Содержание

Введение

Основной целью являлось: закрепление в производственных условиях теоретических знаний и дисциплин, а также приобретение практических навыков в области защиты персональных данных, обеспечения информационной безопасности в автоматизированных системах и получение практических знаний.

Основными задачами за прохождение производственной практики были:

- Закрепление теоретических знаний, полученных в техникуме;
- Изучение технологии и организации деятельности предприятия;
- Ознакомление с организацией обеспечения информационной безопасности при помощи инженерно-технических средств другим организациям;
- Приобретение практических знаний и умений по основным направлениям деятельности предприятия;

В изучение также входило:

- ознакомление с общей организацией информационной безопасности предприятия;
- изучение применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами в организации;
- Ознакомление с техническими задачами, возникающими при аттестации объектов, помещений, программ.

1. Изучение требования безопасности на рабочем месте. Прохождение инструктажа.

Охрана труда и техника безопасности на предприятии – это комплекс мер, необходимых, чтобы обезопасить трудящихся во время выполнения ими порученных работодателем задач. По направлениям работы они подразделяются на:

• обеспечение безопасности электрооборудования, кабельных линий, ЛЭП, молниезащиту;

• защиту от пожаров, возгораний и задымления;

• безопасную организацию всех категорий работ;

• поддержание исправности оборудования (поверка, ремонт, своевременная замена);

• содержание в надлежащем состоянии зданий различного назначения, сооружений, построек, а также территории;

• нейтрализацию влияния на работников шума, запыленности, вибрации и других вредных факторов;

• защиту людей, которые трудятся в опасных условиях: на высоте, под землей, в условиях повышенных или пониженных температур, различных излучений, контактируют с горячими или движущимися предметами и их частями и т.д.;

• обучение работников, учащихся, управленческого персонала (инструктажи по охране труда и технике безопасности, специальные курсы, плакаты, схемы, рисунки и др.);

• мониторинг показателей здоровья работников (предварительные, пред сменные, ежегодные, внеочередные медосмотры и освидетельствования), организация санаторного лечения, выдачи лечебно-профилактическое питания, молока;

• общественный мониторинг организации охраны труда и техники безопасности на предприятии: работа уполномоченных по ОТ, профсоюзов, других общественных объединений.

ГОСТ 12.0.004-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Организация обучения безопасности труда. Общие положения (вместе с Программами обучения безопасности труда) (введен в действие Приказом Росстандарта от 09.06.2016 N 600-ст)> ГОСТ 12.0.004-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Организация обучения безопасности труда. Общие положения.

Обучение безопасности труда в форме проведения инструктажа.

Проведение инструктажей (инструктирование) заключается в изложении (выдаче) в устной или письменной форме инструктирующим лицом (инструктором) инструктируемому лицу конкретных руководящих и обязательных для исполнения требований (указаний) по условиям, порядку и последовательности безопасного совершения тех или иных конкретных действий (трудовых функций, производственных операций и т.п.) во время исполнения инструктируемым лицом порученных ему трудовых и (или) поведенческих функций.

Проведение инструктажей по безопасности труда включает в себя: ознакомление инструктируемого лица с имеющимися на его рабочем месте (местах) условиями труда (опасными и/или вредными производственными факторами производственной среды и факторами трудового процесса), с требованиями безопасности и охраны труда, содержащимися в локальных нормативных актах организатора обучения, инструкциях по охране труда на рабочем месте и по безопасному выполнению работ, в другой необходимой при выполнении трудовой функции инструктируемым лицом технической и эксплуатационной документации, а также с безопасными методами и приемами выполнения работ и оказания первой помощи пострадавшему.

Инструктаж по охране труда проводится в утвержденном руководителем организатора обучения порядке, разработанном с учетом характера производственной деятельности, условий труда на рабочем месте и трудовой функции инструктируемого лица, а также вида инструктажа.

Для проведения инструктажа по охране труда могут быть использованы специальная программа проведения инструктажа, разработанная и утвержденная на предприятии, иные методы и средства обучения, в том числе инструкции по охране труда, по безопасности выполнения видов работ, нормативные документы, учебные пособия, наглядные пособия, тренажеры, компьютеры, видео инструктажи и т.п.

Проведение инструктажа по безопасности и (или) охране труда завершается устной проверкой инструктирующим лицом степени усвоения содержания инструктажа инструктируемым лицом. При необходимости рекомендуется использовать те или иные системы тестов. Результаты тестирования оформляются в письменной (компьютерной) форме и хранятся до проведения очередного инструктажа и тестирования.

2. Определение статуса, структуры и системы управления функциональных подразделений и служб предприятия.

Функциональная структура – это система, которая должна быть сформирована с учетом видов деятельности организации. Под функциями рассматриваются основные направления. На основании этого формируют структурные подразделения:

- производственные;
- управленческие;
- социальные и т.д.

Функциональная организационная структура управления позволяет возложить на каждый руководящий орган выполнение определенные функции на конкретном уровне управления. Это особенно важно для производственных подразделений, которые должны выполнять указания функционального органа с учетом его компетенции. Такая система управления повышает эффективность работы, все решения по общим вопросам управляющий аппарат принимает коллегиально. Вместо менеджеров с универсальной специализацией создают штат специалистов с высоким уровнем квалификации. Организационная функциональная структура управления особенно эффективна при выполнении рутинных задач, которые постоянно повторяются, что не требует принятия оперативных решений.

Такую систему управления используют в крупносерийном или массовом производстве. Область применения:

- одно продуктовые компании;
- компании, которые реализуют длительные и сложные инновационные проекты;
- крупные организации специализированного назначения;
- предприятия с узкой спецификацией.

Сущность функциональной структуры управления предприятием основана на необходимости возложить на менеджмент специфические задачи, они заключаются в:

- тщательном подборе руководителей в функциональные структурные подразделения;
- разделении и выравнивании загрузки подразделений; координировании действий руководителей;
- разработке механизмов мотивации;
- предотвращении сепаратистского развития;
- создании приоритета специалистов над линейным руководством.

Суть функциональной структуры управления заключается в объединении специалистов одного профиля в отдельные специализированные структурные подразделения. Например, специалисты по финансам работают в финансовом подразделении, по маркетингу – в маркетинговом, по планированию – в плановом и т.д. Начиная со среднего звена, управление строят с учетом функционального признака. Рассмотрим на примере. Маркетинговый отдел подчиняется руководителю структурного подразделения. Он в свою очередь обязан выполнять распоряжения генерального директора, который является единым руководителем всей компании. Сотрудники отдела относятся к исполнителям. Они обязаны выполнять распоряжения своего непосредственного руководителя и подчиняться требованиям, которые выдвигает генеральный директор. Это и есть функциональная структура управления.

3. Изучение положения о деятельности выбранного предприятия и его правовой статус.

Субъект административного права - лицо «общество с ограниченной ответственностью "Фирма"», которое в соответствии с действующим законодательством является участником управления отношений, регулируемых нормами административного права, и наделенное определенными правами и обязанностями в сфере государственного управления. Организация, создающая материальные и духовные ценности, как участник административно-правовых отношений различают по своему правовому положению.

Главным направлением организационной структуры является установление четких взаимосвязей между отдельными подразделениями организации, распределения между ними ответственности и прав. В ней осуществляются разного рода требования к совершенствованию систем управления, которые выражаются в определенных принципах.

Организационная структура компании «Фирма» является простейшая линейно-функциональной. Особенностью такого рода структуры управления является то, что управляющие воздействия на объект могут быть переданы лишь одним доминантным

лицом – руководителем, официально получающим данные лишь от лиц, напрямую подчиненных ему, принимает решения по всем вопросам, которые относятся к руководимой им части объекта, и отвечает за его работу перед начальством.

Главной составляющей технического обеспечения ИС компании является комплекс технических средств (КТС) – совокупность взаимосвязанных единым управлением и (или) автономных технических средств сбора, передачи, накопления, регистрации, обработки, вывода и представления данных, а также средств оргтехники.

Входящие в комплекс технические средства должны быть совместимы и адаптированы к условиям функционирования службы управления персоналом. Также должна быть предусмотрена возможность расширения с целью подключения новых устройств.

4. Ознакомление с перечнем и конфигурацией средств вычислительной техники, архитектурой сети, программными средствами, установленными на предприятии.

Выбирая оборудование, необходимо учитывать состав и назначение комплектов оборудования, и его главные характеристики: производительность при осуществлении технологических операций, надежность работы, совместимость работы разного рода оборудования, включая персональные компьютеры, стоимость оборудования, состав и количество обслуживающего персонала, площадь, необходимая для размещения оборудования.

Важнейшей задачей выбора технических средств является определение затрат на их покупку и эффективность будущего функционирования службы управления персоналом.

В состав АПП должны входить:

- персональный компьютер типа Intel Celeron G1820 с тактовой частотой от 2.8 ГГц и выше, Pentium G и выше;
- клавиатура;
- мышь;
- монитор любой модели;
- принтер любой модели и типа;
- внешний блок коммутации
- специализированное программное обеспечение на диске.

Структура технического обеспечения представлена ниже, она является условной и классифицирует техническое обеспечение лишь по назначению.

1) Базовое техническое обеспечение.

- микропроцессор;
- постоянная память;
- оперативная память;
- регистровая память;
- видеопамять;
- блок питания.

2) Периферийное ТО.

- устройства ввода;
- устройства вывода;
- устройства (накопители) внешней памяти.

Техническое обеспечение магазина «Фирма» представлено в таблице 1.

