**Содержание**

Введение

1. Пути и методы защиты информации в системах обработки данных

1.1 Пути несанкционированного доступа, классификация способов и средств защиты информации

1.1.1 Средства защиты информации

1.1.2 Способы защиты информации

1.2 Анализ методов защиты информации в ЛВС

1.2.1 Защита информации в ПЭВМ. Каналы утечки информации

1.2.2 Организационные и организационно-технические меры защиты информации в локальных вычислительных сетях

1.2.3 Основные методы защиты ПЭВМ от утечек информации по электромагнитному каналу

1.2.4 Идентификация и аутентификация

1.2.5 Управление доступом

1.2.6 Протоколирование и аудит

1.2.7 Криптография

1.2.8 Экранирование

1.3 Основные направления защиты информации в ЛВС

1.3.1 Меры непосредственной защиты ПЭВМ

1.3.2 Идентификация и установление личности

1.3.3 Защита против электронного и электромагнитного перехвата

1.3.4 Основные понятия безопасности компьютерных систем

1.3.5 Современные программные угрозы информационной безопасности

1.3.6 Основные типы угроз вычислительным системам

1.3.7 Анализ и классификация удаленных атак в ЛВС

2. Защиты информации в локальных вычислительных сетях ЗАО завода Лит

2.1 Анализ системы защиты информации в ЛВС ЗАО завода ЛИТ

2.1.1 Отдел АСУ: назначение и задачи решаемые отделом

2.1.2 Структура отдела АСУ ЗАО завода ЛИТ

2.2 Программное обеспечение отдела АСУ ЗАО завода ЛИТ

2.2.1 Особенности работы отдела АСУ в конкретной операционной системе

2.2.2 Прикладное и специальное программное обеспечение

2.2.3 Защита информации в ЛВС программными средствами

2.3 Компьютерная телекоммуникационная сеть отдела АСУ

2.3.1 Структура сети, топология ЛВС ЗАО завода ЛИТ

2.3.2 Основные технические характеристики сетевого оборудования

2.3.3 Управление доступом к информации в локальной сети

2.4 Политика безопасности ЗАО завода ЛИТ при его информатизации

2.4.1 Концепция безопасности ЛВС ЗАО завода ЛИТ

2.4.2 Обеспечение безопасности при групповой обработке информации в подразделениях и отделах ЗАО завода ЛИТ

3. Экономическая часть

Заключение

Список литературы

Приложения

Приложение 1 Структурная схема локальной сети ЗАО завода ЛИТ

**Введение**

Вопрос защиты информации поднимается уже с тех пор, как только люди научились письменной грамоте. Всегда существовала информацию, которую должны знать не все. Люди, обладающие такой информацией, прибегали к разным способам ее защиты. Из известных примеров это такие способы как тайнопись, шифрование. В настоящее время всеобщей компьютеризации благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности множества компьютерных систем обработки информации, а также контроля и управления различными объектами. К таким объектам можно отнести системы телекоммуникаций, банковские системы, атомные станции, системы управления воздушным и наземным транспортом, системы обработки и хранения секретной и конфиденциальной информации. Для нормального и безопасного функционирования этих систем необходимо поддерживать их безопасность и целостность. В настоящее время для проникновения в чужие секреты используются такие возможности как:

1. подслушивание разговоров в помещении или автомашине с помощью предварительно установленных "радиожучков" или магнитофонов;
2. контроль телефонов, телефаксных линий связи и радиостанций;
3. дистанционный съем информации с различных технических средств, в первую очередь по локальной сети, с мониторов и печатающих устройств компьютеров и другой электронной техники;
4. лазерное облучение оконных стекол в помещении, где ведутся "интересные разговоры".

Обилие приемов съема информации противодействует большое количество организационных и технических способов, так называемая специальная защита. Одним из основных направлений специальной защиты является поиск техники подслушивания или поисковые мероприятия. В системе защиты объекта поисковые мероприятия выступают как средства обнаружения и ликвидации угрозы съема информации.

Проблемы защиты информации в локальных вычислительных сетях (ЛВС) постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Под защитой информации понимается использование специальных средств, методов и мероприятий с целью предотвращения утери информации, находящейся в ЛВС. Широкое распространение и повсеместное применение вычислительной техники очень резко повысили уязвимость накапливаемой, хранимой и обрабатываемой в ЛВС информации.

Четко обозначилось три аспекта уязвимости информации:

1. Подверженность физическому уничтожению или искажению.
2. Возможность несанкционированной (случайной или злоумышленной) модификации.
3. Опасность несанкционированного получения информации лицами, для которых она не предназначена.

Основные направления защиты информации в ЛВС:

1. совершенствование организационных и организационно-технических мероприятий технологии обработки информации в ЭВМ;
2. блокирование несанкционированного доступа к обрабатываемой в ЭВМ информации;
3. блокирование несанкционированного получения информации с помощью технических средств.

Основными факторами затрудняющими решение проблемы защиты информации в ЛВС являются:

1. массовость применения;
2. постоянно растущая сложность функционирования;
3. разнообразие программного обеспечения персональных компьютеров, архитектурных решений и легкая адаптируемость для решения разнообразных задач пользователей.

Следует отметить, что использование USB флеш-накопителей (гибких магнитных дисков) создает условия для злоумышленных действий (подмена, хищение, внесение в систему «компьютерного вируса», несанкционированное копирование информации, незаконное использование сети ЭВМ и др.). Важнейшая мера защиты информации на этом направлении - четкая организация и контроль использования USB флеш-накопителей (ГМД).

Любая ЭВМ при работе создает электромагнитное поле, которое позволяет несанкционированно принимать и получать информацию. В ПК это особенно опасно, так как информация, обрабатываемая в них более структурирована. В целях защиты используются самые различные мероприятия от экранирования зданий и помещений до подавления излучений специальными генераторами шумов.

Так же одним из основных средств защиты информации в ЭВМ являются криптографические средства. Они имеют своей задачей защиту информации при передаче по линиям связи локальной сети, хранении на магнитных носителях, а так же препятствуют вводу ложной информации.

Чтобы надежно защитить информацию, система защиты должна регулярно обеспечивать защиту:

1. Системы обработки данных от посторонних лиц.
2. Системы обработки данных от пользователей.
3. Пользователей друг от друга и каждого пользователя от самого себя.
4. Систем обработки от самой себя.

Целью дипломной работы является разработка общих рекомендаций для данного отдела АСУ, по обеспечению защиты информации в ЛВС и разработка типового пакета документов по недопущению несанкционированного доступа к служебной и секретной информации.

Актуальность выбранной мною темы состоит:

* в разработке политики безопасности учреждения в условиях информационной борьбы;
* в глубокой проработке и решении ряда важных проблем, направленных на повышение информационной безопасности в ЛВС;
* в разработке и введении в работу пакета документов по безопасности информации в данном учреждении.

защита информация компьютерная система

**1. Пути и методы защиты информации в локальных вычислительных сетях**

**1.1Пути несанкционированного доступа, классификация способов и средств защиты информации**

Архитектура ЛВС и технология ее функционирования позволяет злоумышленнику находить или специально создавать лазейки для скрытого доступа к информации, причем многообразие и разнообразие даже известных фактов злоумышленных действий дает достаточные основания предполагать, что таких лазеек существует или может быть создано много. Пути несанкционированного получения информации приведены на рисунке 1.1.

Несанкционированный доступ к информации, находящейся в ЛВС бывает:

* косвенным - без физического доступа к элементам ЛВС;
* прямым - с физическим доступом к элементам ЛВС.

В настоящее время существуют следующие пути несанкционированного получения информации (каналы утечки информации):

1. применение подслушивающих устройств;
2. дистанционное фотографирование;
3. перехват электромагнитных излучений;
4. хищение носителей информации и производственных отходов;
5. считывание данных в массивах других пользователей;
6. копирование носителей информации;
7. несанкционированное использование терминалов;
8. маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;
9. использование программных ловушек;
10. получение защищаемых данных с помощью серии разрешенных запросов;
11. использование недостатков языков программирования и операционных систем;
12. преднамеренное включение в библиотеки программ специальных блоков типа “троянских коней”;
13. незаконное подключение к аппаратуре или линиям связи вычислительной системы;
14. злоумышленный вывод из строя механизмов защиты.

**1.1.1 Средства защиты информации**

Для решения проблемы защиты информации основными средствами, используемыми для создания механизмов защиты принято считать:

1. Технические средства - реализуются в виде электрических, электромеханических, электронных устройств. Технические средства подразделяются на:

1. аппаратные - устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой ЛВС по стандартному интерфейсу (схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры);
2. физические - реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения. Замки на дверях, решетки на окнах).
3. Программные средства - программы, специально предназначенные для выполнения функций, связанных с защитой информации.

В ходе развития концепции защиты информации специалисты пришли к выводу, что использование какого-либо одного из выше указанных способов защиты, не обеспечивает надежного сохранения информации. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации.

