приходится именно на файлы с этих серверов.

Если скачали какую-то программу - ОБЯЗАТЕЛЬНО необходимо проверить ее на наличие вирусов и других вредоносных программ.

Никогда не надо запускать программы, пришедшие по E-MAIL.

В качестве паролей надо всегда использовать замысловатые наборы символов, типа Jqp2FQs, и по возможности стараться их вводить в окне терминала вручную - это обезоружит Троянов, отсылающих пароли на чей-то E-MAIL адрес.

Следует ограничить число посторонних, имеющих доступ к компьютеру, поскольку достаточно большое число троянов и вирусов переносится на внешних носителях (дискетах и дисках). Также рекомендуется периодически менять пароли на особо важные аккаунты.

Те троянские программы, которые постоянно обеспечивают доступ к зараженной ЭВМ, а, следовательно, держат на ней открытый порт какого-либо транспортного протокола, можно обнаруживать с помощью утилит контроля за сетевыми портами. Например, для операционных систем клона Microsoft Windows такой утилитой является программа NetStat. Запуск ее с ключом "netstat - a" выведет на экран все активные порты ЭВМ. От оператора в этом случае требуется знать порты стандартных сервисов, которые постоянно открыты на ЭВМ, и тогда, любая новая запись на мониторе должна привлечь его внимание. На сегодняшний день существует уже несколько программных продуктов, производящих подобный контроль автоматически.

Ещё один способ обнаружить троянцев - посмотреть открытые порты компьютера и процессы, которые их открыли. Обычно троянская программа использует порты >1000

(например, 30003,47891,6666,31337). Список портов, использующихся троянскими программами - Приложение 1.

В Windows XP Professional SP2 есть встроенное средство защиты - брандмауэр Windows.

Брандмауэр (межсетевой экран или фаервол) - комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Брандмауэры бывают двух видов, программные и аппаратные.

Брандмауэр используется для защиты компьютера от несанкционированного доступа через сеть или Интернет. Брандмауэр Windows встроен в Windows XP и включен автоматически для защиты компьютера от вирусов и других угроз безопасности. Брандмауэр отличается от антивирусного программного обеспечения, однако их совместная работа обеспечивает надежную защиту компьютера. Можно сказать, что брандмауэр охраняет окна и двери от проникновения неизвестных и нежелательных программ, в то время как антивирусное программное обеспечение предотвращает появление вирусов или других угроз безопасности, которые стремятся пробраться через парадный вход. В Microsoft Windows XP (SP2) брандмауэр Windows включен по умолчанию. Необязательно использовать именно брандмауэр Windows - можно установить и включить любой брандмауэр по выбору.

3.9.3 Результаты и выводы:

В ходе практической работы студент освоил организацию управления доступом и защиты ресурсов операционной системы, а также практические методы ее защиты.

3.10 Практическое занятие № 10 (2 часа).

Тема: «Разработка защищенных приложений. Программное управление файловыми ресурсами и сессиями»

3.10.1 Задание для работы:

1. Типы защищённых приложений.
2. Основные компоненты программы и их управление.

3.10.2 Краткое описание проводимого занятия:

1. Типы защищённых приложений.

Основная часть уязвимостей появляется на ранних стадиях создания программного обеспечения. Поэтому, наибольшей эффективностью обладает подход, который устраняет проблемы безопасности на начальной стадии разработки приложений, нежели стандартный метод их исправления по необходимости. Консультанты моделируют потенциальные угрозы безопасности еще до создания программного продукта, что позволяет закрыть всевозможные бреши на стадии его разработки.

Глубокие знания процесса разработки прикладных приложений, позволяют им устранять существующие бреши в программном обеспечении, а также избежать потенциальных уязвимостей при создании собственного продукта.
Специалисты регулярно проводят проверку безопасности:

- сайтов интернет торговли, банков, финансовых и других учреждений;
- программного продукта для разработчиков, интернет-порталов и настольных систем.

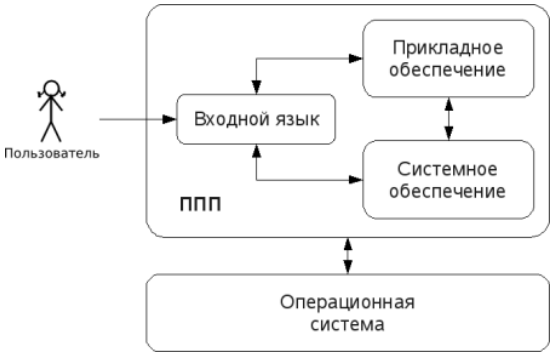
Наша компания предлагает полный объем услуг по обеспечению информационной безопасности бизнес проектов, включая:

- оценка уязвимости встроенных систем;
- устранение брешей в системе предварительно записанных голосовых сообщений IVR;
- обнаружение «дыр» в настольных и мобильных приложениях, оценка величины рисков, практические рекомендации по их снижению;
- моделирование потенциальных угроз безопасности приложений, а также обнаружение и устранение их на ранней стадии разработки;
- определение уязвимостей, рисков, прочих угроз безопасности в инфраструктуре веб-подразделений организации;
- повышения уровня безопасности установленных приложений, проверка скриптов и исходного программного кода, устранение выявленных ошибок;
- оценка потенциальных способов проникновения хакеров в веб-приложение, обнаружение уязвимостей рабочих версий веб-порталов, определение степени коммерческих рисков и проведение консультаций по их снижению.

2. Основные компоненты программы и их управление.

Со времени появления первых компьютеров появилось множество прикладных разработок, но, несмотря на разнообразие, их обобщенную внутреннюю структуру можно представить в виде трех взаимосвязанных элементов (рис. 1):

1. входной язык (макроязык, язык управления) — представляет средство общения пользователя с пакетом;
2. предметное обеспечение (функциональное наполнение) — реализует особенности конкретной предметной области;
3. системное обеспечение (системное наполнение) — представляет низкоуровневые средства, например, доступ к функциям операционной системы.



Входной язык — основной инструмент при работе пользователя с пакетом прикладных программ. В качестве входного языка могут использоваться как универсальные (Pascal, Basic и т.п.), так и специализированные, проблемно-ориентированные языки программирования (Cobol — для бизнес-приложений, Lisp — списочные структуры данных, Fortran и MathLAB — математические задачи и т.п.).

Развитый пакет может обладать несколькими входными языками, предназначенными для выполнения различных функций в рамках решаемого класса задач. Так, например в пакете OpenOffice.org поддерживаются языки StarBasic, Python, JavaScript и Java. StarBasic является основным входным языком, предназначенным для автоматизации работы с пакетом, для этого языка имеется интегрированная среда разработки и встроенный отладчик. Скрипты на языках Python и JavaScript загружаются и исполняются из внешних файлов. На Java (через SDK и функции API OpenOffice) можно создавать модули расширения и полнофункциональные приложения-компоненты.

Входные языки отражают объем и качество предоставляемых пакетом возможностей, а также удобство их использования. Таким образом, именно входной язык является основным показателем возможностей ППП. Однако стоит отметить, что в современных пакетах обращение пользователя к языковым средствам обычно происходит косвенно, через графический интерфейс.

Предметное обеспечение отражает особенности решаемого класса задач из конкретной предметной области и включает:

- программные модули, реализующие алгоритмы (или их отдельные фрагменты) прикладных задач;
- средства сборки программ из отдельных модулей.