Программное обеспечение предприятия содержит общесистемные, специальные программные продукты и техническую документацию.

К общесистемному программному обеспечению принято относить комплексы программ, которые предназначены для решения типовых задач обработки данных. С их помощью расширяют функциональных возможности компьютеров, выполняется контроль и управление процессом обработки информации.

Таблица 1 - Техническое обеспечение магазина «Фирма»

№	Наименование технической единицы	Характеристики
Базовое техническое обеспечение		
2	Микропроцессор	Intel® Core TM i7 4510U, Intel® Core TM i5 4210U, Intel core i7 2.40 GHz
3	Постоянная память – ПЗУ.	1TB HDD
4	Оперативная память – ОЗУ.	DDR3 4096 Мб
5	Материнская плата	MB LGA-775S GIGABYTE GA-EP45-DS3L (IP45+SB+2xGLAN), ATX 1600Mhz, 4xDDRII, PCI-Ex16, 3xPCI, 1IDE, 4SATA, BOX
6	Видеокарта	GeFoce 920M 2 Гб
Периферийное техническое обеспечение		
7	Монитор	19" SAMSUNG SM943NW 0.285mm, (1280x1024@75), 1.5ms, 300 cd/m2, 1000:1.5 , VGA, D-Sub, DVI, TCO99 Silver
8	Клавиатура	Keyboard USB CHD KB-4322-01-U, MM+Int keys, Eng/Rus/Kaz, Silver/Black
9	Мышь	Mouse Wireless USB Hama M3050, 8 buttons, Laser (800, 1600dpi), 2AAA, black/silver (52470)
10	Принтер	HP LaserJet Pro MFP M225dn (A4/1200dpi/26стр.м/макс размер скан 216x297мм/USB/256Mb, 600МГц, лоток 260листов, LAN10/100)

Специальное ПО является комплексом программ, которые разработаны при создании определенной ИС. В состав программного обеспечения входят пакеты прикладных программ, которые реализуют разработанные модели разной степени адекватности и отражают функционирование реального объекта. Операционная система

является основой программного обеспечения ЭВМ. Операционная система является совокупностью служебных и системных программных средств, обеспечивающей взаимодействие пользователя с ЭВМ и реализацию всех остальных программ.

5. Изучение должностных инструкций инженерно-технических работников среднего звена в соответствии с подразделением предприятия.

В однозадачных системах применяются средства управления файлами, периферийными устройствами и средства общения с пользователями. Многозадачные операционные системы применяют все эти средства и управляют разделением совместно применяемых ресурсов.

Каждый пользователь многопользовательских операционных систем настраивает интерфейс для себя. Помимо этого, имеются средства защиты данных каждого пользователя от несанкционированного доступа остальных пользователей.

На ЭВМ, являющихся рабочими местами пользователей, используется операционная система Windows 10.

Данная операционная система является современной многозадачной многопользовательской ОС с графическим интерфейсом пользователя. Операционная система Microsoft Windows 10, созданная как персональная высококлассная ОС, имеет более совершенные функциональные возможности и высокие системные требования по сравнению с ее конкурентами.

Для работы с данной ОС требуется как минимум 12-Мбайт ОЗУ, а для инсталляции может потребоваться до 75 Мбайт свободного места на жестком диске. Данная многозадачная ОС также имеет важные средства обеспечения безопасности, надежную новую файловую систему с регистрационным журналом.

Наряду с введенными новшествами и усовершенствованиями, самым главным достоинством ОС Windows 10 является совместимость с ПК с довольно простыми техническими характеристиками: подойдет даже процессор всего на 1 ГГц, оперативная память объемом в 1 Гб и обычная видеокарта с поддержкой DirectX. Также стоит отметить, что в состав дистрибутива ОС содержит комплекс драйверов, подходящий практически для любой материнской платы, аудио карты и видеоадаптера.

Компания «Фирма» использует Microsoft Windows 10 PRO, Microsoft Office 2013, в качестве архиватора пользуются WINRAR v5.20 (64 bit), для обеспечения безопасности ESET Endpoint Antivirus для Microsoft Windows. Для оформления актов и набора текстовых документов используют Microsoft Word 2013 и Microsoft Excel 2013. Для записи CD и DVD дисков используют UltraISO v.9.6.5.

Локальная вычислительная сеть построена по технологии коммутации независимых сегментов Ethernet с применением множественного доступа с контролем несущей и обнаружением коллизий (метод CSMA/CD).

Локальная сеть построена по топологии «звезда».

Топология «звезда» является самой распространенной топологией сети. Она имеет явно выделенный центр, к которому подключаются все остальные абоненты.

В сети с данной топологией рабочие станции напрямую подключены к концентратору. Данный важный элемент сети может быть как активным,

восстанавливающим сигнал, так и пассивным, просто обеспечивающим физическое соединение кабеля. Как и остальные компьютеры, сервер тоже подключён к концентратору, что делает связь между ними предельно простой.

Как правило, размер сети, имеющей топологию «звезда», ограничен лишь количеством портов на хабе, однако чисто теоретически их не может быть более 1024, но трудно представить концентратор, имеющий такое количество портов. Поскольку через хаб проходит весь трафик в сети такого типа, от данного устройства полностью зависит работоспособность и надёжность системы.

Вся локальная вычислительная сеть разбита на две подсети: первого и второго этажей здания. Каждая из подсетей содержит коммутационное оборудование (switch), которое осуществляет ее высокую производительность и надежную коммутацию. В качестве среды передачи данных используется кабель UTP категории 5. Длина кабельного сегмента колеблется от 5 до 25 метров (что не превышает максимально допустимые 100 метров). Рабочие станции сети подключаются к портам коммутаторов, которые обеспечивают скорость передачи данных в пределах коллизионного сегмента – 10/100 Mb/c для каждого порта.

Остальные порты коммутаторов находятся в резерве для того, чтобы в случае, если понадобится расширить ЛВС, можно было подключить дополнительный коммутатор в стек. Сеть разработана на базе стандарта IEEE 802.3 (Fast Ethernet или 100BASE-TX) для медного кабеля (витая пара).

В состав ЛВС предприятия входят:

- сервер сети;
- коммутационное оборудование (switch);
- пассивное оборудование (коммутационные шкафы, короба, розетки);
- рабочие станции (персональные компьютеры);
- рабочая среда (кабель).

Комплектация сервера и рабочих станций представлена в таблице 2.

Таблица 2 - Комплектация сервера и рабочих станций

Номер	Наименование	Количество
1	CPU Intel Xeon CPU E5-2620 v3 2.4 GHz.	2
2	DIMM 8 Gb DDR4.	8
3	HDD – 2TB SAS.	4
4	Mb Intel Server Board.	1
5	Корпус FUDJITSU PRIMERGY TX2560 M1	1
6	Ноутбук Asus X555L	4
7	Монитор 20” HP W2072a	4
8	Кабель UTP 5 категории	610 м.
9	Коммутатор	2
10	Розетки питания	12
11	Сетевые розетки	12

6. Настройка компонентов подсистем защиты информации операционных систем.

Обязанности инженерно-технических работников среднего звена

Инженерно-технические работники среднего звена должны обеспечивать:

Выполнение плановых заданий, ритмичный выпуск продукции высокого качества, эффективное использование основных фондов и оборотных средств участка, соблюдение правильного соотношения между ростом производительности труда и средней заработной платой. Проводит работу по совершенствованию организации производства, механизации и автоматизации производственных процессов, предупреждению брака и повышению качества выпускаемой продукции, экономии всех видов ресурсов, аттестации и рационализации рабочих мест, использованию резервов повышения производительности труда, а также по повышению рентабельности производства, снижению трудоемкости и себестоимости продукции;

Максимальное использование производственных мощностей, полную загрузку и правильную эксплуатацию оборудования, производительную работу участка на протяжении всей смены;

Своевременную подготовку производства материалами, полуфабрикатами, инструментом, приспособлениями, технической документацией и др. для ритмичной работы участка;

Пересмотр в установленном порядке устаревших норм выработки, а также норм на работы, по которым осуществлены организационно-технические мероприятия, обеспечивающие снижение трудовых затрат.

Строжайшее соблюдение работниками участка трудовой и производственной дисциплины, чистоты и порядка на рабочих местах. Осуществляет контроль за своевременным вывозом отходов и готовой продукции без загромождения проходов и проездов и захламления рабочих мест;

Высокое качество выпускаемой продукции, производит проверку в процессе изготовления деталей, сборки узлов и изделий, их качества, а также изучает причины брака и дефектов, разрабатывает и осуществляет мероприятия по их устранению;

Технически правильную эксплуатацию оборудования и других основных средств и выполнение графиков их ремонта, безопасные и здоровые условия труда, а также своевременное представление работающим льгот по условиям труда;

Программно-аппаратные средства защиты ОС обязательно должны дополняться административными мерами защиты. Без постоянной квалифицированной поддержки со стороны администратора даже надежная программно-аппаратная защита может давать сбои. Перечислим основные административные меры защиты.

1. Постоянный контроль корректности функционирования ОС, особенно ее подсистемы защиты. Такой контроль удобно организовать, если ОС поддерживает автоматическую регистрацию наиболее важных событий в специальном журнале.

2. Организация и поддержание адекватной политики безопасности. Политика безопасности ОС должна постоянно корректироваться, оперативно реагируя на попытки злоумышленников преодолеть защиту ОС, а также на изменения в конфигурации ОС, установку и удаление прикладных программ.

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

4. Регулярное создание и обновление резервных копий программ и данных ОС.