**1.1.2 Способы защиты информации**

Способы защиты информации представлены на рисунке 1.2. Способы защиты информации в ЛВС включают в себя следующие элементы:

1. Препятствие - физически преграждает злоумышленнику путь к защищаемой информации (на территорию и в помещения с аппаратурой, носителям информации).

2. Управление доступом - способ защиты информации регулированием использования всех ресурсов системы (технических, программных средств, элементов данных).

Управление доступом включает следующие функции защиты:

1. идентификацию пользователей, персонала и ресурсов системы, причем под идентификацией понимается присвоение каждому названному выше объекту персонального имени, кода, пароля и опознание субъекта или объекта по предъявленному им идентификатору;
2. проверку полномочий, заключающуюся в проверке соответствия дня недели, времени суток, а также запрашиваемых ресурсов и процедур установленному регламенту;
3. разрешение и создание условий работы в пределах установленного регламента;
4. регистрацию обращений к защищаемым ресурсам;
5. реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.

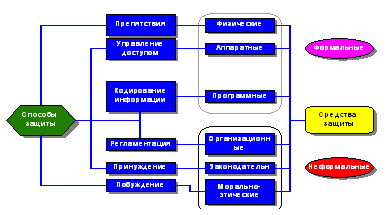


Рисунок 1.1 Способы и средства защиты информации в ЛВС

3. Маскировка - способ защиты информации в ЛВС путем ее криптографического преобразования. При передаче информации по линиям связи большой протяженности криптографическое закрытие является единственным способом надежной ее защиты.

4. Регламентация - заключается в разработке и реализации в процессе функционирования ЛВС комплексов мероприятий, создающих такие условия автоматизированной обработки и хранения в ЛВС защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму. Для эффективной защиты необходимо строго регламентировать структурное построение ЛВС (архитектура зданий, оборудование помещений, размещение аппаратуры), организацию и обеспечение работы всего персонала, занятого обработкой информации.

5. Принуждение - пользователи и персонал ЛВС вынуждены соблюдать правила обработки и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Рассмотренные способы защиты информации реализуются применением различных средств защиты, причем различают технические, программные, организационные, законодательные и морально-этические средства.

Организационными средствами защиты называются организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации ЛВС для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы ЛВС на всех этапах: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

К законодательным средствам защиты относятся законодательные акты страны, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

К морально-этическим средствам защиты относятся всевозможные нормы, которые сложились традиционно или складываются по мере распространения вычислительных средств в данной стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета, престижа человека или группы лиц.

Рассмотренные выше средства защиты подразделяются на:

1. формальные - выполняющие защитные функции строго по заранее предусмотренной процедуре и без непосредственного участия человека.
2. неформальные - такие средства, которые либо определяются целенаправленной деятельностью людей, либо регламентируют эту деятельность.

**1.2 Анализ методов защиты информации в ЛВС**

Обеспечение надежной защиты информации предполагает:

1. Обеспечение безопасности информации в ЛВС это есть процесс непрерывный, заключающийся в систематическом контроле защищенности, выявлении узких и слабых мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.
2. Безопасность информации в ЛВС может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.
3. Надлежащую подготовку пользователей и соблюдение ими правил защиты.
4. Ни одна система защиты не считается абсолютно надежной. Надо исходить их того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

**1.2.1 Защита информации в ПЭВМ. Каналы утечки информации**

Защита информации в ПЭВМ - организованная совокупность правовых мероприятий, средств и методов (организационных, технических, программных), предотвращающих или снижающих возможность образования каналов утечки, искажения обрабатываемой или хранимой информации в ПЭВМ.

Организационные меры защиты - меры общего характера, затрудняющие доступ к ценной информации посторонним лицам, вне зависимости от особенностей способа обработки информации и каналов утечки информации.

Организационно-технические меры защиты - меры, связанные со спецификой каналов утечки и метода обработки информации, но не требующие для своей реализации нестандартных приемов и/или оборудования.

Технические меры защиты - меры, жестко связанные с особенностями каналов утечки и требующие для своей реализации специальных приемов, оборудования или программных средств.

Каналы утечки информации.

Канал утечки информации - совокупность источника информации, материального носителя или среды распространения несущего эту информацию сигнала и средства выделения информации из сигнала или носителя.

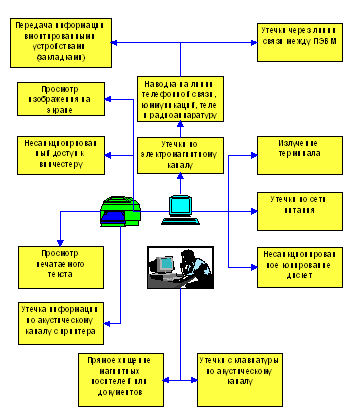


Рисунок 1.2 Основные каналы утечки информации при ее обработке на ПЭВМ

Известны следующие каналы утечки информации (Рисунок 1.3):

1. Электромагнитный канал. Причиной его возникновения является электромагнитное поле, связанное с протеканием электрического тока в технических средствах обработки информации. Электромагнитное поле может индуцировать токи в близко расположенных проводных линиях (наводки).

Электромагнитный канал в свою очередь делится на:

1. Радиоканал (высокочастотные излучения).
2. Низкочастотный канал.
3. Сетевой канал (наводки на провода заземления).
4. Канал заземления (наводки на провода заземления).
5. Линейный канал (наводки на линии связи между ПЭВМ).
6. Акустический канал. Он связан с распространением звуковых волн в воздухе или упругих колебаний в других средах, возникающих при работе устройств отображения информации.
7. Канал несанкционированного копирования.
8. Канал несанкционированного доступа.

Программные “вирусы” - программы, обладающие свойствами самодублирования и могущие скрывать признаки своей работы и причинять ущерб информации в ПЭВМ.

Вирусы делятся на:

1. файловые - присоединяются к выполняемым файлам;
2. загрузочные - размещаются в загрузочных секторах ПЭВМ.

**1.2.2 Организационные и организационно-технические меры защиты информации в системах обработки данных**

Организационные меры предусматривают:

1. Ограничение доступа в помещения, в которых происходит обработка конфиденциальной информации.
2. Допуск к решению задач на ПЭВМ по обработке секретной, конфиденциальной информации проверенных должностных лиц, определение порядка проведения работ на ПЭВМ.
3. Хранение магнитных носителей в тщательно закрытых прочных шкафах.
4. Назначение одной или нескольких ПЭВМ для обработки ценной информации и дальнейшая работа только на этих ПЭВМ.
5. Установка дисплея, клавиатуры и принтера таким образом, чтобы исключить просмотр посторонними лицами содержания обрабатываемой информации.
6. Постоянное наблюдение за работой принтера и других устройств вывода на материальных носитель ценной информации.
7. Уничтожение красящих лент или иных материалов, содержащих фрагменты ценной информации.
8. Запрещение ведения переговоров о непосредственном содержании конфиденциальной информации лицам, занятым ее обработкой.

Организационно-технические меры предполагают:

1. Ограничение доступа внутрь корпуса ПЭВМ путем установления механических запорных устройств.
2. Уничтожение всей информации на винчестере ПЭВМ при ее отправке в ремонт с использованием средств низкоуровневого форматирования.
3. Организацию питания ПЭВМ от отдельного источника питания или от общей (городской) электросети через стабилизатор напряжения (сетевой фильтр).
4. Использование для отображения информации жидкокристаллических или плазменных дисплеев, а для печати - струйных или лазерных принтеров.
5. Размещение дисплея, системного блока, клавиатуры и принтера на расстоянии не менее 2,5-3,0 метров от устройств освещения, кондиционирования воздуха, связи (телефона), металлических труб, телевизионной и радиоаппаратуры, а также других ПЭВМ, не использующихся для обработки конфиденциальной информации.
6. Отключение ПЭВМ от локальной сети или сети удаленного доступа при обработке на ней конфиденциальной информации, кроме случая передачи этой информации по сети.
7. Установка принтера и клавиатуры на мягкие прокладки с целью снижения утечки информации по акустическому каналу.
8. Во время обработки ценной информации на ПЭВМ рекомендуется включать устройства, создающие дополнительный шумовой фон (кондиционеры, вентиляторы), обрабатывать другую информацию на рядом стоящих ПЭВМ.
9. Уничтожение информации непосредственно после ее использования.

**1.2.3 Основные методы защиты ПЭВМ от утечек информации по электромагнитному каналу**

Основным источником высокочастотного электромагнитного излучения является дисплей. Изображение с его экрана можно принимать на расстоянии сотен метров. Полностью нейтрализовать утечку можно лишь с использованием генераторов шума. Другим способ защиты является использование плазменных или жидкокристаллических дисплеев.

Еще одним надежным способом является полное экранирование помещения стальными, алюминиевыми или из специальной пластмассы листами толщиной не менее 1 мм с надежным заземлением. На окна в этом случае рекомендуется помещать сотовый фильтр - алюминиевую решетку с квадратными ячейками размером не более 1 см.