Наиболее распространено в настоящее время оформление программных модулей в виде библиотек, подключаемых статически или динамически. В зависимости от использованного разработчиками подхода к проектированию и реализации ППП такие библиотеки содержат встроенные классы и описания их интерфейсов (при использовании объектно-ориентированного программирования). При использовании парадигмы структурного программирования в библиотечных модулях содержатся процедуры и функции, предназначенные для решения некоторых самостоятельных задач. В обоих случаях библиотеки связаны с другими модулями пакета лишь входной и выходной информацией.

Системное обеспечение представляет собой совокупность низкоуровневых средств (программы, файлы, таблицы и т.д.), обеспечивающих определенную дисциплину работы пользователя при решении прикладных задач и формирующих окружение пакета. К системному обеспечению ППП относят следующие компоненты:

- монитор — программа, управляющая взаимодействием всех компонентов ППП;
- транслятор(ы) с входных языков — для ППП характерно использование интерпретируемых языков;
- средства доступа к данным — драйверы баз данных и/или компоненты, представляющие доступ через унифицированные интерфейсы (ODBC, JDBC, ADO, BDE и т.п.);
- информационно-справочный модуль — предоставляет функции поддержки, среди которых информационные сообщения, встроенная справочная системы и т.п.
- различные служебные программы, выполняющие низкоуровневые операции (автосохранение, синхронизация совместно используемых файлов и т.д.)

Приведенная трехкомпонентная логическая структура ППП достаточна условна, она зависит от использованных подходов к проектированию ПО, используемым технологиям программирования, предметной области и других факторов, вплоть до индивидуальных

предпочтений разработчика. Так, в конкретном ППП может отсутствовать четкое разделение программ на предметное и системное обеспечение. Например, программа планирования вычислений, относящаяся к прикладному обеспечению, может одновременно выполнять и ряд служебных функций (информационное обеспечение, связь с операционной системой и т.п.). С другой стороны, распределенные приложениядобавляют свою специфику в структуру ППП.

Кроме того, одни и те же программы в одном пакете могут относиться к предметному обеспечению, а в другом — к системному. Так, программы построения диаграмм в рамках специализированного пакета машинной графики естественно отнести к предметному обеспечению. Однако те же программы следует считать вспомогательными и относящимися к системному обеспечению, например, в пакете решения вычислительных задач.

3.10.3 Результаты и выводы:

В ходе практической работы студент изучил разработку защищенных приложений, а также управление файловыми ресурсами и сессиями.

3.11 Практическое занятие № 11 (2 часа).

Тема: «Анализ симптома атаки и методы защиты»

3.11.1 Задание для работы:

1. Симптомы атаки.
2. Виды атак.

3.11.2 Краткое описание проводимого занятия:

1. Симптомы атаки.

Существует ряд признаков, свидетельствующих о заражении компьютера. Если вы замечаете, что с компьютером происходят "странные" вещи, а именно:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- неожиданно открывается и закрывается лоток CD-ROM-устройства;
- произвольно, без Вашего участия, на вашем компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя Вы никак не инициировали такое ее поведение,

то, с большой степенью вероятности, можно предположить, что ваш компьютер поражен вирусом.

Кроме того, есть некоторые характерные признаки поражения вирусом через почту:

- друзья или знакомые говорят вам о сообщениях от вас, которые вы не отправляли;
- в вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка.

Следует отметить, что не всегда такие признаки вызываются присутствием вирусов. Иногда они могут быть следствием других причин. Например, в случае с почтой

зараженные сообщения могут рассылаться с вашим обратным адресом, но не с вашего компьютера. Существуют также косвенные признаки заражения компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску (часто мигает лампочка на системном блоке);
- Microsoft Internet Explorer "зависает" или ведет себя неожиданным образом (например, окно программы невозможно закрыть).

В 90% случаев наличие косвенных симптомов вызвано сбоем в аппаратном или программном обеспечении. Несмотря на то, что подобные симптомы с малой вероятностью свидетельствуют о заражении, при их появлении рекомендуем вам:

2. Виды атак.

Сетевые атаки столь же разнообразны, как и системы, против которых они направлены. Некоторые атаки отличаются большой сложностью. Другие может осуществить обычный оператор, даже не предполагающий, какие последствия может иметь его деятельность. Для оценки типов атак необходимо знать некоторые ограничения, изначально присущие протоколу TPC/IP. Сеть Интернет создавалась для связи между государственными учреждениями и университетами в помощь учебному процессу и научным исследованиям. Создатели этой сети не подозревали, насколько широко она распространится. В результате, в спецификациях ранних версий интернет-протокола (IP) отсутствовали требования безопасности. Именно поэтому многие реализации IP являются изначально уязвимыми. Через много лет, получив множество рекламаций (RFC - Request for Comments), мы, наконец, стали внедрять средства безопасности для IP. Однако ввиду того, что изначально средства защиты для протокола IP не разрабатывались, все его реализации стали дополняться разнообразными сетевыми процедурами, услугами и продуктами, снижающими риски, присущие этому протоколу. Далее мы кратко обсудим типы атак, которые обычно применяются против сетей IP, и перечислим способы борьбы с ними.

Снифферы пакетов
Сниффер пакетов представляет собой прикладную программу, которая использует сетевую карту, работающую в режиме promiscuous mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки). При этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако ввиду того, что некоторые сетевые приложения передают данные в текстовом формате (telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли).

Перехват имен и паролей создает большую опасность, так как пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи вообще имеют один пароль для доступа ко всем ресурсам и приложениям. Если приложение работает в режиме клиент/сервер, а аутентификационные данные передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам. Хакеры слишком хорошо знают и используют наши человеческие слабости

(методы атак часто базируются на методах социальной инженерии). Они прекрасно знают, что мы пользуемся одним и тем же паролем для доступа к множеству ресурсов, и поэтому им часто удается, узнав наш пароль, получить доступ к важной информации. В самом худшем случае хакер получает доступ к пользовательскому ресурсу на системном уровне и с его помощью создает нового пользователя, которого можно в любой момент использовать для доступа в сеть и к ее ресурсам.

IP-спуфинг происходит, когда хакер, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, хакер может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример - атака DoS, которая начинается с чужого адреса, скрывающего истинную личность хакера.

Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи хакер должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые хакеры, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения.

DoS, без всякого сомнения, является наиболее известной формой хакерских атак. Кроме того, против атак такого типа труднее всего создать стопроцентную защиту. Даже среди хакеров атаки DoS считаются тривиальными, а их применение вызывает презрительные усмешки, потому что для организации DoS требуется минимум знаний и умений. Тем не менее, именно простота реализации и огромный причиняемый вред привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность.

3.12 Практическое занятие № 12 (2 часа).

Тема: «Анализ установок безопасности системы»

3.12.1 Задание для работы:

1. Основные параметры защиты.
2. Характеристики установок безопасности.

3.12.2 Краткое описание проводимого занятия:

1. Основные параметры защиты.

К процедурному уровню относятся меры безопасности, реализуемые сотрудниками предприятия. Выделяются следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

В рамках управления персоналом для каждой должности должны существовать квалификационные требования по информационной безопасности. В должностные инструкции должны входить разделы, касающиеся защиты информации. Каждого

сотрудника предприятия необходимо обучить мерам обеспечения информационной безопасности теоретически и отработать выполнение этих мер практически.
Информационная безопасность ИС предприятия зависит от окружения, в котором она работает. Необходимо принять меры для обеспечения физической защиты зданий и прилегающей территории, поддерживающей инфраструктуры и самих компьютеров.
При разработке проекта СОИБ предполагается адекватная реализация мер физической защиты офисных зданий и других помещений, принадлежащих предприятию, по следующим направлениям:

- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры.