5. Постоянный контроль изменений в конфигурационных данных и политике безопасности ОС. Информацию об этих изменениях целесообразно хранить на неэлектронных носителях информации, для того чтобы злоумышленнику, преодолевшему защиту ОС, было труднее замаскировать свои несанкционированные действия.

7. Работа в операционных системах с соблюдением действующих требований по защите информации.

В конкретных ОС могут потребоваться и другие административные меры защиты информации.

Подсистема защиты ОС выполняет следующие основные функции.

1. Идентификация и аутентификация. Ни один пользователь не может начать работу с ОС, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.

2. Разграничение доступа. Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.

3. Аудит. ОС регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

4. Управление политикой безопасности. Политика безопасности должна постоянно поддерживаться в адекватном состоянии, т. е. должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в ОС.

5. Криптографические функции. Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.

6. Сетевые функции. Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе и задач, имеющих прямое отношение к защите информации.

В защищенной ОС любой пользователь, перед тем как начать работу с системой, должен пройти идентификацию, аутентификацию и авторизацию. Субъектом доступа называют любую сущность, способную инициировать выполнение операций над элементами ОС. В частности, пользователи являются субъектами доступа. Авторизация субъекта доступа происходит после успешной идентификации и аутентификации. При авторизации субъекта ОС выполняет действия, необходимые для того, чтобы субъект мог начать работу в системе.

8. Контроль целостности подсистем защиты информации операционных систем.

Рабочее место пользователя Системы использует СКЗИ для обеспечения целостности, конфиденциальности и подтверждения авторства информации, передаваемой в рамках Системы. Порядок обеспечения информационной безопасности при работе в Системе определяется руководителем организации, подключающейся к Системе, на основе рекомендаций по организационно-техническим мерам защиты, изложенным в данном разделе, эксплуатационной документации на СКЗИ, а также действующего российского законодательства в области защиты информации.

Персонал должен быть определен и утвержден список лиц, имеющих доступ к ключевой информации. К работе на АРМ (Автоматизированное рабочее место) с установленным СКЗИ допускаются только определенные для эксплуатации лица, прошедшие соответствующую подготовку и ознакомленные с пользовательской документацией на СКЗИ, а также другими нормативными документами по использованию электронной подписи. К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются доверенные лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

Рекомендуется назначение в организации, эксплуатирующей СКЗИ, администратора безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности.

Должностные инструкции пользователей АРМ и администратора безопасности должны учитывать требования настоящих Правил. В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям (ЭП и шифрования), должна быть проведена смена ключей, к которым он имел доступ.

На технических средствах АРМ с установленным СКЗИ необходимо использовать только лицензионное программное обеспечение фирм-изготовителей, полученное из доверенных источников.

На АРМ должна быть установлена только одна операционная система. При этом не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

Не допускается установка на АРМ средств разработки и отладки программного обеспечения. Если средства отладки приложений необходимы для технологических потребностей пользователя, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ. Необходимо исключить попадание в систему средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратор.

Рекомендуется ограничить возможности пользователя запуском только тех приложений, которые разрешены администратором безопасности.

Рекомендуется установить и использовать на АРМ антивирусное программное обеспечение. Необходимо регулярно отслеживать и устанавливать обновления безопасности для программного обеспечения АРМ (Service Packs, Hot fix и т п.), обновлять антивирусные базы.

9. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных.

Целостности данных - при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Методы контроля целостности данных:

- Полная копия данных
- Контрольная сумма
- Хеш
- Имитовставка
- ЭЦП

Полная копия данных.

Создаются полные копии данных и потом сверяются.

- Преимущества:
- простота реализации
- полный контроль данных (до бита)

Недостатки:

- большой объем
- копии можно подменить
- копиями можно воспользоваться (например: если данные - пароль)

Контрольная сумма - значение, рассчитанное по входным данным с помощью определённого алгоритма.

Преимущества:

- высокая скорость вычисления
- малый размер
- стандартный размер

Недостатки:

- можно подменить
- для одного значения существует множество исходных данных
- можно подобрать исходные данные к значению за приемлемое время (например: получить пароль)

Хеш (хэш, криптографический хеш) - значение, рассчитанное по входным данным с помощью криптографического алгоритма.

Преимущества:

- малый размер
- стандартный размер
- нельзя подобрать исходные данные к значению за приемлемое время (например: получить пароль)

Недостатки:

- низкая скорость вычисления (сопоставима с шифрованием)
- можно подменить
- для одного значения существует множество исходных данных

Имитовставка - значение, рассчитанное по входным данным с помощью криптографического алгоритма с использованием секретного элемента (ключа), известного только отправителю и получателю.

Преимущества:

малый размер

- стандартный размер
- нельзя подобрать исходные данные к значению за приемлемое время (например: получить пароль)
- нельзя подменить без секретного элемента (ключа)

Недостатки:

- низкая скорость вычисления (сопоставима с шифрованием)
- для одного значения существует множество исходных данных
- секретный ключ известен как минимум двоим

Электронная цифровая подпись - зашифрованное значение вычисленного хеша по входным данным.

Преимущества:

- малый размер
- стандартный размер
- нельзя подобрать исходные данные к значению за приемлемое время (например: получить пароль)
- нельзя подменить без секретного элемента (ключа)
- секретный ключ известен одному

Недостатки:

- низкая скорость вычисления (сопоставима с шифрованием)
- для одного значения существует множество исходных данных

Чтобы выполнять резервное копирование, прежде всего, нужно иметь подходящую программу. Эта программа должна не только уметь делать простые копии данных на резервные носители, но и хорошо подходить для сотрудников вашей организации и требований бизнеса. Оценивая программы для резервного копирования, следует обратить внимание на:

Возможности выполнения резервного копирования по расписанию. Управление размещением, циклами копий и использованием носителей. Взаимодействие с операторами (и/или автоматическими устройствами смены носителей), когда требуется определённый носитель. Возможности, облегчающие поиск носителя с определённой копией заданного файла. Как вы могли заметить, настоящее решение для резервного копирования должно не только сбрасывать биты и байты на резервный носитель. Придя к этому, многие системные администраторы рассматривают одно из двух решений:

- Приобретение коммерческого решения
- Разработка своими силами системы резервного копирования с нуля (возможно, с применением одной или нескольких технологий с открытым кодом)

Некоторые центры данных делают резервные копии на диски, а после завершения копирования эти копии записывают на ленту с целью архивации. Это позволяет максимально быстро завершить копирование в отведённом для него окне. Запись резервных копий на ленту может выполняться позже, в любое другое время дня, главное, чтобы запись на ленту закончилась к моменту, когда будет готова следующая копия. Все типы копий следует периодически проверять, чтобы убедиться в том, что эти копии можно прочитать. Действительно, иногда копии, по той или иной причине, могут не читаться. Но самое печальное в этом то, что чаще всего это обнаруживается только при потере данных, когда требуется резервная копия.

10. Использование программных средств для архивирования информации.

Архив - файл, содержащий в себе информацию из одного или нескольких, иногда сжатых (без потерь), других файлов. Является результатом работы программы-архиватора. Сжатие данных (англ. data compression) - алгоритмическое преобразование данных, производимое с целью уменьшения их объёма. Применяется для более рационального использования устройств хранения и передачи данных. Сжатие данных делится на два вида: без потерь и с потерями. Архивация — это сжатие данных без потерь.

Методы сжатия с потерей информации обычно обеспечивают гораздо более высокую степень сжатия, чем обратимые методы, но их нельзя применять к текстовым документам, базам данных и, тем более, к программному коду. Характерными форматами сжатия с потерей информации являются:

- .JPG для графических данных;
- .MPG для видеоданных;
- .MP3 для звуковых данных.

Если при сжатии данных происходит только изменение их структуры, то метод сжатия обратим. Из результирующего кода можно восстановить исходный массив путем применения обратного метода. Обратимые методы применяют для сжатия любых типов данных. Характерными форматами сжатия без потери информации являются:

- .GIF, .TIF, .PCX и многие другие для графических данных;
- .AVI для видеоданных;
- .ZIP, .ARJ, .RAR, .LZH, .LH, .CAB и многие другие для любых типов данных.

На предприятие «Фирма» используется программа для архивирования «WinRAR», данная программа обладает рядом преимуществ:

- Поддержка файлов размером до 16 эксабайт (1018-1 байт).
- Размер скользящего словаря от 1 МБ до 1 ГБ (в 32-разрядной версии для Windows до 256 МБ). Размер по умолчанию — 32 МБ.
- Вместо применяемых по умолчанию 32-разрядных контрольных сумм CRC32 можно использовать значительно более надёжное 256-разрядное хеширование BLAKE2sp.
- Возможность шифрования архивов с использованием алгоритма AES в режиме CBC с длиной ключа 256 бит (в версии 4 — 128 бит).

- Добавление в архивы дополнительных, основанных на кодах Рида — Соломона, данных для восстановления архива в случае его повреждения, а также создание специальных томов для восстановления, позволяющих восстановить многотомный архив при повреждении или даже полном отсутствии его отдельных томов.
- Добавление в архивы особой дополнительной информации для ускорения их открытия.
- Создание многотомных (состоящих из нескольких частей) архивов указанного или автоматически выбираемого размера.
- Создание непрерывных (solid) архивов, позволяющих достигать значительно более высокой степени сжатия при упаковке нескольких файлов, особенно однотипных.
- Поддержка расширенных возможностей NTFS, например жёстких и символических ссылок.

11. Разработка концепции защиты автоматизированной (информационной) системы.