Принтер является источником мощного низкочастотного электромагнитного излучения, которое быстро затухает с ростом расстояния. Тем не менее, это излучение также опасно. Борьба с ним крайне затруднена, так как оно имеет сильную магнитную составляющую, которая плохо зашумляется и экранируется. Поэтому рекомендуется либо зашумление мощным шумовым сигналом, либо использование струйного или лазерного принтеров, или термопечати.

Очень опасны специально встроенные в ПЭВМ передатчики или радиомаяки (закладки - программные или технические средства, облегчающие выделение информации из каналов утечки или нарушающие предписанный алгоритм работы ПЭВМ). По этой же причине не рекомендуется обрабатывать ценную информацию на случайных ПЭВМ и подделках под фирму из развивающихся стран. Если компьютер отсылался в ремонт, то необходимо убедиться, что в нем нет закладок.

Электромагнитное излучение от внешних проводников и кабелей ПЭВМ невелика, но необходимо следить, чтобы они не пересекались с проводами, выходящими за пределы помещения.

Монтаж заземления от периферийного оборудования необходимо вести в пределах контролируемой зоны. Нельзя допускать, чтобы заземление пересекалось с другими проводниками. Все соединения ПЭВМ с “внешним миром” необходимо проводить через электрическую развязку.

Основными сервисами безопасности являются:

* идентификация и аутентификация,
* управление доступом,
* протоколирование и аудит,
* криптография,
* экранирование.

**1.2.4 Идентификация и аутентификация**

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация - это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту - пользователю или процессу, действующему от имени определенного пользователя, назвать себя, сообщив свое имя. Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого себя выдает. В качестве синонима слова "аутентификация" иногда используют сочетание "проверка подлинности". Субъект может подтвердить свою подлинность, если предъявит, по крайней мере, одну из следующих сущностей:

* нечто, что он знает: пароль, личный идентификационный номер, криптографический ключ и т.п.;
* нечто, чем он владеет: личную карточку или иное устройство аналогичного назначения;
* нечто, что является частью его самого: голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики.

Надежная идентификация и аутентификация затруднена по ряду принципиальных причин.

Во-первых, компьютерная система основывается на информации в том виде, в каком она была получена; строго говоря, источник информации остается неизвестным. Например, злоумышленник мог воспроизвести ранее перехваченные данные. Следовательно, необходимо принять меры для безопасного ввода и передачи идентификационной и аутентификационной информации; в сетевой среде это сопряжено с особыми трудностями.

Во-вторых, почти все аутентификационные сущности можно узнать, украсть или подделать.

В-третьих, имеется противоречие между надежностью аутентификации с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это повышает вероятность подглядывания за вводом.

В-четвертых, чем надежнее средство защиты, тем оно дороже.

Необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации. Обычно компромисс достигается за счет комбинирования двух первых из перечисленных базовых механизмов проверки подлинности.

Наиболее распространенным средством аутентификации являются пароли. Система сравнивает введенный и ранее заданный для данного пользователя пароль; в случае совпадения подлинность пользователя считается доказанной. Другое средство, постепенно набирающее популярность и обеспечивающее наибольшую эффективность, - секретные криптографические ключи пользователей.

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее по совокупности характеристик их следует признать самым слабым средством проверки подлинности. Надежность паролей основывается на способности помнить их и хранить в тайне. Ввод пароля можно подсмотреть. Пароль можно угадать методом подбора. Если файл паролей зашифрован, но доступен на чтение, его можно перекачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор.

Пароли уязвимы по отношению к электронному перехвату - это наиболее принципиальный недостаток, который нельзя компенсировать улучшением администрирования или обучением пользователей. Практически единственный выход - использование криптографии для шифрования паролей перед передачей по линиям связи или вообще их не передавать.

Тем не менее следующие меры позволяют значительно повысить надежность парольной защиты:

* наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
* управление сроком действия паролей, их периодическая смена;
* ограничение доступа к файлу паролей;
* ограничение числа неудачных попыток входа в систему, что затруднит применение метода подбора;
* обучение и воспитание пользователей;
* использование программных генераторов паролей, которые, основываясь на несложных правилах, могут порождать только благозвучные и, следовательно, запоминающиеся пароли.

Устройства контроля биометрических характеристик сложны и недешевы, поэтому пока они применяются только в специфических организациях с высокими требованиями к безопасности.

Очень важной и трудной задачей является администрирование службы идентификации и аутентификации. Необходимо постоянно поддерживать конфиденциальность, целостность и доступность соответствующей информации, что особенно непросто в сетевой разнородной среде. Целесообразно, наряду с автоматизацией, применить максимально возможную централизацию информации. Достичь этого можно применяя выделенные серверы проверки подлинности или средства централизованного администрирования. Некоторые операционные системы предлагают сетевые сервисы, которые могут служить основой централизации административных данных.

Централизация облегчает работу не только системным администраторам, но и пользователям, поскольку позволяет реализовать важную концепцию единого входа. Единожды пройдя проверку подлинности, пользователь получает доступ ко всем ресурсам сети в пределах своих полномочий.

**1.2.5 Управление доступом**

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты - пользователи и процессы могут выполнять над объектами - информацией и другими компьютерными ресурсами. Речь идет о логическом управлении доступом, который реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность путем запрещения обслуживания неавторизованных пользователей. Задача логического управления доступом состоит в том, чтобы для каждой пары (субъект - объект) определить множество допустимых операций, зависящее от некоторых дополнительных условий, и контролировать выполнение установленного порядка.

Контроль прав доступа производится разными компонентами программной среды - ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением и т.д.

При принятии решения о предоставлении доступа обычно анализируется следующая информация.

* Идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера). Подобные идентификаторы являются основой добровольного управления доступом.
* Атрибуты субъекта (метка безопасности, группа пользователя). Метки безопасности - основа принудительного управления доступом.
* Место действия (системная консоль, надежный узел сети).
* Время действия (большинство действий целесообразно разрешать только в рабочее время).
* Внутренние ограничения сервиса (число пользователей согласно лицензии на программный продукт).

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ.

**1.2.6 Протоколирование и аудит**

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе предприятия. У каждого сервиса свой набор возможных событий, но в любом случае их можно подразделить на внешние - вызванные действиями других сервисов, внутренние - вызванные действиями самого сервиса и клиентские - вызванные действиями пользователей и администраторов.

Аудит - это анализ накопленной информации, проводимый оперативно, почти в реальном времени, или периодически.

Реализация протоколирования и аудита преследует следующие цели:

* обеспечение подотчетности пользователей и администраторов;
* обеспечение возможности реконструкции последовательности событий;
* обнаружение попыток нарушений информационной безопасности;
* предоставление информации для выявления и анализа проблем.

Обеспечение подотчетности важно в первую очередь как средство сдерживания. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Если есть основания подозревать какого-либо пользователя в нечестности, можно регистрировать его действия особенно детально, вплоть до каждого нажатия клавиши. При этом обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и откат некорректных изменений. Тем самым обеспечивается целостность информации.

Реконструкция последовательности событий позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

Выявление и анализ проблем позволяют помочь улучшить такой параметр безопасности, как доступность. Обнаружив узкие места, можно попытаться переконфигурировать или перенастроить систему, снова измерить производительность и т.д.

**1.2.7 Криптография**

Одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации является криптография. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности, являясь основой реализации многих из них и, в то же время, последним защитным рубежом.

Различают два основных метода шифрования, называемые симметричными и асимметричными. В первом из них один и тот же ключ используется и для шифровки, и для расшифровки сообщений. Существуют весьма эффективные методы симметричного шифрования. Имеется и стандарт на подобные методы - ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это ставит новую проблему рассылки ключей. С другой стороны, получатель, имеющий шифрованное и расшифрованное сообщение, не может доказать, что он получил его от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать и сам.

В асимметричных методах применяются два ключа. Один из них, несекретный, используется для шифровки и может публиковаться вместе с адресом пользователя, другой - секретный, применяется для расшифровки и известен только получателю. Самым популярным из асимметричных является метод RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (100-значными) простыми числами и их произведениями.

Асимметричные методы шифрования позволяют реализовать так называемую электронную подпись, или электронное заверение сообщения. Идея состоит в том, что отправитель посылает два экземпляра сообщения - открытое и дешифрованное его секретным ключом (естественно, дешифровка незашифрованного сообщения на самом деле есть форма шифрования). Получатель может зашифровать с помощью открытого ключа отправителя дешифрованный экземпляр и сравнить с открытым. Если они совпадут, личность и подпись отправителя можно считать установленными.

Существенным недостатком асимметричных методов является их низкое быстродействие, поэтому их приходится сочетать с симметричными, при этом следует учитывать, что асимметричные методы на 3 - 4 порядка медленнее симметричных. Так, для решения задачи рассылки ключей сообщение сначала симметрично шифруют случайным ключом, затем этот ключ шифруют открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Криптографические методы позволяют надежно контролировать целостность информации. В отличие от традиционных методов контрольного суммирования, способных противостоять только случайным ошибкам, криптографическая контрольная сумма (имитовставка), вычисленная с применением секретного ключа, практически исключает все возможности незаметного изменения данных.