Предполагается также адекватная реализация следующих направлений поддержания работоспособности:

- поддержка пользователей ИС;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;
- регламентные работы.

Программа информационной безопасности должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.
Реакция на нарушения режима информационной безопасности преследует две главные цели:

- блокирование нарушителя и уменьшение наносимого вреда;
- недопущение повторных нарушений.

На предприятии должен быть выделен сотрудник, доступный 24 часа в сутки, отвечающий за реакцию на нарушения. Все пользователи ИС должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В случае невозможности связи с данным сотрудником, должны быть разработаны и внедрены процедуры первичной реакции на информационный инцидент.
Планирование восстановительных работ позволяет подготовиться к авариям ИС, уменьшить ущерб от них и сохранить способность к функционированию, хотя бы в минимальном объеме.
Механизмы контроля, существенные для предприятия с юридической точки зрения, включают в себя:

- Защиту данных и тайну персональной информации;
- Охрану документов организации;
- Права на интеллектуальную собственность.

В соответствии с международным стандартом ISO 17799, а также руководящими документами ФСТЭК, ключевыми также являются следующие механизмы контроля:

- Политика информационной безопасности;
- Распределение ролей и ответственности за обеспечение информационной безопасности;
- Обучение и тренинги по информационной безопасности;
- Информирование об инцидентах безопасности;
- Управление непрерывностью бизнеса.

Меры обеспечения информационной безопасности программно-технического уровня
Программно-технические средства защиты располагаются на следующих рубежах:

- Защита внешнего периметра КСПД;

- Защита внутренних сетевых сервисов и информационных обменов;
- Защита серверов и рабочих станций;
- Защита системных ресурсов и локальных приложений на серверах и рабочих станциях;
- Защита выделенного сегмента руководства компании.

На программно-техническом уровне выполнение защитных функций ИС осуществляется следующими служебными сервисами обеспечения информационной безопасности:

- идентификация/аутентификация пользователей ИС;
- разграничение доступа объектов и субъектов информационного обмена;
- протоколирование/аудит действий легальных пользователей;
- экранирование информационных потоков и ресурсов КСПД;
- туннелирование информационных потоков;
- шифрование информационных потоков, критической информации;
- контроль целостности;
- контроль защищенности;
- управление СОИБ.

На внешнем рубеже информационного обмена располагаются средства выявления злоумышленной активности и контроля защищенности. Далее идут межсетевые экраны, защищающие внешние подключения. Они, вместе со средствами поддержки виртуальных частных сетей, объединяемых с межсетевыми экранами, образуют внешний периметр информационной безопасности, отделяющий информационную систему предприятия от внешнего мира.

Сервис активного аудита СОИБ (как и управление) должен присутствовать во всех критически важных компонентах и, в частности, в защитных. Это позволит быстро обнаружить атаку, даже, если по каким-либо причинам, она окажется успешной.

Управление доступом также должно присутствовать на всех сервисах, функционально полезных и инфраструктурных. Доступу пользователя к ИС предприятия должна предшествовать идентификация и аутентификация субъектов информационного обмена (пользователей и процессов).

Средства шифрования и контроля целостности информации, передаваемой по каналам связи, целесообразно выносить на специальные шлюзы, где им может быть обеспечено квалифицированное администрирование.

Последний рубеж образуют средства пассивного аудита, помогающие оценить последствия реализации угроз информационной безопасности, найти виновного, выяснить, почему успех атаки стал возможным.

Расположение средств обеспечения высокой доступности определяется критичностью соответствующих сервисов или их компонентов.

2.Характеристики установок безопасности

Установки безопасности ОС:

- препятствие;
- управление доступом;
- механизмы шифрования;
- противодействие атакам вредоносных программ;
- регламентация;
- принуждение;
- побуждение.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Управление доступом включает следующие функции зашиты:

· идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

· опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

· проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

· разрешение и создание условий работы в пределах установленного регламента;

· регистрацию (протоколирование) обращений к защищаемым ресурсам;

· реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

Принуждение – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Вся совокупность технических средств подразделяется на *аппаратные* и *физические*.

Аппаратные средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – это специальные программы и программные комплексы, предназначенные для защиты информации в ИС. Как отмечалось, многие из них слиты с ПО самой ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). Криптография – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер

реализуется группой информационной безопасности, но должен находиться под контролем первого руководителя.

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения (которые традиционно сложились ранее), складываются по мере распространения ИС и ИТ в стране и в мире или специально разрабатываются. Морально-этические нормы могут быть неписаные (например честность) либо оформленные в некий свод (устав) правил или предписаний. Эти нормы, как правило, не являются законодательно утвержденными, но поскольку их несоблюдение приводит к падению престижа организации, они считаются обязательными для исполнения. Характерным примером таких предписаний является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США.

3.12.3 Результаты и выводы:

В ходе практической работы студент освоил анализ установок безопасности системы. Также студент более глубоко изучил материал.

3.13 Практическое занятие № 13 (2 часа).

Тема: «Основные механизмы безопасности: средства и методы аутентификации в ОС**»**

3.13.1 Задание для работы:

1. Мотивации, как функция управления.
2. Необходимость контроля. Этапы контроля.

3.13.2 Краткое описание проводимого занятия:

1. Мотивации, как функция управления.

Природа мотивации. Для достижения целей организации руководству необходимо обеспечить эффективные действия персонала. Для этого нужно не только обеспечить функциональную загрузку работников и создать им необходимые условия, но и вызвать у них желание энергично совершать именно те действия, которые приближают организации к достижению поставленных целей. В связи с этим руководство организации должно выполнять весьма важную функцию - создание условий для мотивации работников и осуществление ее на практике.

Мотивация как функция управления — это процесс, с помощью которого руководство организации побуждает работников действовать так, как было ранее запланировано и организовано, поскольку успех организации в определенной мере зависит от того, насколько эффективно действуют участники производственного процесса. Таким образом, *мотивацию в организации* можно трактовать как *побуждение членов организации к действию.* При этом мотивация представляет собой, с одной стороны, побуждение, навязанное индивидам извне, а с другой — это самопобуждение.

Чтобы разобраться в этой двойственной природе мотивации, важно понять, что поведение человека в трудовом процессе определяется взаимодействием различных внешних и внутренних побудительных сил, среди которых следует прежде всего выделить

стимулы и мотивы. Стимул понимается как внешняя причина, побуждающая людей к деятельности, а мотив выступает как внутренняя побудительная сила. Если стимул заметен, его можно заранее спланировать или отменить, то мотив скрыт, его действие часто бывает неожиданным для наблюдателей, так как он зависит от инстинктивных импульсов, влечений, потребностей.

Вместе с тем стимулы и мотивы самым тесным образом связаны между собой. Процесс стимулирования деятельности члена организации — это такое воздействие на его поведение, которое включает в свою сферу все потребности, интересы, цели, стремления, мотивы. Следовательно, основу стимулирования составляет взаимодействие внешних условий и внутренней структуры личности члена организации. Стимулирование реализуется через создание условий, изменяющих трудовую ситуацию, чтобы у работника возникало желание, стремление к эффективной деятельности. Однако для успешного стимулирования необходимо знать внутренние мотивы, которые можно приобрести, только изучая социологию и психологию личности.