Информационная безопасность предприятия – это защищенность информации, которой располагает предприятие (производит, передает или получает) от несанкционированного доступа, разрушения, модификации, раскрытия и задержек при поступлении. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Компьютеризация, развитие телекоммуникаций предоставляют сегодня широкие возможности для автоматизированного доступа к различным конфиденциальным, персональным и другим важным, критическим данным в обществе (его граждан, организаций и т.д.).

Перед началом осуществления плана по защите данных в АС следует выделить информационные ресурсы, нуждающиеся в защите и оценить важность защищаемой информации. Чтобы определить информацию, подлежащую защите при администрировании государственного сайта, необходимо обратиться к следующим нормативным документам:

- ФЗ № 149 от 27.07.2006 «Об информации, информационных технологиях и защите информации»;
- ФЗ № 98 от 29.07.2004 «О коммерческой тайне»;
- ФЗ № 152 от 27.07.2006 «О персональных данных»;
- Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями на 23 сентября 2005 г.).

Данные нормативные документы позволяют выделить следующие виды информации организации, подлежащей защите:

- Общедоступная информация - открытая информация об организационно-штатной структуре, распорядительные документы.
- Персональные данные - данные пользователей сайта, клиентов, данные о сотрудниках и руководителе гос. аппарата
- Коммерческая тайна — это сведения о компании, которые связаны с производственными процессами, управлением, технологиями, финансами и прочей

деятельностью организации, разглашение которых может привести к ущербу для интересов руководства предприятия.

В настоящее время наиболее критичными данными, с точки зрения защиты информации, являются персональные данные. Критичность выделенных данных обусловлена тем, что их разглашение может привести к значительным негативным последствиям для субъектов персональных данных, а также влечет за собой наложение больших штрафов на организацию, методы административного, а иногда и уголовного воздействия.

Необходимо обеспечивать комплексную защиту всех информационных служб и коммуникационных каналов между ними. Чтобы определить необходимые механизмы безопасности, нужно разработать программно-аппаратную реализацию всех серверов, рабочих мест, каналов связи информационной системы, а также других коммуникационных систем, особенно связанных с элементами информационной системы.

Для того чтобы сформировать набор требований по безопасности, которым должна отвечать АС, был определен ее класс защищенности. Класс защищенности согласно руководящему документу Гостехкомиссии «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации» определялся на основании:

- перечня защищаемых ресурсов АС и их уровней конфиденциальности;
- перечня лиц, имеющих доступ к штатным средствам, АС, с указанием их уровня полномочий;
- матрицы доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режимов обработки данных в АС.

Определение класса защищенности АС позволяет сформировать набор требований по безопасности, которые предъявляются к этому классу систем. Эти требования изложены в РД ФСТЭК «Средства вычислительной техники. Защита от НСД. Показатели защищенности от несанкционированного доступа к информации». Кроме того, на основе класса защищаемой АС выбираются средства вычислительной техники (СВТ), которые должны иметь соответствующий класс защищенности СВТ. Также необходимо обратить внимание на то, что в АС обрабатываются персональные данные, следовательно, необходимо определить и класс ИСПД.

Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

- внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

- внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Предотвращение сбоев в системе: наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка источников бесперебойного питания.

Организация надежной и эффективной системы архивации данных:

ПО для автоматической архивации информации с серверов и рабочих станций в указанное администратором локальной вычислительной сети время, выдавая отчет о проведенном резервном копировании.

Защита от компьютерных вирусов: Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Защита от несанкционированного доступа: ПО для дополнительной аутентификации пользователя и шифрования критической информации. Смарт-карты управления доступом позволяют реализовать, в частности, такие функции, как контроль входа, доступ к устройствам персонального компьютера, доступ к программам, файлам и командам. Кроме того, возможно также осуществление контрольных функций, в частности, регистрация попыток нарушения доступа к ресурсам, использования запрещенных утилит, программ, команд DOS.

Защита информации при удаленном доступе: Маршрутизатор удаленного доступа. В мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов - их разделение и передача параллельно по двум линиям, - что делает невозможным "перехват" данных при незаконном подключении "хакера" к одной из линий. К тому же используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможность расшифровки "перехваченных" данных.

Механизмы обеспечения безопасности: Криптография. Для обеспечения секретности применяется шифрование, или криптография, позволяющая трансформировать данные в зашифрованную форму, из которой извлечь исходную информацию можно только при наличии ключа.

Защита сетей: Брандмауэр. Система или комбинация систем, позволяющие разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Брандмауэр пропускает через себя весь трафик и для каждого проходящего пакета принимает решение - пропускать его или отбросить.

12. Анализ журнала аудита ОС на рабочем месте.

Анализ форматов и структур представления данных о событиях безопасности, принятых в существующих системах аудита, позволяет определить и выделить основные

поля данных, характеризующие события безопасности, и разработать универсальный формат для внутреннего представления событий безопасности в системе.

В ОС семейства Linux каждая строка текстового файла журнала аудита является отдельной записью о событии. Значения отдельных полей разделяются пробелом. Каждая строка – запись о событии обычно содержит следующую информацию:

- дату и время регистрации события;
- символьный идентификатор модуля, зарегистрировавшего событие;
- подробное описание события.

События могут регистрироваться различными модулями. Например, идентификатор модуля «$AUDIT» обозначает, что событие зарегистрировано основным модулем аудита. Для записей о событиях, генерируемых этим модулем характерна, структура подробного описания события, состоящая из следующих полей:

- идентификатор типа события;
- идентификатор пользователя (UID), в сеансе которого произошло событие;
- идентификатор группы пользователя (GID), в сеансе которого произошло событие;
- информация об операции (функции) и ее параметрах.

В ОС семейства Microsoft Windows NT для доступа к данным аудита необходимо использовать специальные функции, которые обеспечивают считывание данных аудита в буферы в оперативной памяти, формат которых хорошо документирован. Запись о событии аудита в ОС семейства

Microsoft Windows NT содержит следующую информацию:

- порядковый номер события;
- время регистрации и время записи события (включая дату);
- идентификаторы типа события;
- категория аудита, к которой относится событие;
- идентификатор безопасности субъекта, в сеансе которого произошло событие;
- дополнительные параметры события, зависящие от типа события.

Данные хранятся и представляются в двоичном виде. С учетом рассмотренных структур данных, описывающих события безопасности в существующих распространенных системах аудита, можно разработать некоторый универсальный формат для представления событий аудита в системе, который бы способствовал ускорению обработки данных событий. При этом новый формат должен полно описывать событие. Структура нашего представления событий безопасности в системе должна содержать следующие поля данных:

- N – порядковый номер события. Тип значения – целое число.
- RegistrationTime – время регистрации события. Тип значения – дата.
- StartTime – время начала обработки. Тип значения – дата.
- EventID – идентификатор разновидности события. Тип значения – целое число.
- EventType – идентификатор типа события. Тип значения – целое число.

- EventCategory – идентификатор категории (группы разновидностей событий), к которой относится событие. Тип значения – целое число.
- EventClasss – класс события – промежуточный результат обработки события в системе, класс события определяется системой на основе анализа данной структуры, описывающей событие. Тип значения - целое число.
- SourceName – имя источника события
- или модуля, зарегистрировавшего событие. Тип значения – строка символов.
- UserName – имя пользователя в сеансе которого зарегистрировано событие. Тип значения – строка символов.
- Domain – имя домена пользователя. Тип значения – строка символов.
- Host – идентификатор (имя или сетевой адрес) компьютера, на котором зарегистрировано событие. Тип значения – строка символов.
- EventParameters – дополнительные параметры события, зависящие от разновидности события. Тип значения - строка символов.

Рисунок 1 - Алгоритм преобразования данных в новый вид

Такая структура (Рисунок 1) позволяет осуществить представление данных распространенных систем аудита в формализованном виде, удобном для дальнейшей обработки и автоматического анализа.

Проанализируем данные, которые мы извлекли из журнала аудита. Разделим все события на классы в зависимости от важности. То есть на основании полей записи будем относить события к какому-нибудь классу.

Каждое событие должно подвергнуться проверке на соответствие множествам правил, задающих классы событий. После проверки (при реализации – некоторая функция) поле EventClass получит значение, которое будет показывать принадлежность

события к некоторому классу. Причем возможен случай, когда событие принадлежит сразу к нескольким классам.

Выделим следующие классы:

1. Архивные – это все события безопасности, регистрируемые на компьютерах сети.

2. Отказы – это события, связанные с отказами в предоставлении доступа, а также со сбоями в работе средств обеспечения безопасности.

3. Информативные – это события, которые целесообразно отфильтровывать от всех архивных событий, поскольку они содержат важную информацию о важных происшествиях. Наличие этого класса объясняется тем, что обычно журналы аудита содержат большое количество малоинформативных событий, присутствие которых затрудняет дальнейший анализ, поэтому целесообразно отделять информативные события и, возможно, хранить их отдельно от архивных.

4. Предостережения – это класс важных событий, сигнализирующих о возникновении опасных ситуаций. Администраторы безопасности обязательно должны быть проинформированы о событиях этого класса, однако эти события не требуют немедленного оповещения.

5. Тревоги – это класс особо важных событий, сигнализирующих о возникновении особо опасных ситуаций, в случае обнаружения которых необходимо немедленно оповестить администратора безопасности.

13. Установка и настройка средств защиты информации в информационной системе должна проводиться в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации.

Средства защиты информации, устанавливаемые в информационной системе, функционирующей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, должны быть совместимы между собой, а также со средствами защиты информации, установленными в информационно-телекоммуникационной инфраструктуре центра обработки данных.

Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

управления (администрирования) системой защиты информации информационной системы;

- выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;
- управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы;
- контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе

- защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

При внедрении организационных мер защиты информации осуществляются:

- реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;
- проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации;
- отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.

Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

При анализе уязвимостей информационной системы проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.

В случае выявления уязвимостей информационной системы, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей.

По результатам анализа уязвимостей должно быть подтверждено, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

Требования к реализации ОЦЛ.1: В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать:

- контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по

контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы;

- контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;
- контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы;
- тестирование с периодичностью, установленной оператором, функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с АНЗ.1 и АНЗ.2(ФСТЭК).

14. Обслуживание средств защиты информации прикладного и системного программного обеспечения.

В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

Правила и процедуры контроля целостности программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОЦЛ.1:

1) в информационной системе контроль целостности средств защиты информации должен осуществляться по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

2) в информационной системе должен обеспечиваться контроль целостности средств защиты информации с использованием криптографических методов в соответствии с законодательством Российской Федерации, всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы;

3) оператором исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды;

4) оператором обеспечивается выделение рабочих мест с установленными средствами разработки и отладки программ в отдельный сегмент (тестовую среду);

5) в информационной системе должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной

системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности.

15. Настройка программного обеспечения с соблюдением требований по защите информации.

Требования к реализации ОПС.3: Оператором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке ("белый список"), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных оператором к установке ("черный список").

Указанные перечни программного обеспечения и (или) его компонентов разрабатываются оператором для информационной системы в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации оператора по защите информации (документируются).

Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5.

Требования к реализации АВЗ.1: Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);
- установку, конфигурирование и управление средствами антивирусной защиты;
- предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;
- проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);

- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов;
- оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации.

16. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам.

Требования к усилению АВЗ.1:

1) в информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности;

2) в информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах);

3) оператором должен обеспечиваться запрет использования съемных машинных носителей информации, которые могут являться источниками вредоносных компьютерных программ (вирусов);

4) в информационной системе должно обеспечиваться использование на разных уровнях информационной системы средств антивирусной защиты разных производителей;

5) в информационной системе должны обеспечиваться проверка работоспособности, актуальность базы данных признаков компьютерных вирусов и версии программного обеспечения средств антивирусной защиты;

6) в информационной системе должна обеспечиваться проверка объектов файловой системы средством антивирусной защиты до загрузки операционной системы;

7) в информационной системе должна обеспечиваться регистрация событий о неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

8) оператором должна обеспечиваться антивирусная защита на этапе инициализации микропрограммного обеспечения средства вычислительной техники.

При приеме на работу новые сотрудники проходят вводный инструктаж, получая общее представление о:

- режиме работы компании;
- правилах безопасности;
- порядке оповещения руководства о чрезвычайных ситуациях, угрозе ущерба.

С учетом специфики деятельности, доступа к информационным ресурсам для предотвращения возможных инцидентов перед допуском к самостоятельному выполнению трудовых обязанностей на рабочем месте сотрудников знакомят с инструкциями, устанавливающими их права и обязанности. При этом обращают внимание на нюансы, возможные риски, учитывая должность работника.

Требования к сотрудникам с доступом к конфиденциальным данным.

Сотрудники, имеющие доступ к сведениям, представляющим коммерческую, государственную, иную тайну, должны соблюдать правила информационной безопасности.

Помимо общих положений, их внимание акцентируют:

- на основных обязанностях по соблюдению правил, исключающих утечку сведений при работе с секретными данными;
- на принимаемых мерах защиты автоматизированных рабочих мест от несанкционированного доступа посторонних;
- на установлении пароля для доступа к данным на персональном компьютере, электронных носителях;
- на необходимых мерах защиты от вредоносных программ;
- на алгоритме действий при возникновении внештатных ситуаций.
- Требования к администратору, отвечающему за защиту локальной вычислительной сети

17. Проведение инструктажа пользователей о соблюдении требований по защите информации при работе с программным обеспечением.

Должностные лица, ответственные за проведение работ по технической защите информации локальных сетевых ресурсов, в процессе эксплуатации и модернизации, руководствуются:

- положениями федеральных законов;
- нормативными актами Российской Федерации;
- распорядительными документами Гостехкомиссии России (ФСТЭК), ФАПСИ (ФСО, ФСБ), Госстандарта России;
- локальными правовыми актами внутреннего пользования.

Администратора под роспись знакомят с установленными правами и обязанностями. Например, он может отключать от доступа к сети пользователей, нарушающих требования по безопасности информации, запрещать установку нештатного программного обеспечения.

Основные обязанности администратора фиксируют документально. Они включают:

- участие в испытаниях и контроле уровня защищенности локальной сети;
- анализ данных, вносимых в журнал учета работы ЛВС для своевременного выявления нарушений требований защиты и оценки возможных последствий;

- обеспечение доступа к информационной системе пользователям при наличии разрешения;
- блокировку попыток внесения изменений в программно-аппаратное обеспечение без согласования;
- немедленное оповещение службы безопасности о попытках несанкционированного доступа, нарушениях защиты.

В инструкции обращают внимание на строгий запрет передавать третьим лицам учетные данные пользователей, пароли, идентификаторы, ключи на твердых носителях.

Требования к реализации АНЗ.3: Оператором должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

- контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;
- контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;
- восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

18. Настройка встроенных средств защиты информации программного обеспечения.

Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

Требования к усилению АНЗ.3:

1) в информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации;

2) оператором в случае обнаружения нарушений работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации должен обеспечиваться перевод информационной системы, сегмента или компонента информационной системы в режим ограничения обработки

информации и (или) запрет обработки информации в информационной системе, сегменте или компоненте информационной системы до устранения нарушений;

3) оператором должны использоваться автоматизированные средства, обеспечивающие инвентаризацию параметров настройки программного обеспечения и средств защиты информации и восстановление параметров настройки программного обеспечения и средств защиты информации;

4) в информационной системе должно использоваться программное обеспечение, прошедшее контроль отсутствия не декларированных возможностей и отсутствия влияния на корректность работы средств защиты информации.

Требования к реализации АН3.4: Оператором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

- контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;
- контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

19. Проверка функционирования встроенных средств защиты информации программного обеспечения.

Требования к усилению АН3.4:

1) в информационной системе должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации;

2) оператором должны использоваться автоматизированные средства, обеспечивающие инвентаризацию технических средств, программного обеспечения и средств защиты информации.

В общем случае за обнаружение присутствия вирусов на компьютере должны отвечать антивирусы - специальные программы, способные быстро и эффективно не только обнаруживать, но и обезвреживать вредоносные программы. Однако известно, и тому есть объективные причины, что ни один антивирус не обеспечивает полную защиту от всех вредоносных программ. Следовательно, хоть и маловероятно, но возможно заражение компьютера, даже если на нем установлен антивирус. При отсутствии антивируса, вероятность проникновения на компьютер вредоносных программ многократно возрастает.

Не все вредоносные программы стремятся скрыть свое присутствие на компьютере. Некоторые ведут себя весьма активно: выводят на экран сообщения, открывают страницы веб-сайтов и т. п. Такие проявления логично назвать явными.

Многие вредоносные программы пытаются отключить или полностью удалить антивирус, другие блокируют доступ к веб-серверам антивирусных компаний, чтобы сделать невозможным обновление антивирусных баз. Соответственно, если антивирус вдруг ни с того, ни с сего перестал запускаться, либо перестали открываться сайты антивирусных компаний при том, что в целом доступ в Интернет работает нормально, это могут быть проявления вирусов. Такого рода проявления будут называться косвенными.

Таким образом проявления вредоносных программ можно условно разбить на три группы по тому, насколько легко их обнаружить:

- Явные - вредоносная программа самостоятельно проявляет заметную активность;
- Косвенные - другие программы начинают выводить сообщения об ошибках или вести себя нестандартно из-за присутствия на компьютере вируса;
- Скрытые - ни явных, ни косвенных проявлений вредоносная программа не имеет.

20. Обслуживание систем защиты информации в компьютерных системах и сетях.

Меры защиты информации реализуются в информационной системе в рамках ее системы защиты информации в зависимости от класса защищенности информационной системы, угроз безопасности информации, структурно-функциональных характеристик информационной системы, применяемых информационных технологий и особенностей функционирования информационной системы.

В информационной системе подлежат реализации следующие меры защиты информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;

- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств и систем связи и передачи данных.

Меры защиты информации, выбираемые для реализации в информационной системе, должны обеспечивать блокирование одной или нескольких угроз безопасности информации, включенных в модель угроз безопасности информации.

Содержание мер защиты информации для их реализации в информационных системах приведено в приложении N 2 к настоящему методическому документу. Описание представленных в приложении N 2 мер защиты информации приведено в разделе 3 настоящего методического документа.