В последнее время получила распространение разновидность симметричного шифрования, основанная на использовании составных ключей. Идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить расшифровку. Если у правоохранительных органов появляются подозрения относительно лица, использующего некоторый ключ, они могут получить половинки ключа и дальше действовать обычным для симметричной расшифровки образом.

**1.2.8 Экранирование**

Экран - это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран выполняет свои функции, контролируя все информационные потоки между двумя множествами систем.

В простейшем случае экран состоит из двух механизмов, один из которых ограничивает перемещение данных, а второй, наоборот, ему способствует. В более общем случае экран или полупроницаемую оболочку удобно представлять себе как последовательность фильтров. Каждый из них может задержать данные, а может и сразу "перебросить" их "на другую сторону". Кроме того, допускаются передача порции данных на следующий фильтр для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю.

Помимо функций разграничения доступа экраны осуществляют также протоколирование информационных обменов.

Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны устанавливают для защиты локальной сети организации, имеющей выход в открытую среду, подобную Internet. Другой пример экрана - устройство защиты порта, контролирующее доступ к коммуникационному порту компьютера до и после независимо от всех прочих системных защитных средств. Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности.

В любой организации найдутся документы и сведения, которые не обязательно знать всем пользователям местной сети. Такая информация должна храниться в специальном каталоге, доступ к которому имеют только уполномоченные лица. Чаще любопытство, чем злой умысел сотрудников заставляют их прочитывать чужие файлы. Одна из причин, по которой в сетях устанавливают систему защиты, состоит в том, чтобы уберечь сетевую информацию от необдуманных действий пользователей.

**1.3 Основные направления защиты информации в ЛВС**

**1.3.1 Меры непосредственной защиты ПЭВМ**

Важным аспектом всестороннего подхода к защите ЭВМ являются меры защиты вычислительных устройств от прямых угроз, которые можно разбить на две категории:

1. Меры защиты от стихийных бедствий.
2. Меры защиты от злоумышленников.

Наиболее опасным из стихийных бедствий можно считать пожар. Соблюдение элементарных пожарных норм позволяет решить эту проблему. Наиболее важен и интересен второй пункт.

Для того, чтобы защитить компьютеры от злоумышленников, а следовательно защитить информацию, необходимо ограничить непосредственный доступ к вычислительной системе. Для этого следует организовать охрану вычислительного комплекса. Можно выделить четыре вида охранных мер:

1. охрана границ территории (некоторой зоны, окружающей здание);
2. охрана самого здания или некоторого пространства вокруг него;
3. охрана входов в здание;
4. охрана критических зон.

Для защиты границ территории можно использовать ограды, инфракрасные или СВЧ-детекторы, датчики движения а также замкнутые телевизионные системы.

Для защиты здания последнее должно иметь толстые стены, желательно из железобетона, толщиной не менее 30-35 см.

При защите входов в здание необходимо надежно охранять все возможные пути проникновения в здание - как обычно используемые входы, так и окна и вентиляционные отверстия.

Обычные входы можно контролировать посредством личного опознавания входящего охраной или с использованием некоторых механизмов, например, ключей или специальных карточек.

Для обнаружения проникновения злоумышленника в критическую зону можно использовать существующие системы сигнализации. Фотометрические системы обнаруживают изменения уровня освещенности. Звуковые, ультразвуковые или СВЧ - системы обнаружения перемещения объектов реагируют на изменение частоты сигнала, отраженного от движущегося тела. Звуковые и сейсмические (вибрационные) системы обнаруживают шум и вибрацию. И наконец, системы, реагирующие на приближение к защищаемому объекту, обнаруживают нарушение структуры электромагнитного или электростатического поля.

**1.3.2 Идентификация и установление личности**

Так как функционирование всех механизмов ограничения доступа, использующих аппаратные средства или средства математического обеспечения основано на предположении, что пользователь представляет собой конкретное лицо, то должен существовать некоторый механизм установления его подлинности. Этот механизм может быть основан на выявлении того, что знает только данный пользователь или имеет при себе, или на выявлении некоторых особенностей самого пользователя.

При использовании замков и электрических или механических кнопочных систем применяются комбинации наборов знаков. Такая система, используемая для регулирования доступа к ЭВМ, называется системой паролей. Недостаток этой системы состоит в том, что пароли могут быть украдены (при этом пользователь может и не заметить потери), забыты или переданы. Для уменьшения опасности связанной с кражей паролей, последние должны часто изменяться, что создает проблемы формирования и распределения паролей. Аналогичный метод, называемый “рукопожатием”, предусматривает успешное выполнение некоторого алгоритма в качестве условия доступа к системе. В процессе “рукопожатия” пользователь должен обменяться с алгоритмом последовательностью паролей (они должны быть названы правильно и в правильной последовательности), хотя сам пользователь не знает алгоритма. Установление подлинности с помощью паролей вследствие своей простоты нашло наиболее широкое применение в вычислительных системах.

Пользователь может иметь при себе стандартный ключ или специальную карточку с нанесенным на нее, например, оптическим, магнитным или другим кодом.

Разработаны знаковые системы, которые основаны на изучении образца подчерка или подписи пользователя. Существуют системы, в которых для установления личности применяют геометрические характеристики руки или спектрограммы голоса пользователя. Также существуют системы, которые используют отпечатки пальцев пользователя и сравнивают их с хранящимися образцами.

**1.3.3 Защита против электронного и электромагнитного перехвата**

Подключение к линиям связи может быть осуществлено двумя способами. При пассивном подключении злоумышленник только прослушивает передаваемые данные, тогда как при активном подключении он передает некоторые собственные данные либо в конце законно передаваемых данных, либо вмести них. Основной мерой противодействия подключениям к линиям связи является шифрование сообщений. Кроме того, так как единственными местами, где легко подключиться к линии передачи данных, являются точки внутри помещений, где расположено передающее или приемное оборудование, линии передачи данных и кабельные шкафы должны надежно охраняться. Подключение к внешним участкам линий связи вынуждает вести передачу данных с высокой степенью уплотнения, что является малоэффективной и дорогостоящей операцией.

Вполне реальной угрозой является перехват электромагнитного излучения от ЭВМ или терминала. Правда, вследствие использования режима мультипрограммирования, когда одновременно обрабатывается несколько заданий пользователей, данные, полученные таким путем от большинства вычислительных систем, очень трудно поддаются дешифрованию. Однако, подслушивание терминалов вполне реально, особенно в пределах дальности порядка 6 м. Трудность выполнения этой операции быстро возрастает с расстоянием, так что подслушивание с расстояния, превышающего 45 м, становится крайне дорогостоящей операцией. При использовании более дорогой аппаратуры можно усилить и слабый сигнал. Например, большинство терминалов с ЭЛТ регенерируют отображаемую информацию через короткие интервалы времени. Следовательно, применяя сложные методы, можно совместно обработать и использовать данные нескольких каких циклов генерации.

**1.3.4 Основные понятия безопасности компьютерных систем**

Под безопасностью информации понимается состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Под целостностью понимается как способность средств вычислительной техники или автоматизированной системы обеспечивать неизменность вида и качества информации в условиях случайного искажения или угрозы разрушения. Согласно руководящему документу Гостехкомиссии России “Защита от несанкционированного доступа к информации. Термины и определения” угрозы безопасности и целостности состоят в потенциально возможных воздействиях на вычислительную систему, которые прямо или косвенно могут нанести ущерб безопасности и целостности информации, обрабатываемой системой.

Ущерб целостности информации состоит в ее изменении, приводящем к нарушению ее вида или качества.

Ущерб безопасности подразумевает нарушение состояния защищенности содержащейся в вычислительной системе информации путем осуществления несанкционированного доступа к объектам вычислительной системы.

Несанкционированный доступ определяется как доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых вычислительными системами. Можно ввести более простое определение несанкционированному доступу: несанкционированный доступ заключается в получении пользователем или программой доступа к объекту, разрешение на который в соответствии с принятой в системе политикой безопасности отсутствует.

Реализация угрозы называется атакой. Человек, стремящийся реализовать угрозу, называется нарушителем, или злоумышленником.  
 Существует множество классификаций видов угроз по принципам и характеру их воздействия на систему, по используемым средствам, по целям атаки и т.д. Рассмотрим общую классификацию угроз безопасности вычислительных систем по средствам воздействия на них. С этой точки зрения все угрозы могут быть отнесены к одному из следующих классов (Рисунок 1.4):

1. Вмешательство человека в работу вычислительной системы. К этому классу относятся организационные средства нарушения безопасности вычислительных систем (кража носителей информации, несанкционированный доступ к устройствам хранения и обработки информации, порча оборудования) и осуществление нарушителем несанкционированного доступа к программным компонентам вычислительной системы (все способы несанкционированного проникновения в вычислительные системы, а также способы получения пользователем-нарушителем незаконных прав доступа к компонентам вычислительной системы). Меры, противостоящие таким угрозам, носят организационный характер (охрана, режим доступа к устройствам вычислительной системы), также включают в себя совершенствование систем разграничения доступа и системы обнаружения попыток атак (попыток подбора паролей).