Обращение к изучению поведения людей в организации обусловлено тем, что не всякое целевое, направленное воздействие на поведение человека активизирует его деятельность, а лишь то, которое становится личностно значимым для данного конкретного человека, соответствует его внутренним устремлениям. Только в этом случае возникает заинтересованность работника в своей деятельности, психологическая предрасположенность по отношению к выполнению ролевых требований и, как следствие этого, побуждение к качественному выполнению работы. Стимулирование включает в себя не только создание внешней ситуации выбора определенной (наиболее привлекательной) формы поведения, но и ее соответствие структуре личности работника. Вместе с внешней стимуляцией эта внутренняя структура (в случае ее активизации) формирует непосредственный мотив действий.

2. Необходимость контроля. Этапы контроля.

Контроль – это процесс, при помощи которого руководство организации определяет, правильные ли его решения и не нуждаются ли они в корректировке. Контроль – это процесс обеспечения достижения организацией своих целей.

Функция контроля – это такая характеристика управления, которая позволяет выявить проблемы и скорректировать деятельность организации до того, как эти проблемы перерастут в кризис. Сущность контроля заключается в трех основных элементах:

установление контролируемых стандартов деятельности;

измерение и анализ результатов деятельности, информация о которых получена с помощью контроля;

корректировка технологических, хозяйственных и иных процессов в соответствии со сделанными выводами и принятыми решениями.

Без надежной системы контроля ни одна организация не может успешно функционировать. Его задачи следующие.

Во-первых, контроль позволяет обнаружить во внешней или внутренней среде

организации факторы, которые могут оказать существенное влияние на ее функционирование и развитие, и своевременно на них отреагировать.

Во-вторых, контроль помогает вскрыть неизбежные в деятельности любой организации нарушения, изъяны, ошибки и оперативно принять меры к их устранению.

В-третьих, результаты контроля служат основой для оценки работы организации и ее персонала за определенный период, эффективности и надежности системы управления ею.

Различают два основных вида контроля: финансовый и административный.

Различают три стадии управленческого контроля: предварительный, текущий и итоговый.

Предварительный контроль осуществляется до фактического начала работ в области человеческих ресурсы (анализ качеств, необходимых для выполнения работ), материальных ресурсов (стандарты качества, контроль за поступающими материалами), финансовых ресурсов (разработка бюджета, установление предельных значений затрат)

Текущий контроль осуществляется непосредственно в ходе выполнения работ, для этого необходим механизм обратной связи, который позволяет выявить непредвиденные проблемы и скорректировать линию поведения.

Оперативный контроль ориентирован на текущую производственную и хозяйственную деятельность, в частности на движение продукции в рамках технологического процесса (соблюдение последовательности операций, норм времени на их выполнение, качество труда); загрузку техники и оборудования; соблюдение общего графика работы.
Итоговый (заключительный) контроль связан с оценкой выполнения организацией планов и составлением новых; он предполагает всесторонний анализ не только конкретных результатов деятельности за текущий период, но и сильных и слабых ее сторон.
Заключительный контроль используется после выполнения работ и имеет две функции: дает информацию для планирования аналогичной продукции в будущем, способствует мотивации на основе измерения полученных результатов и определения степени вознаграждения.

Причины необходимости контроля.

1. Неопределенность - изменение законов, технологий, условий конкуренции приводят к необходимости к постоянной корректировки планов через систему обратной связи, которую обеспечивает контроль.

2. Предупреждение кризисных ситуаций - одно из главных назначений контроля - выявить проблемы и скорректировать деятельность организации до того, как эти проблемы перерастут в кризис

3.13.3 Результаты и выводы:

В ходе практической работы студент изучил основы безопасности, а именно средства и методы аутентификации в операционной системе.

3.14 Практическое занятие № 14 (2 часа).

Тема: «Аудит. Реализация политики аудита»

3.14.1 Задание для работы:

1. Возможности систем Windows.
2. Возможности систем UNIX

3.14.2 Краткое описание проводимого занятия:

2. Возможности систем Windows.

Практически повсеместно существуют проектные отделы, бухгалтерия, разработчики и другие категории сотрудников, совместно работающие над группами документов, хранящихся в общедоступной (Shared) папке на файловом сервере или на одной из рабочих станций. Может случиться так, что кто-то удалит важный документ или директорию из этой папки, в результате чего труд целого коллектива может быть потерян. В таком случае, перед системным администратором возникает несколько вопросов:

- Когда и во сколько произошла проблема?
- Из какой наиболее близкой к этому времени резервной копии следует восстановить данные?
- Это случилось непреднамеренно, или же кто-то действовал с умыслом?
- Может, имел место системный сбой, который может повториться ещё раз?

В Windows имеется система **Аудита,** позволяющая отслеживать и журналировать информацию о том, когда, кем и с помощью какой программы были удалены документы. По умолчанию, Аудит не задействован — слежение само по себе требует определённый процент мощности системы, а если записывать всё подряд, то нагрузка станет слишком большой. Тем более, далеко не все действия пользователей могут нас интересовать, поэтому политики Аудита позволяют включить отслеживание только тех событий, что для нас действительно важны.

Система Аудита встроена во все операционные системы **Microsoft Windows NT:** Windows XP/Vista/7, Windows Server 2000/2003/2008. К сожалению, в системах серии Windows Home аудит спрятан глубоко, и его настраивать слишком сложно.

Эта функция зачастую используется при обычной работе программ — например, исполненяя команду **Save (Сохранить),** программы пакета **MicrosoftOffice** сначала создают новый временный файл, сохраняют в него документ, после чего удаляют предыдущую версию файла. Аналогично, многие приложения баз данных при запуске сначала создают временный файл блокировок **(.lck),** затем удаляют его при выходе из программы.

Например, конфликтный сотрудник некоей компании при увольнении с места работы решил уничтожить все результаты своего труда, удалив файлы и папки, к которым он имел отношение. События такого рода хорошо заметны — они генерируют десятки, сотни записей в секунду в журнале безопасности. Конечно, восстановление документов из **Shadow Copies (Теневых Копий)** или ежесуточно автоматически создаваемого архива не составляет особого труда, но при этом я мог ответить на вопросы «Кто это сделал?» и «Когда это произошло?».

2. Возможности систем UNIX

Одним из инструментов, позволяющих повысить уровень безопасности в Linux, является подсистема аудита. С её помощью можно получить подробную информацию обо всех системных событиях.
Она не обеспечивает никакой дополнительной защиты, но предоставляет подробную информацию о нарушениях безопасности, на основании которой можно принять конкретные меры. Особенности работы с подсистемой аудита мы рассмотрим в этой статье.

Подсистема аудита: архитектура и принцип работы

Подсистема аудита была добавлена в ядро Linux начиная с версии 2.6. Она предназначена для отслеживания критичных с точки зрения безопасности системных событий.
В качестве примеров таких событий можно привести следующие (список далеко не полный):

- запуск и завершение работы системы;
- чтение, запись и изменение прав доступа к файлам;
- инициация сетевых соединений;
- попытки неудачной авторизации в системе;
- изменение сетевых настроек;
- изменение информации о пользователях и группах;
- запуск и остановка приложений;
- выполнение системных вызовов.

Ни одно из названных событий не может произойти без использования системных вызовов ядра. Чтобы их отслеживать, достаточно просто перехватывать соответствующие системные вызовы. Именно это и делает подсистема аудита:

Получив вызов от приложения в пространстве пользователя, подсистема аудита пропускает его через один из следующих фильтров: user, task или exit (более подробно о них речь пойдёт ниже). После этого вызов пропускается через фильтр exclude, который исходя из правил аудита передаёт его демону auditd для дальнейшей обработки.