Выбор мер защиты информации для их реализации в информационной системе включает (Рисунок 2):

- определение базового набора мер защиты информации для установленного класса защищенности информационной системы;
- адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы;
- уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации для блокирования (нейтрализации) всех угроз безопасности информации, включенных в модель угроз безопасности информации;
- дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

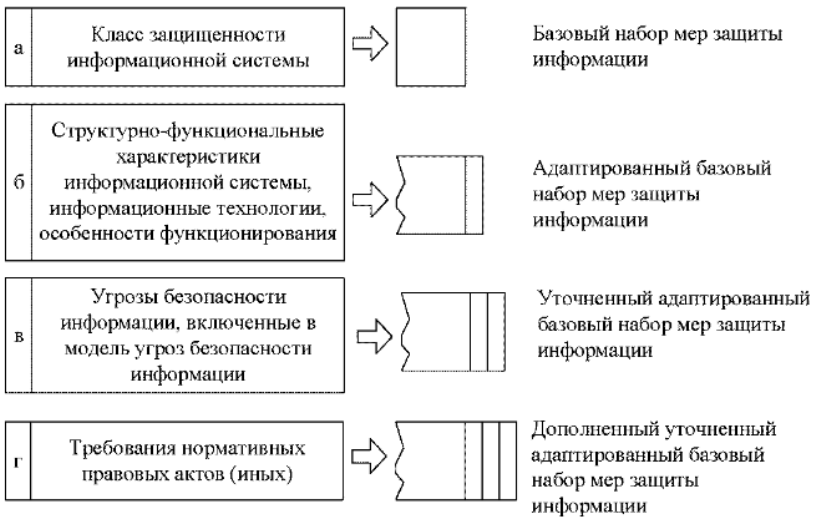

Рисунок 2 - Общий порядок действий по выбору мер защиты

- планирование мероприятий по обеспечению защиты информации в автоматизированной системе управления;
- обеспечение действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации автоматизированной системы управления;
- информирование и обучение персонала автоматизированной системы управления;
- периодический анализ угроз безопасности информации в автоматизированной системе управления и рисков от их реализации;
- управление (администрирование) системой защиты автоматизированной системы управления;
- выявление инцидентов в ходе эксплуатации автоматизированной системы управления и реагирование на них;
- управление конфигурацией автоматизированной системы управления и ее системы защиты;
- контроль (мониторинг) за обеспечением уровня защищенности автоматизированной системы управления.

В ходе управления (администрирования) системой защиты автоматизированной системы управления осуществляются:

- определение лиц, ответственных за управление (администрирование) системой защиты автоматизированной системы управления;
- управление учетными записями пользователей и поддержание правил разграничения доступа в автоматизированной системе управления в актуальном состоянии;
- управление средствами защиты информации в автоматизированной системе управления, в том числе параметрами настройки программного обеспечения, включая восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

- управление обновлениями программного обеспечения, включая программное обеспечение средств защиты информации, с учетом особенностей функционирования автоматизированной системы управления;
- централизованное управление системой защиты автоматизированной системы управления (при необходимости);
- анализ зарегистрированных событий в автоматизированной системе управления, связанных с безопасностью информации (далее - события безопасности);
- сопровождение функционирования системы защиты автоматизированной системы управления в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

Для выявления инцидентов и реагирования на них осуществляются:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в автоматизированной системе управления персоналом;
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению автоматизированной системы управления в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

В ходе управления конфигурацией автоматизированной системы управления и ее системы защиты осуществляются:

- поддержание конфигурации автоматизированной системы управления и ее системы защиты (структуры системы защиты автоматизированной системы управления, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты (поддержание базовой конфигурации автоматизированной системы управления и ее системы защиты);
- определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;
- регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления;

- управление изменениями базовой конфигурации автоматизированной системы управления и ее системы защиты, в том числе определение типов возможных изменений базовой конфигурации автоматизированной системы управления и ее системы защиты, санкционирование внесения изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты, документирование действий по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты, сохранение данных об изменениях базовой конфигурации автоматизированной системы управления и ее системы защиты, контроль действий по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;
- анализ потенциального воздействия планируемых изменений в базовой конфигурации автоматизированной системы управления и ее системы защиты на обеспечение ее безопасности, возникновение дополнительных угроз безопасности информации и работоспособность автоматизированной системы управления;
- определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты
- внесение информации (данных) об изменениях в базовой конфигурации автоматизированной системы управления и ее системы защиты в эксплуатационную документацию на систему защиты информации автоматизированной системы управления.

21. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации.

Основная задача контроля – предупреждение нарушений установленных требований и правил в области защиты информации и выработка рекомендаций по совершенствованию объектовой системы защиты информации.

Контроль состояния защиты информации складывается из контроля организации защиты информации и контроля эффективности защиты информации.

Согласно ГОСТ Р50922-96 «Защита информации. Термины и определения»:

Контроль состояния защиты информации – проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

Контроль организации защиты информации – проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

Контроль эффективности защиты информации – проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Его можно разделить на организационный контроль эффективности защиты информации - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации; технический контроль

эффективности защиты информации - контроль эффективности защиты информации, проводимой с использованием технических средств контроля.

22. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем.

Осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты автоматизированной системы управления и организационно-распорядительными документами по защите информации и в том числе включает:

- архивирование информации, содержащейся в автоматизированной системе управления;
- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.
- Архивирование информации, содержащейся в автоматизированной системе управления, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора.
- Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю автоматизированной системы управления или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе автоматизированной системы управления из эксплуатации производится уничтожение машинных носителей информации, содержащих энергонезависимую память.

На стадиях опытной и рабочей эксплуатации ЛВС основным методом оценки их качества следует считать экспериментальное исследование. Оно позволяет собрать статистическую информацию о действительном ходе вычислительного, процесса, использовании оборудования, степени удовлетворения требований пользователей системы и т.п. и затем по результатам ее обработки сделать заключение о качестве проектных решений, заложенных при создании системы, а также принять решение по модернизации системы (устранению "узких" мест) . Однако не исключено и использование методов моделирования, с помощью которых можно оценить эффект от модернизации ЛВС, не изменяя рабочей конфигурации и организации работы системы.

Моделирование - один из наиболее распространенных методов исследования. Модель ЛВС — это такое ее представление, которое состоит из определенного количества организованной информации о ней и построено с целью ее изучения. Другими словами, модель физическая или абстрактная система, представляющая объект исследования.

Использование аналитических методов связано с необходимостью построения математических моделей ЛВС в строгих математических терминах. Аналитические модели ВС носят обычно вероятностный характер и строятся на основе понятий аппарата теорий массового обслуживания, вероятностей и марковских процессов, а также методов диффузной аппроксимации. Могут также применяться дифференциальные и алгебраические уравнения.

При использовании этого математического аппарата часто удается быстро получить аналитические модели для решения достаточно широкого круга задач исследования ЛВС. В то же время аналитические модели имеют ряд существенных недостатков, к числу которых следует отнести: - значительные упрощения, свойственные большинству аналитических моделей. Подобные упрощения, а зачастую искусственное приспособление аналитических моделей с целью использования хорошо разработанного математического аппарата для исследования реальных ЛВС ставят иногда под сомнение результаты аналитического моделирования:

- громоздкость вычислений для сложных моделей, например, использование для представления в модели процесса функционирования современной ЛВС по методу дифференциальных уравнений Колмогорова требует (для установившегося режима) решения сложной системы алгебраических уравнений;
- сложность аналитического описания вычислительных процессов ЛВС. Большинство известных аналитических моделей можно рассматривать лишь как попытку подхода к описанию процессов функционирования ЛВС;
- недостаточная развитость аналитического аппарата в ряде случаев не позволяет в аналитических моделях выбирать для исследования наиболее важные характеристики (показатели эффективности) ЛВС.

Указанные особенности позволяют заключить, что аналитические методы имеют самостоятельное значение лишь при исследовании процессов функционирования ЛВС в первом приближении и в частных, достаточно специфичных задачах.

Практическое использование моделей ЛВС во многих случаях предполагает наличие информации о реальных характеристиках вычислительного процесса. Такая информация может быть получена эмпирическими методами, на основе которых в настоящее время создаются средства для исследования аппаратно-программных компонентов ЛВС.

23. Работа в существующей на предприятии локальной сети.

Экспериментальные методы позволяют создать основу количественной оценки эффективности ВС для достижения следующих практических целей: анализа имеющихся ЛВС, выбора наилучшей и синтеза новой ЛВС. Оценка характеристик аппаратно-программных средств связана с проведением экспериментов и измерений, которые с практической точки зрения могут рассматриваться как процесс получения полезной информации.

Информация в локальных сетях, как правило, передается отдельными порциями, кусками, называемыми пакетами. Причем предельная длина этих пакетов строго ограничена (обычно величиной в несколько килобайт). Ограничена длина пакета и снизу (как правило, несколькими десятками байт). Выбор пакетной передачи связан с несколькими важными соображениями.

Локальная сеть, как уже отмечалось, должна обеспечивать качественную, связь всем абонентам сети. Важнейшим параметром является так называемое время доступа к сети (access time), которое определяется как временной интервал между моментом готовности абонента к передаче (когда ему есть, что передавать) и моментом начала этой

передачи. Это время ожидания абонентом начала своей передачи. Естественно, оно не должно быть слишком большим, иначе величина реальной, интегральной скорости передачи информации между приложениями сильно уменьшится даже при высокоскоростной связи.

Ожидание начала передачи связано с тем, что в сети не может происходить несколько передач одновременно (во всяком случае, при топологиях шина и кольцо). Всегда есть только один передатчик и один приемник (реже – несколько приемников). В противном случае информация от разных передатчиков смешивается и искажается. В связи с этим абоненты передают свою информацию по очереди. И каждому абоненту, прежде чем начать передачу, надо дождаться своей очереди. Вот это время ожидания своей очереди и есть время доступа.