2. Аппаратно-техническое вмешательство в работу вычислительной системы. Это нарушения безопасности и целостности информации в вычислительной системе с помощью технических средств, например, получение информации по электромагнитному излучению устройств вычислительной системы, электромагнитные воздействия на каналы передачи информации и другие методы. Защита от таких угроз, кроме организационных мер, предусматривает соответствующие аппаратные (экранирование излучений аппаратуры, защита каналов передачи информации от прослушивания) и программные меры (шифрация сообщений в каналах связи).

3. Разрушающее воздействие на программные компоненты вычислительной системы с помощью программных средств. Такие средства называются разрушающими программными средствами. К ним относятся компьютерные вирусы, троянские кони (или «закладки»), средства проникновения в удаленные системы с использованием локальных и глобальных сетей. Средства борьбы с подобными атаками состоят из программно и аппаратно реализованных систем защиты.

**1.3.5 Современные программные угрозы информационной безопасности**

Класс разрушающих программных средств (РПС) составляют компьютерные вирусы, троянские кони (закладки) и средства проникновения в удаленные системы через локальные и глобальные сети (Рисунок 1.5).

Компьютерный вирус – суть его сводится к тому, что программы приобретают свойства, присущие живым организмам, причем самые неотъемлемые – они рождаются, размножаются, умирают. Главное условие существования вирусов – универсальная интерпретация информации в вычислительных системах. Вирус в процессе заражения программы может интерпретировать ее как данные, а в процессе выполнения как исполняемый код. Этот принцип был положен в основу всех современных компьютерных систем, использующих архитектуру фон Неймана.

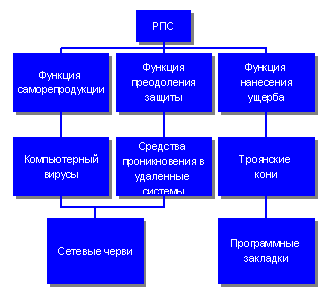


Рисунок 1.3 Типы разрушающих программных средств

Дать формальное определение понятию «компьютерный вирус» очень непросто. Традиционное определение, данное Ф.Коэном, «компьютерный вирус – это программа, которая может заражать другие программы, модифицируя их посредством добавления своей, возможно измененной, копии», ключевым понятием в определении вируса является его способность к саморазмножению, – это единственный критерий, позволяющий отличить программы-вирусы от остальных программ. При этом «копии» вируса действительно могут структурно и функционально отличаться между собой.

Современная ситуация характеризуется двумя моментами: появлением полиморфных вирусов и генераторов (конструкторов) вирусов.

Полиморфные вирусы характеризуются тем, что для их обнаружения неприменимы обычные алгоритмы поиска, так как каждая новая копия вируса не имеет со своим родителем ничего общего. Это достигается шифровкой тела самого вируса и расшифровщиком, не имеющим ни одного постоянного бита в каждом своем экземпляре. На сегодняшний день известно около десятка алгоритмов (вирусов намного больше!) генерации таких расшифровщиков. Появление генераторов вирусов позволяет, задав программе-генератору в виде входных параметров способ распространения, тип, вызываемые эффекты, причиняемый вред, получить ассемблерный текст нового вируса. Вирусы постоянно расширяют свою «среду обитания» и реализуют принципиально новые алгоритмы внедрения и поведения.

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Троянские кони представляют собой программы, реализующие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Программные закладки также содержат некоторую функцию, наносящую ущерб вычислительной системе, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

В качестве примера приведем возможные деструктивные функции, реализуемые троянскими конями и программными закладками:

1. Уничтожение информации.

2. Перехват и передача информации.

3. Целенаправленная модификация кода программы.

Если вирусы и троянские кони наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция разрушающих программных средств, действующих в компьютерных сетях, — взлом атакуемой системы, т.е. преодоление защиты с целью нарушения безопасности и целостности. Этот процесс может быть автоматизирован с помощью специального вида разрушающего программного средства, называемого сетевой червь.

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 100 миллионов компьютеров, подключенных к этой сети.

**1.3.6 Основные типы угроз вычислительным системам**

Существуют три различных типа угроз относящиеся к раскрытию, целостности или отказу служб вычислительной системы.

Угроза раскрытия заключается том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемая от одной системы к другой. Иногда в связи с угрозой раскрытия используется термин «утечка».

Угроза целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда взломщики преднамеренно изменяют информацию, говорят, что целостность этой информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка. Санкционированными изменениями являются те, которые сделаны определенными лицами с обоснованной целью (таким изменением является периодическая запланированная коррекция некоторой базы данных).

Угроза отказа служб возникает всякий раз, когда в результате преднамеренных действий, предпринятых другим пользователем, умышленно блокируется доступ к некоторому ресурсу вычислительной системы. То есть, если один пользователь запрашивает доступ к службе, а другой предпринимает что-либо для недопущения этого доступа, мы говорим, что имеет место отказ службы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Политика безопасности подразумевает множество условий, при которых пользователи системы могут получить доступ к информации и ресурсам. Таким образом, политика безопасности определяет множество требований, которые должны быть выполнены в конкретной реализации системы. Очевидно, для проведения желаемой политики безопасности в системе должны присутствовать соответствующие механизмы. В большинстве случаев механизмы безопасности содержат некоторые автоматизированные компоненты, зачастую являющиеся частью базового вычислительного окружения (операционной системы), с соответствующим множеством процедур пользователя и администратора.

Одним из важнейших аспектов проблемы информационной безопасности компьютерных систем является противодействие разрушающим программным средствам. Рассмотрим подходы к решению этой задачи:

- создание специальных программных средств, предназначенных исключительно для поиска и ликвидации конкретных видов разрушающих программных средств (антивирусные программы);

- проектирование вычислительных систем, архитектура и модель безопасности которых не допускает существование разрушающих программных средств, либо ограничивает область их активности и возможный ущерб;

- создание и применение методов и средств анализа программного обеспечения на предмет наличия в них угроз информационной безопасности вычислительных систем и элементов разрушающих программных средств.

Процедуру анализа программного обеспечения на предмет наличия в них угроз информационной безопасности вычислительной системы называются анализом безопасности программного обеспечения. Данный подход требует разработки соответствующих теоретических моделей программ, вычислительных систем и разрушающих программных средств, создания методов анализа безопасности и методик их применения.

Модель реализации угроз информационной безопасности изображена на рисунке 1.4



Рисунок 1.4 Модель реализации угроз информационной безопасности

**1.3.7 Анализ и классификация удаленных атак в ЛВС**

Основой любого анализа безопасности компьютерных систем является знание основных угроз, присущих им. Для подобного анализа представляется необходимым выделение из огромного числа видов угроз обобщенных типов угроз, их описание и классификация.

Классификация удаленных атак на ЛВС.

Удаленные атаки можно классифицировать по следующим признакам:

1. По характеру воздействия:

* активные,
* пассивные.

Под активным воздействием на сетевую систему понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации сети, нарушение работы сети) и нарушающее политику безопасности, принятую в системе. Практически все типы удаленных атак являются активными воздействиями.

Пассивным воздействием на сетевую систему называется воздействие, которое не оказывает непосредственного влияния на работу сети, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу сети приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Единственным примером пассивного типового удаленного воздействия служит прослушивание канала в сети.

2. По цели воздействия:

* перехват информации,
* искажение информации.

Основная цель практически любой атаки – получить несанкционированный доступ к информации. Существуют две принципиальных возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Примером перехвата информации может служить прослушивание канала в сети. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения.

Возможность к искажению информации означает полный контроль над информационном потоком. Информацию можно не только прочитать, как в случае перехвата, а иметь возможность ее модификации.

3. По условию начала осуществления воздействия.

Защита информации включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Применительно к персоналу, работающему с информационными системами, используются операционные регуляторы, действующие на окружение компьютерных комплексов. Имеются в виду способы подбора персонала, его обучения, обеспечения дисциплины. Сюда же относятся меры по физической защите помещений и оборудования и некоторые другие.

Перед принятием каких-либо защитных мер необходимо произвести анализ угроз.

Наиболее распространенные угрозы

Самыми частыми и самыми опасными, с точки зрения размера ущерба, являются непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки являются угрозами: неправильно введенные данные, ошибка в программе, а иногда они создают слабости, которыми могут воспользоваться злоумышленники - таковы обычно ошибки администрирования. Согласно статистики 65% потерь - следствие непреднамеренных ошибок. Пожары и наводнения можно считать пустяками по сравнению с безграмотностью и расхлябанностью. Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация и строгий контроль за правильностью совершаемых действий.