Такая простая схема позволяет вполне эффективно отслеживать любой аспект работы ОС, а в случае компрометации системы выявлять подозрительные действия и определять их причину.

3.14.3 Результаты и выводы:

В ходе практической работы студент изучил основные принципы аудита, а также методы и способы аудита в операционных системах Windows и Unix.

3.15 Практическое занятие № 15-16 (4 часа).

Тема: «Модели разграничения доступа»

3.15.1 Задание для работы:

1. Нормативно-правовые документы аудита.

2. Причины проведения аудита.

3.15.2 Краткое описание проводимого занятия:

1.Нормативно-правовые документы аудита.

В соответствии с Федеральным законом "Об аудиторской деятельности" в 2015 году приняты нормативные правовые и иные акты, обеспечивающие правовые основы непосредственного применения международных стандартов аудита (МСА) в российской аудиторской практике. (Подробнее см. Постановление Правительства РФ от 11.06.2015 N 576, Приказ Минфина России от 05.08.2015 N 122н, Информационное сообщение Минфина России от 01.12.2015).

До 01.01.2017 года саморегулируемые организации аудиторов, сведения о которых внесены в государственный реестр саморегулируемых организаций аудиторов по состоянию на 02.12.2014 года обязаны выполнить требование к количеству членов саморегулируемой организации аудиторов. В случае, если по истечении указанного срока саморегулируемая организация аудиторов не представит в уполномоченный федеральный орган доказательство исполнения требования к количеству членов саморегулируемой организации аудиторов, сведения о некоммерческой организации исключаются уполномоченным федеральным органом из государственного реестра саморегулируемых организаций аудиторов. (Подробнее см. Федеральный закон от 01.12.2014 N 403-ФЗ).

Аудиторская деятельность осуществляется в соответствии с Федеральным законом от 30.12.2008 N 307-ФЗ "Об аудиторской деятельности" (далее - Закон N 307-ФЗ), другими федеральными законами и иными нормативными правовыми актами, которые регулируют отношения, возникающие при осуществлении аудиторской деятельности.

Согласно ч.9.1. ст. 23 Закон N 307-ФЗ до года, следующего за годом, в котором международные стандарты аудита признаны для применения на территории Российской Федерации, обязательными для аудиторских организаций, аудиторов, саморегулируемых организаций аудиторов и их работников являются федеральные правила (стандарты) аудиторской деятельности, утвержденные Правительством Российской Федерации, ифедеральные стандарты аудиторской деятельности, утвержденные уполномоченным федеральным органом.

3. Причины проведения аудита.

Обязательный аудит - это аудит, проведение которого обусловлено прямым указанием в Федеральном законе РФ и других федеральных законах.

Тот факт, что необходимость аудита в ряде случаев установлена актами законодательства, а не желанием руководителей экономических субъектов, имеет свои причины и определенные последствия как для аудиторов, проводящих аудит, обязательный для экономических субъектов, так и для этих экономических субъектов.

Причины необходимости проведения обязательного аудита:

1. Субъекты обязательного аудита, как правило, работают с денежными средствами физических и/или юридических лиц - это банки, страховые организации, негосударственные пенсионные фонды, открытые акционерные общества. Работники указанных организаций не всегда умеют квалифицированно читать бухгалтерскую отчетность, анализировать финансовые показатели, делать адекватные выводы. В случае

аудита таких экономических субъектов аудитор выступает посредником между проверяемым экономическим субъектом и заинтересованным в деятельности экономического субъекта, но не вполне квалифицированным пользователем бухгалтерской отчетности;

2. Устанавливая обязательность подтверждения отчетности предприятий, имеющих большой объем выручки от реализации, размеры имущества, государство таким образом организует контроль деятельности этих предприятий как крупных налогоплательщиков.

Обязательный аудит - это ежегодная обязательная аудиторская проверка ведения бухгалтерского учета и финансовой (бухгалтерской) отчетности организации или индивидуального предпринимателя.

В соответствии со ст.13 Федерального закона "О бухгалтерском учете" N 129-ФЗ от 21 ноября 1996 г. (в ред. Федерального закона от 23.07.98 N 123-ФЗ) бухгалтерская отчетность коммерческих организаций состоит из:

а) бухгалтерского баланса;

б) отчета о прибылях и убытках;

в) приложений к ним, предусмотренных нормативными актами;

г) аудиторского заключения, подтверждающего достоверность бухгалтерской отчетности организации, если она в соответствии с федеральными законами подлежит обязательному аудиту;

д) пояснительной записки.

Законом "Об аудиторской деятельности" (ст.7*)* определено осуществление обязательного аудита в следующих случаях:
1) организация имеет организационно-правовую форму открытого акционерного общества;

2) организация является кредитной организацией, страховой организацией или обществом взаимного страхования, товарной или фондовой биржей, инвестиционным фондом, государственным внебюджетным фондом, источником образования средств которого являются предусмотренные законодательством Российской Федерации обязательные исчисления, производимые физическими и юридическими лицами, фондом, источниками образования средств которого являются добровольные отчисления физических и юридических лиц;

3) объем выручки рублей (без учета НДС, акцизов и экспортных пошлин) организации или индивидуального предпринимателя от реализации продукции (выполнения работ, оказания услуг) за один год превышает в 500 тысяч раз установленный законодательством Российской Федерации минимальный размер оплаты труда (МРОТ принимается равным 100 рублям, строка 010 формы N 2) или сумма активов баланса (строка 300) превышает на конец отчетного года в 200 тысяч раз минимальный размер оплаты труда (МРОТ принимается равным 100 рублям);
4) организация является государственным унитарным предприятием, муниципальным унитарным предприятием, основанным на праве хозяйственного ведения, если финансовые показатели его деятельности соответствуют указанным выше настоящей

статьи. Для муниципальных унитарных предприятий законом субъекта Российской Федерации финансовые показатели могут быть понижены;

5) обязательный аудит в отношении этих организаций или индивидуальных предпринимателей предусмотрен федеральным законом.

3.15.3 Результаты и выводы:

В ходе практической работы студент изучил основные принципы аудита, а также знакомится с моделью разграничения доступа.

3.16 Практическое занятие № 17-18 (4 часа).

Тема: «Симметричное шифрование и формирование ключа на основе пароля»

3.16.1 Задание для работы:

1. Применение симметричного шифрования.
2. Основы дешифровки.

3.16.2 Краткое описание проводимого занятия:

1. Применение симметричного шифрования.

Симметричное шифрование предусматривает использование одного и того же ключа и для зашифрования, и для расшифрования. К симметричным алгоритмам применяются два основных требования: полная утрата всех статистических закономерностей в объекте шифрования и отсутствие линейности. Принято разделять симметричные системы на блочные и поточные. В блочных системах происходит разбиение исходных данных на блоки с последующим преобразованием с помощью ключа.

В поточных системах вырабатывается некая последовательность (выходная гамма), которая в последующем накладывается на само сообщение, и шифрование данных происходит потоком по мере генерирования гаммы. Схема связи с использованием симметричной криптосистемы представлена на рисунке.