Если бы вся требуемая информация передавалась каким-то абонентом сразу, непрерывно, без разделения на пакеты, то это привело бы к монопольному захвату сети этим абонентом на довольно продолжительное время. Все остальные абоненты вынуждены были бы ждать окончания передачи всей информации, что в ряде случаев могло бы потребовать десятков секунд и даже минут (например, при копировании содержимого целого жесткого диска). С тем чтобы уравнять в правах всех абонентов, а также сделать примерно одинаковыми для всех них величину времени доступа к сети и интегральную скорость передачи информации, как раз и применяются пакеты ограниченной длины.

Каждый пакет помимо собственно данных, которые требуется передать, должен содержать некоторое количество служебной информации. Прежде всего, это адресная информация, которая определяет, от кого и кому передается данный пакет.

Таким образом, процесс информационного обмена в сети представляет собой чередование пакетов, каждый из которых содержит информацию, передаваемую от абонента к абоненту.

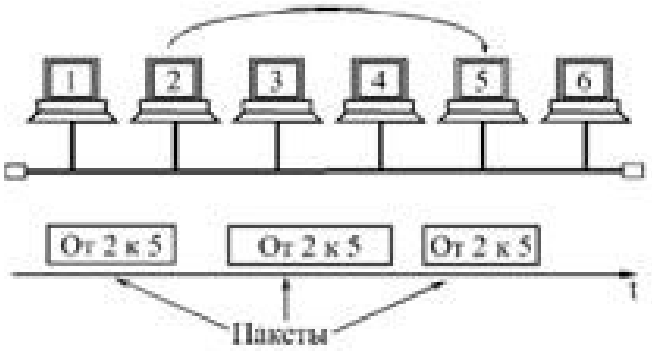

Рисунок 3 - Передача пакетов в сети между двумя абонентами

В частном случае (Рисунок 3) все эти пакеты могут передаваться одним абонентом (когда другие абоненты не хотят передавать). Но обычно в сети чередуются пакеты, посланные разными абонентами (Рисунок 4).

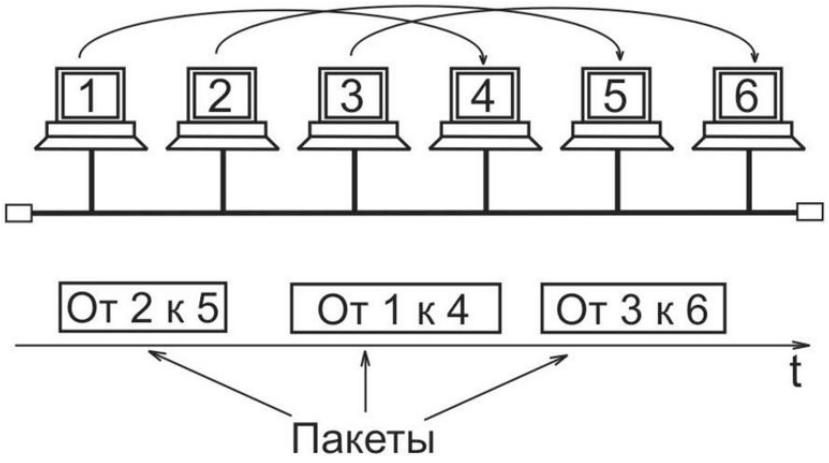

Рисунок 4 - Передача пакетов в сети между несколькими абонентами.

24. Создание технического задания проекта новой локальной сети.

Структура и размеры пакета в каждой сети жестко определены стандартом на данную сеть и связаны, прежде всего, с аппаратными особенностями данной сети, выбранной топологией и типом среды передачи информации. Кроме того, эти параметры зависят от используемого протокола (порядка обмена информацией).

Но существуют некоторые общие принципы формирования структуры пакета, которые учитывают характерные особенности обмена информацией по любым локальным сетям.

Чаще всего пакет содержит в себе следующие основные поля или части (Рисунок 5).

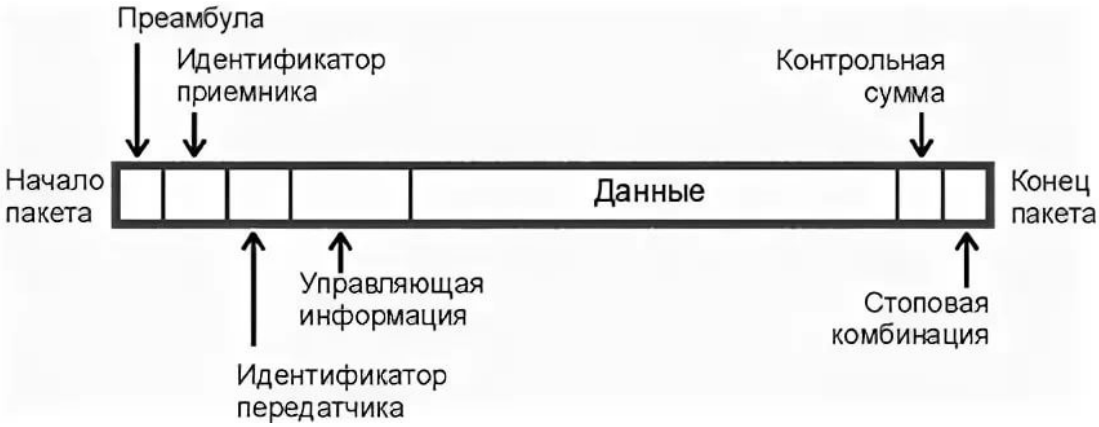

Рисунок 5 - Типичная структура пакета

Пример простейшего протокола показан на рисунке 6.

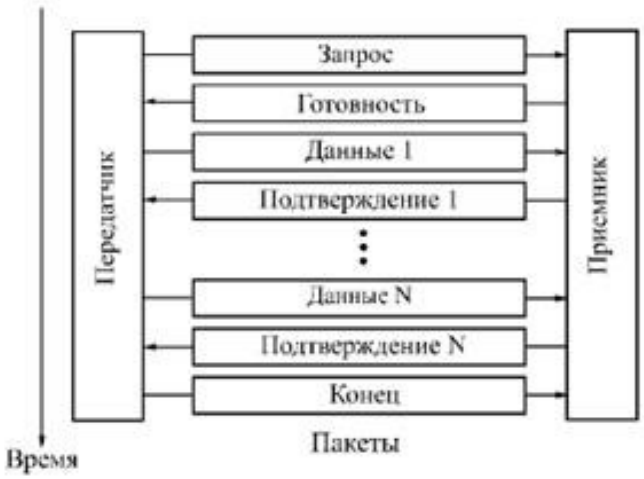

Рисунок 6 - Пример обмена пакетами при сеансе связи

Сеанс обмена начинается с запроса передатчиком готовности приемника принять данные. Для этого используется управляющий пакет "Запрос". Если приемник не готов, он отказывается от сеанса специальным управляющим пакетом. В случае, когда приемник готов, он посылает в ответ управляющий пакет "Готовность". Затем начинается собственно передача данных. При этом на каждый полученный информационный пакет приемник отвечает управляющим пакетом "Подтверждение". В случае, когда пакет данных передан с ошибками, в ответ на него приемник запрашивает повторную передачу. Заканчивается сеанс управляющим пакетом "Конец", которым передатчик сообщает о разрыве связи. Существует множество стандартных протоколов, которые используют как передачу с подтверждением (с гарантированной доставкой пакета), так и передачу без подтверждения (без гарантии доставки пакета).

Для топологии звезда лучше всего подходит централизованный метод управления. Это связано с тем, что все информационные потоки проходят через центр, и именно этому центру логично доверить управление обменом в сети. Причем не так важно, что находится в центре звезды: компьютер (центральный абонент), или же специальный концентратор, управляющий обменом, но сам не участвующий в нем. В данном случае речь идет не о пассивной звезде а, о некой промежуточной ситуации, когда центр не является полноценным абонентом, но управляет обменом. Это, к примеру, реализовано в сети 100VG-AnyLAN.

Самый простейший централизованный метод состоит в следующем. Периферийные абоненты, желающие передать свой пакет (или, как еще говорят, имеющие заявки на передачу), посылают центру свои запросы (управляющие пакеты или специальные сигналы). Центр же предоставляет им право передачи пакета в порядке очередности, например, по их физическому расположению в звезде по часовой стрелке. После окончания передачи пакета каким-то абонентом право передавать получит следующий по порядку (по часовой стрелке) абонент, имеющий заявку на передачу (Рисунок 7). Например, если передает второй абонент, то после него имеет право на передачу третий. Если же третьему абоненту не надо передавать, то право на передачу переходит к четвертому и т.д.

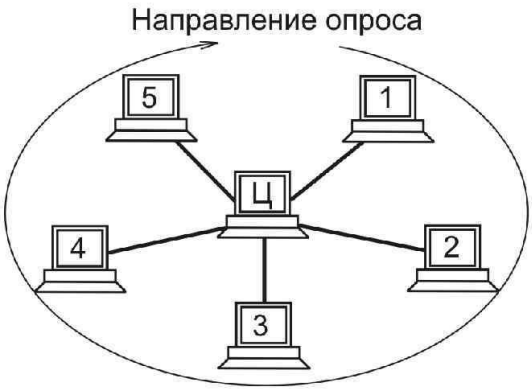

Рисунок 7 - Централизованный метод управления обменом в сети с топологией звезда

Рассмотренный метод управления можно назвать методом с пассивным центром, так как центр пассивно прослушивает всех абонентов. Возможен и другой принцип реализации централизованного управления (его можно назвать методом с активным центром).

В этом случае центр посылает запросы о готовности передавать (управляющие пакеты или специальные сигналы) по очереди всем периферийным абонентам. Тот периферийный абонент, который хочет передавать (первый из опрошенных) посылает ответ (или же сразу начинает свою передачу). В дальнейшем центр проводит сеанс обмена именно с ним. После окончания этого сеанса центральный абонент продолжает опрос периферийных абонентов по кругу. Если желает передавать центральный абонент, он передает вне очереди.