На втором месте по размерам ущерба располагаются кражи и подлоги. Подлинный ущерб от краж и подлогов намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты. В большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами. Это еще раз свидетельствует о том, что внутренняя угроза гораздо опаснее внешней.

Весьма опасны так называемые обиженные сотрудники - нынешние и бывшие. Как правило, их действиями руководит желание нанести вред организации-обидчику (повредить оборудование; встроить логическую бомбу; оторая со временем разрушит программы и/или данные; ввести неверные данные; удалить данные; изменить данные).

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны вредить весьма эффективно. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа к информационным ресурсам аннулировались.

Угрозы, исходящие от окружающей среды, отличаются большим разнообразием. В первую очередь, следует выделить нарушения инфраструктуры - аварии электропитания, временное отсутствие связи, перебои с водоснабжением, гражданские беспорядки. Опасны стихийные бедствия и события, воспринимаемые как стихийные бедствия - пожары, наводнения, землетрясения, ураганы. По статистическим данным, на долю огня, воды и аналогичных "врагов", в том числе - низкое качество электропитания, приходится 13% потерь, нанесенных информационным системам.

Таковы основные угрозы, на которые приходится основная доля урона, наносимого информационным системам.

**2. Защита информации в локальных вычислительных сетях ЗАО завода ЛИТ**

**2.1 Анализ системы защиты информации в ЛВС ЗАО завода ЛИТ**

Защиту информации, локальной сети и ЭВМ на заводе от прямых угроз можно разбить на две категории:

1. Защита от стихийных бедствий.
2. Защиты от злоумышленников.

Наиболее опасным из стихийных бедствий можно считать пожар. Соблюдение элементарных пожарных норм позволяет решить эту проблему. Наиболее важен и интересен второй пункт.

Для того, чтобы защитить компьютеры от злоумышленников, а следовательно защитить информацию, необходимо ограничить непосредственный доступ к вычислительной системе в целом. Для этого следует организовать охрану вычислительного комплекса, расположенного на территории завода. Можно выделить следующие виды охранных мер:

1. охрана границ территории (некоторой зоны, окружающей завод);
2. охрана самого здания или некоторого пространства вокруг него (создание контролируемой зоны вокруг подразделения АСУ);
3. охрана входов в отделение АСУ;
4. охрана критических зон.

Пропуск на территорию завода осуществляется через контрольный пропускной пункт, охраняемый специальным подразделением охраны в строго определенном порядке по пропускам.

Все подразделения, где используются ЭВМ имеют прочные надежные стены из кирпича или железобетона, толщиной не менее 30 см.

Входы в здания имеют надежные двери, которые постоянно закрыты на кодовые замки, коды которых знают лишь ограниченный круг персонала подразделения. Некоторые входы контролируются посредством личного опознавания входящего охраной или с использованием ключей (специальных карточек). Окна на первых этажах и у лестничных клеток, козырьков имеют металлические решетки.

**2.1.1 Отдел АСУ: название, назначение и задачи решаемые отделом**

Отдел АСУ (Автоматизированные системы управления) является самостоятельным структурным подразделением ЗАО завода ЛИТ.

Задачами данного отдела являются:

* Выполнение работ по разработке, подготовке и отладке компьютерных программ для решения экономических и других задач;
* Обеспечение бесперебойного функционирования компьютерной техники;
* Поддержка функционирования IT – структуры предприятия;
* Ремонт и обслуживание компьютерной техники и периферийного оборудования.

Бюро АСУ руководствуется в своей деятельности:

* Действующим законодательством РФ и другими нормативными актами;
* Приказами и распоряжениями по заводу;
* Положениями и инструкциями, действующими на заводе;
* Инструкцией (№ 104) по охране труда для операторов и пользователей ПЭВМ и работников, занятых эксплуатацией ПЭВМ и ВДТ;
* Ежемесячными планами работы бюро АСУ.

**2.1.2 Структура отдела АСУ ЗАО завода ЛИТ**

Сотрудниками данного отдела являются 6 человек:

* Начальник бюро АСУ;
* Системный администратор;
* 2 Инженера – электронщика;
* Администратор БД;
* Программист.

Структурная схема отдела АСУ представлена на рисунке 2.1.

Начальник бюро АСУ руководит отделом, дает распоряжения.

Системный администратор является организатором и исполнителем работ по выявлению и устранению сбоев в работе ЛВС и сетевых сервисов. Основной задачей Администратора сети является обеспечение бесперебойного функционирования ЛВС и сетевых сервисов.

Администратор БД занимается созданием структуры и минимизацией таблиц в базах данных их внедрением, обслуживанием и сохранением данных.

Программист составляет программу по готовому техническому заданию, а при отсутствии такового составляет его. Занимается написанием, отладкой, внедрением и обслуживанием программ.

Инженеры – электронщики занимаются ремонтом компьютерной техники и периферийного оборудования.

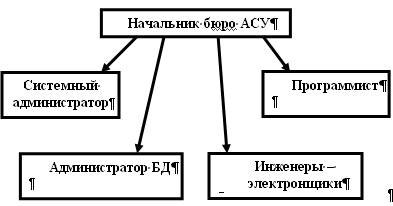


Рисунок 2.1. Структурная схема отдела и его подразделений

Взаимосвязь бюро АСУ с другими подразделениями завода:

* со всеми подразделениями завода – представляет сопровождение действующих задач, внесение изменений по мере необходимости
* с социально-правовым отделом – представляет проекты графиков ежегодных отпусков, характеристик, листов временной нетрудоспособности, сведения по кадровым вопросам, заявки на потребность в кадрах, получает приказы по кадровым вопросам, утвержденные графики ежегодных отпусков
* с отделом планирования производства и организации труда – представляет предложения по совершенствованию организации труда, систем оплаты труда и материального стимулирования, предложения по проекту штатного расписания, получает штатное расписание, положение о премировании, график.
* со службой логистики перевозок – представляет заявки на подачу автотранспорта с указанием рода груза и количества.

**2.2 Программное обеспечение отдела АСУ ЗАО завода ЛИТ**

**2.2.1 Особенности работы отдела АСУ в конкретной операционной системе**

Отдел АСУ работает в 2-х операционных системах:

* Linux;
* Windows XP Professional editions.

Linux – общее название Unix-подобных операционных систем на основе одноимённого ядра и собранных для него библиотек и системных программ, разработанных в рамках проекта GNU. Linux работает на PC-совместимых системах семейства Intel x86, AMD64, PowerPC, IBM, и многих других.

Семейство ОС на базе ядра Linux – третье по популярности в мире на рынке настольных компьютеров. На рынке веб-серверов доля Linux порядка 50 %. Linux используется на 91 % самых мощных суперкомпьютеров планеты.

Основные области применения ОС Linux:

* Сервера, требующие высоких показателей uptime.
* Компьютеры нестандартной архитектуры (суперкомпьютеры) – из-за возможности быстрой адаптации ядра ОС и большого количества ПО.
* Системы военного назначения (МСВС РФ) – по соображениям безопасности.
* Компьютеры, встроенные в различные устройства (банкоматы, терминалы оплаты, мобильные телефоны) – из-за широких возможностей по конфигурированию Linux под задачу, выполняемую устройством, а также отсутствия платы за каждое устройство.
* Массовые специализированные рабочие места (нетбуки) – из-за отсутствия платы за каждое рабочее место.

Windows XP (кодовое название при разработке — Whistler; внутренняя версия — Windows NT 5.1) — операционная система семейства Windows NT корпорации Microsoft. Она была выпущена 25 октября 2001 года и является развитием Windows 2000 Professional. Название XP происходит от англ. experience (опыт). Название вошло в практику использования, как профессиональная версия.

Системные требования ОС Windows XP Professional указаны в таблице 2.2:

Таблица 2.2

|  |  |  |
| --- | --- | --- |
|  | Декларируемые как минимальные | Рекомендуемые |
| Процессор | 233 MHz | 300 MHz или выше |
| Оперативная память | 64 Мб RAM (могут быть ограничены некоторые возможности) | 128 Мб RAM или выше |
| Видеоадаптер и монитор | VGA (640 x 480) | Super VGA (800 x 600) или большее разрешение |
| Свободное место на HDD | 1.5 Гб | 1.5 Гб или выше |
| Оптические накопители | CD-ROM (требуется для установки) | CD-ROM или DVD-ROM |
| Устройства взаимодействия с пользователем | клавиатура | клавиатура и мышь |
| Другие устройства | Звуковая карта, колонки и/или наушники | Звуковая карта, колонки и/или наушники |

**2.2.2 Прикладное и специальное программное обеспечение**

К прикладному программному обеспечению относятся следующие программы:

* + Браузер Mozilla Firefox
  + Офис Open Office

Mozilla Firefox – свободно распространяемый браузер. Второй по популярности браузер в мире и первый среди свободного ПО – в начале апреля 2010 года его рыночная доля составила 31,52 %, в отдельных странах – до 45 %. В браузере присутствуют вкладочный интерфейс, проверка орфографии, поиск по мере набора, «живые закладки», менеджер закачек, поисковая система. Новые функции можно добавлять при помощи расширений. Firefox выпускается для Microsoft Windows и множества других операционных систем.