Схема связи с использованием симметричной криптосистемы, где M - открытый текст, K - секретный ключ, передаваемый по закрытому каналу, En(M) - операция зашифрования, а Dk(M) - операция расшифрования

Обычно при симметричном шифровании используется сложная и многоступенчатая комбинация подстановок и перестановок исходных данных, причем ступеней (проходов) может быть множество, при этом каждой из них должен соответствовать «ключ прохода». Операция подстановки выполняет первое требование, предъявляемое к симметричному шифру, избавляясь от любых статистических данных путем перемешивания битов сообщения по определенному заданному закону. Перестановка необходима для выполнения второго требования – придания алгоритму нелинейности. Достигается это за счет замены определенной части сообщения заданного объема на стандартное значение путем обращения к исходному массиву.

Симметричные системы имеют как свои преимущества, так и недостатки перед асимметричными. К преимуществам симметричных шифров относят высокую скорость шифрования, меньшую необходимую длину ключа при аналогичной стойкости, большую изученность и простоту реализации. Недостатками симметричных алгоритмов считают в первую очередь сложность обмена ключами ввиду большой вероятности нарушения секретности ключа при обмене, который необходим, и сложность управления ключами в большой сети.

2. Основы дешифровки.

То есть, было необходимо разработать программу, которая позволит не просто хранить данные на сервере, но и предоставит возможность работы с ними через web-интерфейс и при этом обеспечит их бесполезность для злоумышленников в случае кражи, что достигается шифрованием/дешифрованием исключительно на стороне клиента.
Для типичного сценария использования возможна работа с тремя типами данных:

- обычный текст, вводимый в поля ввода формы и хранящийся на сервере в базе данных в зашифрованном виде
- файлы, которые хранятся на сервере в зашифрованном виде, и при необходимости пользователь может их скачать
- изображения, хранящиеся на сервере как зашифрованные файлы, но при необходимости они расшифровываются на стороне клиента и вставляются на web-страницу как обычные картинки.

Тот факт, что обработка данных должна производиться исключительно на стороне клиента, ограничивал выбор средств для реализации. На начальной стадии разработки была опробована связка «Java-апплет – Java-сервлет», но через какое-то время пришлось искать другой способ, потому что были трудности в отладке и передаче данных между апплетом и сервлетом.
Я остановился на использовании возможностей HTML5 и JavaScript-объекта «XmlHttpRequest Level 2» в частности, потому что они позволили с меньшими усилиями реализовать необходимый функционал.

Работа с текстом

Алгоритм шифрования:

- вносим текст в поле формы на web-странице
- шифруем текст с помощью функций Java Script
- отправляем зашифрованный текст на сервер, где сохраняем в базу данных.

Обратный процесс:

- получаем зашифрованные данные из базы данных с сервера
- дешифруем их с помощью функций Java Script
- выводим расшифрованный текст в нужное место на web-странице.

Работа с файлами

Процесс шифрования/дешифрования файлов происходит немного другим образом.
Алгоритм шифрования:

- выбираем файл с компьютера пользователя

- получаем содержимое файла в объект Java Script, используя XmlHttpRequest Level 2 и возможности HTML 5
- шифруем его с помощью функций Java Script
- отправляем зашифрованные данные на сервер, где сохраняем как файл.

Обратный процесс:

- получаем содержимое зашифрованного файла с сервера
- записываем его в объект Java Script, используя XmlHttpRequest Level 2 и возможности HTML 5
- дешифруем с помощью функций Java Script
- передаём расшифрованные данные в Java-апплет, чтобы дать пользователю возможность указать путь и имя для сохраняемого файла, т. к. на данный момент развития технологий в браузерах нельзя штатно вызывать диалог сохранения файла в произвольное место на компьютере пользователя, только в ограниченную «песочницу», что нам не подходит. Если по каким-либо причинам использование Java-апплета не подходит, эту часть можно заменить на Flash с аналогичным функционалом.

Работа с изображениями

Алгоритм шифрования:

- выбираем файл с изображением с компьютера пользователя
- записываем его содержимое в объект Java Script, используя XmlHttpRequest Level 2 и возможности HTML 5
- кодируем в формат Base64
- шифруем с помощью функций Java Script
- отправляем зашифрованные данные на сервер, где сохраняем в файл.

Обратный процесс:

- получаем содержимое зашифрованного изображения с сервера
- записываем его в объект Java Script, используя XmlHttpRequest Level 2 и возможности HTML 5
- дешифруем с помощью функций Java Script. На этом этапе получаем изображение, закодированное в формате Base64
- вставляем содержимое в тег на web-странице (браузеры по умолчанию поддерживают вставку изображений в формате Base64).

3.16.3 Результаты и выводы:

В ходе практической работы студент освоил симметричное шифрование. Также бы рассмотрен материал о формировании ключа на основе пароля.

3.17Практическое занятие № 19-22 (8 часов).

Тема: «Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС**»**

3. 17.1 Задание для работы:

1. Задачи и принципы сопровождения системного программного обеспечения.
2. Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС

3.17.2 Краткое описание проводимого занятия:

1. Задачи и принципы сопровождения системного программного обеспечения.

Организация эффективной и надежной защиты операционной системы невозможна с помощью одних только программно-аппаратных средств. Эти средства обязательно должны, дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже самая надежная программно-аппаратная защита оборачивается фикцией.

Основные административные меры защиты.

1. Постоянный контроль корректности функционирования операционной системы, особенно ее подсистемы защиты. Такой контроль наиболее удобно организовать, если операционная система поддерживает регистрацию событий (event logging). В этом случае операционная система автоматически регистрирует в специальном журнале (или нескольких журналах) наиболее важные события, произошедшие в процессе функционирования системы.
2. Организация и поддержание адекватной политики безопасности. Политика безопасности должна постоянно корректироваться, оперативно реагируя на изменения в конфигурации операционной системы, установку, удаление и изменение конфигурации прикладных программных продуктов и расширений операционной системы, попытки злоумышленников преодолеть защиту операционной системы и т.д.
3. Инструктирование пользователей операционной системы о необходимости соблюдения мер безопасности при работе с операционной системой и контроль за соблюдением этих мер.
4. Регулярное создание и обновление резервных копий программ и данных операционной системы.

Постоянный контроль изменений в конфигурационных данных и политике безопасности операционной системы.

Основные принципы администрирования ОС.

- Непрерывность;
- Комплексность;
- Актуальность;
- Адекватность;
- Непротиворечивость. (разграничение доступа, настроек процессов);
- Формальный подход. Применение методик (инструкций, положений, приказов, РД и прочих рекомендательных документов) и четких концептуальных принципов при постановке задач администрирования и их реализации;
- Подконтрольность.

Задачи и принципы управления безопасностью.

Отдельные средства ИБ не обеспечивают эффективного функционирования и требуют объединения в единую и централизованно управляемую и постоянно

действующую *систему информационной безопасности* Система ИБ обычно должна решать следующие задачи:

- ввод в систему списка имен пользователей и терминалов, допущенных к информации ИС;
- подготовку и ввод в систему, запись паролей пользователей на носители;
- ввод в систему назначенных полномочий пользователей и терминалов;
- раздачу пользователям носителей с паролями и значений паролей, запоминаемых и вводимых пользователями вручную с клавиатуры;
- сбор сигналов несовпадения паролей и нарушения полномочий пользователей;
- установление времени, места и причины НСД;
- анализ ситуации, принятие адекватных мер и восстановление нормального функционирования ИС
- контроль конфигурации системы;
- сбор сигналов вскрытия аппаратуры и контроль ввода (вывода) аппаратуры в (из) ремонт (а) и на (из) профилактику(и);
- контроль журнала регистрации доступа к информации ИС и периодический вызов справок из него;
- взаимодействие со службой функционального контроля ИС;
- контроль функционирования системы защиты;
- подготовку ключей, контроль и обеспечение функционирования средств шифрования информации;
- контроль стирания и уничтожения остатков секретной информации на машинных и бумажных носителях;
- регистрацию, учет и разграничение доступа к носителям информации и ПО;
- ведение статистики и прогнозирование НСД.