Как в первом, так и во втором случае никаких конфликтов быть не может (решение принимает единый центр, которому не с кем конфликтовать). Если все абоненты активны, и заявки на передачу поступают интенсивно, то все они будут передавать строго по очереди. Но центр должен быть исключительно надежен, иначе будет парализован весь обмен. Механизм управления не слишком гибок, так как центр работает по жестко заданному алгоритму. К тому же скорость управления невысока. Ведь даже в случае, когда передает только один абонент, ему все равно приходится ждать после каждого переданного пакета, пока центр опросит всех остальных абонентов.

Как правило, централизованные методы управления применяются в небольших сетях (с числом абонентов не более чем несколько десятков). В случае больших сетей нагрузка по управлению обменом на центр существенно возрастает.

Предприятие «Фирма» – динамично развивающаяся компания, отвечающее высоким требования. Компания осуществляет многоуровневую продажу товаров для торговли и строительной деятельности.

В здание компании «Фирма» имеется 8 компьютеров. В компании уже имеется ЛВС, поэтому спроектируем простую сеть в ходе практике, которая не будет мешать работоспособности предприятию. Во время проектирования ЛВС решались следующие задачи:

- анализ методов управления обмена в сети;
- обзор и анализ возможных технологий построения сети;
- выбор оборудования и программного обеспечения для ЛВС;
- проектирование общей схемы ЛВС колледжа;
- расчет затрат на покупку сетевого оборудования и программного обеспечения.

При выборе оборудования и программного обеспечения подразумевается наличие в колледже нужного количества ПК, с установленным лицензионным ПО, которое указанно в разрабатываемом проекте ЛВС предприятия. На каждом ПК и сервере установлены сетевые платы для подключения к сети. В качестве коммутаторов будут использоваться гигабитные и 100 мегабитные Switch фирмы D-Link. Кабель будет использоваться экранированный и неэкранированный категории 5 (витая пара).

Для выхода в Internet используется технология ADSL, позволяющая получать скорость потока данных в пределах от 1,5 Мбит/сек, до 8 Мбит/сек. Технология ADSL позволяет телекоммуникационным компаниям предоставлять частный защищенный канал между пользователем и провайдером. Технология ADSL – самая распространенная и востребованная услуга на настоящий момент. Эта технология способна превратить телефонные аналоговые линии пользователей в линии высокоскоростного доступа. В помещении абонента устанавливается ADSL-модем, который при помощи специального частотного разделителя – сплиттера подключается параллельно телефонному аппарату. При этом телефонная линия остается свободной, и пользователь может одновременно работать в сети Интернет и разговаривать по телефону.

Данная технология в настоящее время является наиболее продвинутой в семействе xDSL. Она позволяет обеспечить скорость передачи данных до 8 Мбит/сек в одном направлении (в сторону пользователя) и до 1,5 Мбит/сек в другом направлении (указанные скорости могут быть снижены в зависимости от установленного оборудования, качества кабеля, протяженности абонентской телефонной линии). Более высокоскоростная версия ADSL 2+ позволяет развивать скорость до 24 Мбит/сек в сторону пользователя и до 256 Кбит/сек в другом направлении.

Огромным плюсом технологии ADSL является то, что при ее использовании нет необходимости организации отдельного "физического" канала от АТС до пользователя, а используется уже имеющееся телефонная линия. ADSL — это технология постоянного, некоммутируемого соединения пользователя, это значит, что не требуется каждый раз устанавливать связь с провайдером, вы всегда подключены к сети передачи данных, а оплата производится не за время нахождения в сети интернет, а за объемы полученной информации. Это создает неоспоримые преимущества при работе с объемами информации, вызывающими долгое ожидание при обычном, коммутируемом доступе.

25. Итоговое тестирование созданной локальной сети в работе отдела предприятия.

Краткое описание используемого сетевого оборудования для составления ЛВС.

1. Коммутаторы:

1. D-LinkDES-1018DG

Коммутатор, имеющий 16 портов + 2 дополнительных порта. Настольный коммутатор с плотностью портов 10/100 Мбит/сек. Имеет 16 портов по технологии Fast Ethernet (100/1000 Base-TX) и 2 порта по технологии Gigabit Ethernet (1000 Base-T). Данный коммутатор позволяет подключать кабель на основе витой пары категории 5.

2. D-Link DES-1016D

Неуправляемый коммутатор 10/100 Мбит/сек, имеющий 2 уровня (переход с технологии Ethernet на Fast Ethernet). Имеет 16 портов, автоматически определяющих сетевую скорость, согласовывающий стандарт 10 Base-T и 10 Base-TX.

3. D-Link DES-1008D

Аналог коммутатора DES-1016-D, но имеет всего лишь 8 портов.

2. Модем: ACORP Sprinter@ADSL LAN410.

Внешний ADSL2+ модем с 4-мя Ethernet-портами и функцией маршрутизатора. Возможна быстрая установка соединений, прост в настройке. При использовании данного модема свободна телефонная линия. Высокая скорость и стабильная связь. Соответствие стандартам обеспечивает совместимость с оборудованием Интернет-провайдеров. Скорость входящего потока – до 8 Мбит/сек для ADSL, до 24 Мбит/сек для ADSL2+.

Скорость исходящего потока до 1 Мбит/сек, 3 Мбит/сек для AnnexM. Автоматический выбор максимально возможной скорости соединения. Оптимизирован для IP TV, VoIP/.

Таблица 3 - Основные технико-экономические показатели проекта

Основные характеристики	Ед. изм.	Проект
Технические		
Скорость передачи данных	Мбит/сек	100 Мбит/сек
Количество рабочих станций		34
Топология		звезда
Среда передачи данных		витая пара
Пороговая граница коэфициента загрузки сети	%	0,3…0,5
Защищенность от перегрузок электропитания	кВ	1,0 кВ электросеть 0,5 кВ сигнальная сеть
Эксплуатационные		
Возможность администрирования всей сети с одной рабочей станции		протокол SNMP
Возможность мониторинга сети		протокол RMON
Высокая надежность		пожизненная гарантия на все оборудование
Экономические		
Стоимость внедрения проекта	у.е.	3138
Экономия заработной платы (прибыль)	у.е.	40379,5
Срок окупаемости	лет	~ 0,08

Таким образом, предприятие внедрив сеть, будет иметь прибыль за счет экономии фондов оплаты труда и за счет экономии на налоговых отчислениях, и, окупит затраты на внедрение сети за ~ 3 месяца.

Общие затраты на проектирование и создание сети определяются:

KLAN = K1 + K2, (4)

Где:

K1 - производственные затраты;

K2 - капитальные вложения.

Оценим производственные затраты:

K1 = C1 + C2 + C3, (5)

Где:

C1 - затраты на НИР и ТЗ;

C2 - затраты на опытную эксплуатацию и внедрение;

C3 - затраты на рабочий проект.

Смета производственных затрат приведена в Таблице 4.

Таблица 4 - Смета производственных затрат

Производственные затраты	Сумма
Затраты на НИР и ТЗ	14439
Затраты на опытную эксплуатацию и внедрение	72197
Затраты на рабочий проект	14439
ИТОГО	101076 руб.

Современная стадия развития ЛВС характеризуется почти повсеместным переходом от отдельных, как правило, уже существующих, сетей, к сетям, которые охватывают все предприятие (фирму, компанию) и объединяют разнородные вычислительные ресурсы в единой среде. Такие сети называются корпоративными.

Важнейшей характеристикой ЛВС является скорость передачи информации. В идеале при посылке и получении данных через сеть время отклика должно быть таким же, как если бы они были получены от ПК пользователя, а не из некоторого места вне сети. Это требует скорости передачи данных от 1 до 10 Мбит/с и более.

В данной работе была спроектирована высокоскоростная - вычислительная сеть Ethernet для предприятия ООО «Фирма».

Заключение

В процессе прохождения практики освоил средства обеспечения информационной безопасности, а также закрепил знания, умения, полученные в техникуме, и приобрел опыт практической работы в организации, получил профессиональные знания, умения и навыки при выполнении конкретных практических задач.

ЛИТЕРАТУРА

1. Торокин А.А. «Инженерно-техническая защита информации», - М: Гелиос АРВ, 2005. -960с.

2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В., Скрыль С.В., Голубятников И.В. «Технические средства и методы защиты информации: Учебник для вузов»,- М.: ООО "Издательство Машиностроение", 2009. - 508с.

3. Герасименко В.Г., Лаврухин Ю.Н., Тупота В.И. Методы защиты акустической речевой информации от утечки по техническим каналам. - М.: РЦИБ «Факел», 2008. - 256 с.

4. Дворянкин С. В., Харченко Л. А., Козлачков С.Б. Оценка защищенности речевой информации с учетом современных технологий шум очистки. /Вопросы защиты информации. М.: ФГУП «ВИМИ», 2007. № 2 (77). С. 37 40.

5. Хорев А.А. Техническая защита информации: учебное пособие для студентов вузов. /Т.1. Технические каналы утечки информации. - М.; НПЦ «Аналитика», 2008. - 436 с.: ил.

6. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2011. – 704 с.

7. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2008

8. Кофлер М., Linux. Полное руководство – Питер, 2011. – 800 с.

9. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2008

10. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 2-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2007.- 531 с.

11. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 4-е изд. – М.: Вильямс, 2004. – 656 с.