OpenOffice.org (OOo, OO.o) – свободный пакет офисных приложений, разработанный с целью предоставить альтернативу Microsoft Office как на уровне форматов, так и на уровне интерфейса пользователя. Одним из первых стал поддерживать новый открытый формат OpenDocument (ISO/IEC 26300). Отлично работает на платформе Microsoft Windows и других платформах. Офисный пакет OpenOffice.org может свободно устанавливаться и использоваться в школах, офисах, вузах, домашних компьютерах, государственных, бюджетных и коммерческих организациях и учреждениях России и стран СНГ согласно GNU General Public License.

К специальному программному обеспечению относятся:

* + Программы выписки доверенностей
  + 1С бухгалтерия
  + Программы выписки командировок
  + Антивирусная программа Касперского 6.0

**2.2.3 Защита информации в ЛВС программными средствами**

Для эффективной защиты информации обрабатываемой, хранящейся и циркулирующей в локальной сети завода отделом АСУ используются следующие программы:

* Программы Firewall
* Антивирусные средства (Антивирус Касперского (6.0.4.1212)
* Программы антиспама

Firewall – межсетевой экран или сетевой экран – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача – не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Антивирус Касперского – антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS.

### Базовая защита Антивируса Касперского:

* Защита от вирусов, троянских программ и червей;
* Защита от шпионских и рекламных программ;
* Проверка файлов в автоматическом режиме и по требованию;
* Проверка почтовых сообщений (для любых почтовых клиентов);
* Проверка интернет-трафика (для любых интернет-браузеров);
* Защита интернет-пейджеров (ICQ, MSN);
* Проактивная защита от новых вредоносных программ;
* Проверка Java- и Visual Basic-скриптов.

### Предотвращение угроз Антивирусом Касперского:

* Поиск уязвимостей в ОС и установленном ПО;
* Анализ и устранение уязвимостей в браузере Mozilla Firefox;
* Блокирование ссылок на зараженные сайты;
* Распознавание вирусов по способу их упаковки;
* Глобальный мониторинг угроз (Kaspersky Security Network).

### Защита конфиденциальных данных

* Блокирование ссылок на фишинговые сайты;
* Защита от всех видов кейлоггеров.

**2.3 Компьютерная телекоммуникационная сеть отдела**

**2.3.1 Структура сети, топология подсети**

В отделе АСУ звездообразная топология подсети. Все компьютеры подключены к одному коммутатору (свитчу), который оптоволоконным кабелем соединен со шлюзом.

Звезда́ (Рисунок 2.1) – базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу, образуя физический сегмент сети. В качестве центрального узла используются концентраторы и коммутаторы. Сегменты сети функционируют в составе сложной сетевой топологии («дерева»). Весь обмен информацией идет исключительно через центральный узел, на который таким способом ложится очень большая нагрузка, потому ничем другим, кроме сети, оно заниматься не может. Никакие конфликты в сети с топологией звезда в принципе невозможны, потому что управление полностью централизовано.

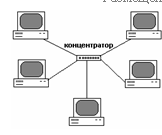


Рисунок 2.1. Топология «Звезда»

**2.3.2 Основные технические характеристики сетевого оборудования**

Оборудование, используемое в ЛВС ЗАО завода ЛИТ:

* Коммутаторы (Рисунок 2.2);
* Концентратор(Рисунок 2.3);
* Маршрутизатор(Рисунок 2.4);
* Оптоволоконный кабель(Рисунок 2.5);
* UTP- и SFTP- кабели(Рисунок 2.6).

Основными целью коммутаторов и концентраторов является соединение компьютеров в локальную сеть.



Рисунок 2.2. Коммутатор Cisco SRW2024-EU

Технические характеристики:

* Тип устройства: коммутатор для рабочей группы
* Корпус: монтируемый в шкаф-стойку корпус
* Тип сети: Gigabit Ethernet, Fast Ethernet, Ethernet
* Кол-во базовых портов: 24
* MDI: 24 автоматически переключающиxся порта
* Индикаторы:
  + активное соединение
  + электропитание
* Поддерживаемые стандарты:
  + IEEE 802.1p (Prioritizing)
  + IEEE 802.1Q (VLAN)
  + IEEE 802.1X
  + IEEE 802.3 (Ethernet)
  + IEEE 802.3ab (TP Gigabit Ethernet)
  + IEEE 802.3af (power over ethernet)
  + IEEE 802.3u (Fast Ethernet)
  + IEEE 802.3x (Flow Control)
* Сертификаты: CE Mark, EN 60950, UL-1950
* Интерфейсы:
  + 24 x Ethernet 10/100/1000BaseT • RJ-45 (auto MDI-II/MDI-X port)
  + 2 x GBIC • Mini-GBIC
* Электропитание:
  + внутренний блок питания
  + 100 / 240В (перемен. ток)
* Габариты (ВысотаХ ШиринаХ Глубина), Вес: 43 x 4.5 x 35 см, 3.4 кг

Концентратор Cisco Systems серии FastHub 200 предлагают самое дешевое управляемое решение для концентраторов 100BaseT, предназначенных малым рабочим группам и группам серверов. Эти отдельно стоящие концентраторы сочетают в рамках весьма недорогого решения производительность в 100 Мб/сек и интегрированные возможности управления при помощи технологии Cisco IOSO.

У маршрутизаторов цель подобна коммутаторам и концентраторам, но отличается тем, что коммутаторы и концентраторы – это инструменты локальных сетей, а маршрутизатор – глобальных. Задачей его является направление пакета в определенную подсеть.

Маршрутиза́тор или роутер – сетевое устройство, на основании информации о топологии сети и определённых правил принимающее решения о пересылке пакетов сетевого уровня (уровень 3 модели OSI) между различными сегментами сети. Маршрутизатор использует адрес получателя, указанный в пакетах данных, и определяет по таблице маршрутизации путь, по которому следует передать данные. Если в таблице маршрутизации для адреса нет описанного маршрута, пакет отбрасывается.

Оптоволоконный кабель для передачи в нем двоичных данных применяют световые импульсы. В силу того, что оптоволоконный кабель использует свет (фотоны) вместо электричества, почти все проблемы, присущие медному кабелю, такие как электромагнитные помехи, перекрестные помехи (переходное затухание) и необходимость заземления, полностью устраняются. Вдобавок, чрезвычайно уменьшается погонное затухание, позволяя протягивать оптоволоконные связи без регенерации сигналов на много большие дистанции, достигающие 120 км.

Оптоволоконный кабель идеально подходит для создания сетевых магистралей, и в особенности для соединения между зданиями, так как он нечувствителен к влажности и другим внешним условиям. Также он обеспечивает повышенную по сравнению с медью секретность передаваемых данных, поскольку не испускает электромагнитного излучения, и к нему практически невозможно подключиться без разрушения целостности.

Оптическое волокно — чрезвычайно тонкий стеклянный цилиндр, называемый жилой (core), покрытый слоем стекла, называемого оболочкой, с иным, чем у жилы, коэффициентом преломления. Иногда оптоволокно производят из пластика. Пластик проще в использовании, но он передает световые импульсы на меньшие расстояния по сравнению со стеклянным оптоволокном. Каждое стеклянное оптоволокно передает сигналы только в одном направлении, поэтому кабель состоит из двух волокон с отдельными коннекторами. Одно из них служит для передачи, а другое — для приема. Жесткость волокон увеличена покрытием из пластика, а прочность – волокнами из кевлара.

Вита́я па́ра – вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой. Свивание проводников производится с целью повышения степени связи между собой проводников одной пары (электромагнитная помеха одинаково влияет на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов. Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом.

В ЛВС применяется два вида кабеля:

* незащищенная витая пара (UTP — Unshielded twisted pair) — отсутствует защитный экран вокруг отдельной пары;
* фольгированная экранированная витая пара (S/FTP — Screened Foiled twisted pair) — внешний экран из медной оплетки и каждая пара в фольгированной оплетке.

**2.3.3 Управление доступом к информации в локальной сети**

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи, процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами).

Речь идет о логическом управлении доступом, который реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и их доступность путем запрещения обслуживания неавторизованных пользователей.

Контроль прав доступа производится разными компонентами программной среды - ядром операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением и т.д.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

* Идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера) – подобные идентификаторы являются основой добровольного управления доступом;
* Атрибуты субъекта (метка безопасности, группа пользователя); метки безопасности - основа принудительного управления доступом;
* Место действия (системная консоль, надежный узел сети);
* Время действия (большинство действий целесообразно разрешать только в рабочее время);
* Внутренние ограничения сервиса (число пользователей согласно лицензии на программный продукт).