И удовлетворять следующим принципом:

- непрерывной. Это требование проистекает из того, что злоумышленники только и ищут возможность, как бы обойти защиту интересующей их информации;
- плановой. Планирование осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации);
- целенаправленной. Защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;
- конкретной. Защите подлежат конкретные данные, объективно подлежащие охране, утрата которых может причинить организации определенный ущерб;
- активной. Защищать информацию необходимо с достаточной степенью настойчивости;
- надежной. Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемым секретам, независимо от формы их представления, языка выражения и вида физического носителя, на котором они закреплены;
- универсальной. Считается, что в зависимости от вида канала утечки или способа несанкционированного доступа его необходимо перекрывать, где бы он ни проявился, разумными и достаточными средствами, независимо от характера, формы и вида информации;
- комплексной. Для защиты информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что защита — это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообусловливающих друг друга сторон, свойств, тенденц

2. Генерация, настройка, измерение производительности и модификация систем, управление безопасностью ОС

Безопасность – одна из наиболее актуальных проблем в области ИТ в настоящее время, ввиду сильной зависимости повседневной деятельности и бизнеса от компьютерных технологий и ввиду резко возрастающего числа сетевых атак (киберпреступности). Особенно важна безопасность для операционных систем и сетей как основных объектов атак. В лекции рассмотрены следующие вопросы:

- Проблема безопасности
- Аутентификация
- Программные угрозы (атаки)
- Системные угрозы (атаки)
- Защита систем
- Обнаружение взлома
- Криптография
- Безопасность в Windows NT / 2000 / XP / 2003 / Vista, в.NET
- Инициатива Trustworthy Computing Initiative корпорации Microsoft.

Проблема безопасности

Безопасность (security) – это защита от внешних атак. В настоящее время наблюдается значительный рост числа самых разнообразных атак хакеров, угрожающих целостности информации, работоспособности компьютерных систем и зависящих от них компаний, благосостоянию и личной безопасности людей. Для защиты от атак необходимы специальные меры безопасности, компьютерные технологии и инструменты.
В любой компьютерной системе должна быть реализована подсистема безопасности, которая должна проверять внешнее окружение системы и защищать ее от:

- Несанкционированного доступа
- Злонамеренной модификации или разрушения
- Случайного ввода неверной информации.

Практика показывает, что легче защитить от случайной, чем от злонамеренной порчи информации.

Аутентификация

Одной из наиболее широко используемых мер безопасности является аутентификация (authentication) – идентификация пользователейпри входе в систему. Такая идентификация пользователей наиболее часто реализуется через логины – зарегистрированные имена пользователей для входа в систему – и пароли – секретные кодовые слова, ассоциируемые с каждым логином.
Основной принцип использования паролей в том, что они должны сохраняться в секрете. Поэтому одна из традиционных целей атакующиххакеров состоит в том, чтобы любыми способами выведать у пользователя его логин и пароль. Для сохранения секретности паролей предпринимаются следующие меры.

- Частая смена паролей. Аналогичные меры применялись в армии во время войны. Большинство сайтов и других систем (например, сайт партнеров фирмы Microsoft) требуют от пользователей регулярной (например, не реже. чем раз в три месяца) смены паролей, иначе сайт блокируется для доступа. Подобные меры вполне оправданы.

- Использование "не угадываемых" паролей. Практически все системы требуют от пользователя при регистрации устанавливать пароли, не являющиеся легко угадываемыми: например, как правило, пароль должен содержать большие и маленькие буквы и цифры, специальные символы и иметь длину не менее 7-8 символов. Используются также автоматические генераторы не угадываемых паролей. Поэтому использование в качестве паролей легко угадываемых слов – например, имени любимой собаки или общеупотребительного понятия – не рекомендуется.
- Сохранение всех неверных попыток доступа. Во многих системах реализован системный журнал, в котором фиксируются все неверные попытки ввода логинов и паролей. Обычно дается фиксированное число таких попыток (например, три).

Пароли также могут быть закриптованы или разрешены для доступа лишь один раз, после чего от пользователя требуется смена пароля.

Программные угрозы (атаки)

Рассмотрим некоторые типичные виды угроз и атак, используемые хакерами.
Троянская программа (Trojan Horse) – атакующая программа, которая "подделывается" под некоторую полезную программу, но при своем запуске не по назначению (злонамеренно) использует свое окружение, например, получает и использует конфиденциальную информацию. Троянские программы используют системные механизмы для того, чтобы программы, написанные одними пользователями, могли исполняться другими пользователями.
Вход в ловушку (Trap Door) - использование логина или пароля, который позволяет избежать проверок, связанных с безопасностью.
Переполнение стека и буфера (Stack and Buffer Overflow) - использование ошибки в программе (переполнение стека или буферов в памяти) для обращения к памяти другого пользователя или процесса с целью нарушения ее целостности.

Системные угрозы (атаки)

Рассмотрим также некоторые типичные атаки, использующие уязвимости (vulnerabilities) в системных программах – ошибки и недочеты, дающие возможность организации атак.
Черви (Worms) – злонамеренные программы, использующие механизмы самовоспроизведения (размножения). Например, один из Интернет-червей использует сетевые возможности UNIX (удаленный доступ) и ошибки в программах finger и sendmail. Принцип его действия следующий: некоторая постоянно используемая в сети системная программа распространяет главную программу червя.
Вирусы – фрагменты кода, встраивающиеся в обычные программы с целью нарушения работоспособности этих программ и всей компьютерной системы. В основном вирусы действуют на микрокомпьютерные системы. Вирусы скачиваются с публично доступных сайтов или с дисков, содержащих "инфекцию". Для предотвращения заражения компьютерными вирусами необходимо соблюдать принципы безопасности при использовании компьютеров (safe computing) – использовать антивирусы, guards – программы, постоянно находящиеся в памяти и проверяющие на вирусы каждый открываемый файл - .exe, doc, и т.д.
Отказ в обслуживании (Denial of Service – DoS) – одна из распространенных разновидностей атак на сервер, заключающаяся в создании искусственной перегрузки сервера с целью препятствовать его нормальной работе. Например, для Web-сервера такая атака может заключаться в том, чтобы искусственно сгенерировать миллион

запросов "GET". Если сервер реализован не вполне надежно, подобная атакачаще всего приводит к переполнению памяти на сервере и необходимости его перезапуска.

Типы сетевых атак

Рассмотрим некоторые типы современных сетевых атак, которых необходимо постоянно остерегаться пользователям.
Phishing – попытка украсть конфиденциальную информацию пользователя путем ее обманного получения от самого пользователя. Даже само слово phishing – искаженное слово fishing (рыбная ловля), т.е. хакер с помощью этого приема как бы пытается поймать чересчур наивного пользователя "на удочку". Например, напугав в своем сообщении пользователя, что его логин и пароль, кредитная карта или банковский счет под угрозой, хакер пытается добиться от пользователя в ответ ввода и отправки некоторой конфиденциальной информации. Обычно phishing-сообщение по электронной почте приходит как бы от имени банка и подделывается под цвета, логотипы и т.д., используемые на сайте банка. Однако для его разоблачения обычно достаточно подвести курсор мыши (не кликая ее) к приведенной web-ссылке или email-адресу (при этом она высвечивается) и убедиться в том, что адрес указывает отнюдь не на банк, а на совершенно посторонний сайт или email. Поэтому пользователям не следует быть слишком наивными. Другая действенная мера, если phishingпроисходит регулярно с одних и тех же email-адресов, - включить эти адреса в черный список на email-сервере. Тогда подобные сообщения вообще не будут доходить до входного почтового ящика пользователя.
Pharming – перенаправление пользователя на злонамеренный Web-сайт (обычно с целью phishing). Меры предотвращения со стороны пользователя мы уже рассмотрели. В современные web-браузеры встроены программы антифишингового контроля, которые запускаются автоматически при обращении к сайту. Хотя это отнимает у пользователя некоторое время, подобные меры помогают предотвратить многие атаки.
Tampering with data – злонамеренное искажение или порча данных. Действенной мерой по борьбе с подобными атаками являетсякриптование информации.
Spoofing – " подделка" под определенного пользователя (злонамеренное применение его логина, пароля и полномочий). Логин и парольпри этом либо получены от пользователя обманным путем (например, в результате phishing), либо извлечены из "взломанного" хакерской программой системного файла.
Elevation of privilege – попытка расширить полномочия (например, до полномочий системного администратора) с целью злонамеренных действий. Поэтому наиболее секретная информация в любой компьютерной системе – пароль системного администратора, который необходимо защищать особенно тщательно.

3.17.3 результаты и выводы:

В ходе практической работы студент изучил основы генерации, настройки, измерения производительности и модификации систем, управление безопасностью ОС. Также был более глубоко усвоен лекционный материал.

3.18 Практическое занятие № 23-26 (8 часов).

Тема: «Цифровая подпись. Процедура оформления подписи и проверка»

3.18.1 Задание для работы:

1. Основы формирования цифровой подписи.
2. Методы передачи цифровой подписи.
3. Средства расшифровки цифровой подписи.

3.18.2 Краткое описание проводимого занятия:

1. Основы формирования цифровой подписи.

- Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;
-
- [Электронная] цифровая подпись (digital signature): Строка бит, полученная в результате процесса формирования подписи. Данная строка имеет внутреннюю структуру, зависящую от конкретного механизма формирования подписи.
-
- Общая суть электронной подписи заключается в следующем. С помощью криптографической хэш-функции на основании документа вычисляется относительно короткая строка символов фиксированной длины (хэш). Затем этот хэш шифруется закрытым ключом владельца — результатом является подпись документа. Подпись прикладывается к документу, таким образом получается подписанный документ. Лицо, желающее установить подлинность документа, расшифровывает подпись открытым ключом владельца, а также вычисляет хэш документа. Документ считается подлинным, если вычисленный по документу хэш совпадает с расшифрованным из подписи, в противном случае документ является подделанным.
- Принципы использования электронной подписи:
- Принципами использования электронной подписи являются:
- ● право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;
- ● возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования Федерального закона №63 «Об электронной подписи» применительно к использованию конкретных видов электронных подписей;
- ● недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.
- Виды электронных подписей:
- Видами электронных подписей, отношения в области использования которых регулируются Федеральным законом №63 «Об электронной подписи», являются простая электронная подпись и усиленная электронная подпись. Различаются

усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

- 1. Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.
- 2. Неквалифицированной электронной подписью является электронная подпись, которая:
- ● получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- ● позволяет определить лицо, подписавшее электронный документ;
- ● позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- ● создается с использованием средств электронной подписи.
- 3. Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:
- ● ключ проверки электронной подписи указан в квалифицированном сертификате;
- ● для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом №63 «Об электронной подписи».
- При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.
-
- Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью:
- 1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.
- 2. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью,

равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны соответствовать требованиям статьи 9 настоящего Федерального закона.

- 3. Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.
- 4. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

2.Методы передачи цифровой подписи.

Шифрование передаваемых через Интернет данных позволяет защитить их от посторонних лиц. Однако для полной безопасности должна быть уверенность в том, что второй участник транзакции является тем лицом, за которое он себя выдает. В бизнесе наиболее важным идентификатором личности заказчика является его подпись. В электронной коммерции применяется электронный эквивалент традиционной подписи — цифровая подпись . С ее помощью можно доказать не только то, что транзакция была инициирована определенным источником, но и то, что информация не была испорчена во время передачи.

Как и в шифровании, технология электронной подписи использует либо секретный ключ (в этом случае оба участника сделки применяют один и тот же ключ), либо открытый ключ (при этом требуется пара ключей — открытый и личный). И в данном случае более просты в использовании и более популярны методы с открытым ключом (такие, как RSA)

Хэш-функции являются одним из важных элементов криптосистем на основе ключей и используются для обнаружения факта модификации сообщения, то есть для электронной подписи. Их относительно легко вычислить, но почти невозможно расшифровать. Хэш-функция имеет исходные данные переменной длины и возвращает строку (иногда называемую дайджестом сообщения — MD) фиксированного размера, обычно 128 бит.

Существует несколько защищенных хэш-функций: Message Digest 5 (MD-5), Secure Hash Algorithm (SHA) и др. Они гарантируют, что разные документы будут иметь разные электронные подписи, и что даже самые незначительные изменения документа вызовут изменение его дайджеста.

Рассмотрим, как работает технология цифровой подписи, использующая алгоритм RSA. Предположим, вы хотите послать сообщение. В этом случае порядок работы следующий:
1. При помощи хеш-функции вы получаете дайджест — уникальным образом сжатый

вариант исходного текста.
2. Получив дайджест сообщения, вы шифруете его с помощью личного ключа RSA, и дайджест превращается в цифровую подпись.
3. Вы посылаете вместе с самим сообщением цифровую подпись.
4. Получив послание, получатель расшифровывает цифровую подпись с помощью вашего открытого ключа и извлекает дайджест сообщения.
5. Получатель, применяя для сообщения ту же хэш-функцию, что и вы, получает свой сжатый вариант текста и сравнивает его с дайджестом, восстановленным из подписи. Если они совпадают, то это значит, что подпись правильная и сообщение действительно поступило от вас. В противном случае сообщение либо отправлено из другого источника, либо было изменено после создания подписи.

При аутентификации личности отправителя открытый и личный ключи играют роли, противоположные тем, что они выполняли при шифровании. Так, в технологии шифрования открытый ключ используется для зашифровки, а личный — для расшифровки. При аутентификации с помощью подписи все наоборот. Кроме того, подпись гарантирует только целостность и подлинность сообщения, но не его защиту от посторонних глаз. Для этого предназначены алгоритмы шифрования. Например, стандартная технология проверки подлинности электронных документов DSS (Digital Signature Standard) применяется в США компаниями, работающими с государственными учреждениями. Однако у технологии RSA более широкие возможности в силу того, что она служит как для генерации подписи, так и для шифрования самого сообщения. Цифровая подпись позволяет проверить подлинность личности отправителя: она основана на использовании личного ключа автора сообщения и обеспечивает самый высокий уровень сохранности информации.

3.18.3 Результаты и выводы:

В ходе практической работы студент изучил понятия цифровой подписи, а также процедуру оформления подписи и проверки. Также был более глубоко усвоен лекционный материал.