Если есть необходимость предоставить одинаковые права доступа некоторой группе сотрудников, лучше пользоваться не специализированными, а групповыми входами. В этом случае каждый пользователь входа имеет как бы отдельный «подвход» с собственным идентификатором и паролем, однако всем абонентам группового входа предоставляются равные права при работе с сетевой системой.

Каждый сотрудник ЗАО завода ЛИТ, допущенный к ЭВМ имеет свой личный идентификатор (логин) и пароль, который он использует для входа в систему обработки информации и доступа к данным, определенным его служебной деятельностью и функциональными обязанностями. Для повышения безопасности и защиты информации можно дополнительно разграничить доступ к данным в ЛВС по IP-адресам и MAC-адресам.

IP-адрес – сетевой адрес узла в компьютерной сети, построенной по протоколу IP, является уникальным адресом в как в локальной, так и в глобальной сети. MAC-адрес – это уникальный идентификатор, сопоставляемый с различными типами оборудования для компьютерных сетей.

Пользовательские входы и пароли – это первая линия обороны системы защиты. После того как пользователь получил доступ к сети, введя правильный идентификатор (логин) и пароль, он переходит ко второй линии, предлагаемой системой защиты: сеть определяет привилегии, которые имеет данный пользователь. Все пользователи сети были задуманы как равные сотрудники одной системы. Но некоторые из них имеют определенные дополнительные права (привилегии) – они отличают таких пользователей от остальных сотрудников.

Обычно права доступа распространяются на целые каталоги, хотя возможно установить и специальный доступ к некоторым отдельным файлам или группам файлов. При этом используется специализированное имя файла. В большинстве сетей права доступа устанавливаются на весь каталог целиком и распространяются на все подкаталоги. Конечно если только на какие-нибудь из подкаталогов, не наложены специальные права. Не обязательно, чтобы каждый пользователь имел доступ ко всем серверам. В целях безопасности системы лучше, если пользователю будет предоставлен доступ только к тем серверным компьютерам, которые нужны ему непосредственно для работы.

Во многих сетях администраторский вход открывается автоматически при установке системы. Идентификатор пользователя и пароль, используемые в этом входе, должны быть отражены в сетевой документации. Они одинаковы для любой системы данного типа. В целях безопасности и защиты информации от злоумышленников необходимо сменить пароль на таком входе, иначе любой пользователь, знающий стандартные идентификатор и пароль, устанавливаемые системой на администраторском входе, сможет работать в сети с неограниченными возможностями доступа к любым компонентам системы.

Рассмотренные способы защиты, предоставляются сетевым программным обеспечением. Но существует много других возможностей защитить сетевую информацию от постороннего вторжения. Вот несколько вариантов подобной защиты. Все компьютеры сети должны быть расположены в надежных и безопасных местах.

Если в сети установлен модем, позволяющий пользователю получать доступ к системе с удаленного компьютера, то посторонних вторжений можно ожидать и со стороны модема. В данном случае необходимо, чтобы каждый идентификатор пользователя был защищен паролем.

**2.4 Политика безопасности ЗАО завода ЛИТ при его информатизации**

**2.4.1 Концепция безопасности ЛВС ЗАО завода ЛИТ**

Рассмотрим локальную сеть, которой владеет ЗАО завод ЛИТ (Приложение 1), и ассоциированную с ней политику безопасности среднего уровня.

Информация, циркулирующая в рамках локальной сети, является критически важной. Локальная сеть позволяет пользователям разделять программы и данные, что увеличивает риск. Следовательно, каждый из компьютеров, входящих в сеть, нуждается в более сильной защите.

На заводе должна быть разработана инструкция по обеспечению безопасности информации преследующая две главные цели:

* продемонстрировать сотрудникам важность защиты сетевой среды, описать их роль в обеспечении безопасности,
* распределить конкретные обязанности по защите информации, циркулирующей в сети, равно как и самой сети.

В сферу действия данной политики попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть завода. Политика ориентирована также на людей, работающих с сетью, в том числе на пользователей, субподрядчиков и поставщиков.

Целью ЗАО завода ЛИТ является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности.

Частными целями являются:

* Обеспечение уровня безопасности, соответствующего нормативным документам.
* Следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности).
* Обеспечение безопасности в каждой функциональной области локальной сети.
* Обеспечение подотчетности всех действий пользователей с информацией и ресурсами.
* Обеспечение анализа регистрационной информации.
* Предоставление пользователям достаточной информации для сознательного поддержания режима безопасности.
* Выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети.
* Обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности.

Перечисленные группы людей отвечают за реализацию сформулированных ранее целей.

* Руководители подразделений отвечают за доведение положений политики безопасности до пользователей и за контакты с ними.
* Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.
* Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности.
* Пользователи обязаны работать с локальной сетью в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.

Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения со стороны персонала должны рассматриваться руководством для принятия мер вплоть до увольнения.

**2.4.2 Обеспечение безопасности при групповой обработке информации в подразделениях и отделах ЗАО завода ЛИТ**

Для обеспечения защиты информации в институте должны быть разработаны и введены в действие инструкции для всех категории персонала, в которых должны найти отражение следующие задачи для каждой категории:

Руководители подразделений обязаны:

* Постоянно держать в поле зрения вопросы безопасности. Следить за тем, чтобы то же делали их подчиненные.
* Проводить анализ рисков, выявляя активы, требующие защиты, и уязвимые места систем, оценивая размер возможного ущерба от нарушения режима безопасности и выбирая эффективные средства защиты.
* Организовать обучение персонала мерам безопасности. Обратить особое внимание на вопросы, связанные с антивирусным контролем.
* Информировать администраторов локальной сети и администраторов сервисов об изменении статуса каждого из подчиненных (переход на другую работу, увольнение и т.п.).
* Обеспечить, чтобы каждый компьютер в их подразделениях имел хозяина или системного администратора, отвечающего за безопасность и имеющего достаточную квалификацию для выполнения этой роли.

Администраторы локальной сети обязаны:

* Информировать руководство об эффективности существующей политики безопасности и о технических мерах, которые могут улучшить защиту.
* Обеспечить защиту оборудования локальной сети, в том числе интерфейсов с другими сетями.
* Оперативно и эффективно реагировать на события, таящие угрозу. Информировать администраторов сервисов о попытках нарушения защиты.
* Оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания.
* Использовать проверенные средства аудита и обнаружения подозрительных ситуаций.
* Ежедневно анализировать регистрационную информацию, относящуюся к сети в целом и к файловым серверам в особенности.
* Следить за новинками в области информационной безопасности, сообщать о них пользователям и руководству.
* Не злоупотреблять данными им большими полномочиями. Пользователи имеют право на тайну.
* Разработать процедуры и подготовить инструкции для защиты локальной сети от зловредного программного обеспечения.
* Оказывать помощь в обнаружении и ликвидации зловредного кода.
* Регулярно выполнять резервное копирование информации, хранящейся на файловых серверах.
* Выполнять все изменения сетевой аппаратно-программной конфигурации.
* Гарантировать обязательность процедуры идентификации и аутентификации для доступа к сетевым ресурсам.
* Выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм.
* Периодически производить проверку надежности защиты локальной сети. Не допускать получения привилегий неавторизованными пользователями.

Администраторы сервисов обязаны:

* Управлять правами доступа пользователей к обслуживаемым объектам. Оперативно и эффективно реагировать на события, таящие угрозу.
* Информировать администраторов локальной сети о попытках нарушения защиты.
* Оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания.
* Регулярно выполнять резервное копирование информации, обрабатываемой сервисом.
* Выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм.
* Ежедневно анализировать регистрационную информацию, относящуюся к сервису.
* Регулярно контролировать сервис на предмет зловредного программного обеспечения.
* Периодически производить проверку надежности защиты сервиса. Не допускать получения привилегий неавторизованными пользователями.

Пользователи обязаны:

* Знать и соблюдать законы, правила, принятые в организации, политику безопасности, процедуры безопасности.
* Использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации.
* Использовать механизм защиты файлов и должным образом задавать права доступа.
* Выбирать хорошие пароли, регулярно менять их. Не записывать пароли на бумаге, не сообщать их другим лицам.
* Помогать другим пользователям соблюдать меры безопасности. Указывать им на проявленные упущения.
* Информировать администраторов или руководство о нарушениях безопасности и иных подозрительных ситуациях.
* Не использовать слабости в защите сервисов и локальной сети в целом.
* Не совершать неавторизованной работы с данными, не создавать помех другим пользователям.
* Всегда сообщать корректную идентификационную и аутентификационную информацию, не пытаться работать от имени других пользователей.
* Обеспечивать резервное копирование информации с жесткого диска своего компьютера.
* Знать принципы работы зловредного программного обеспечения, пути его проникновения и распространения, слабости, которые при этом могут использоваться.
* Знать и соблюдать процедуры для предупреждения проникновения зловредного кода, для его обнаружения и уничтожения.
* Знать слабости, которые используются для неавторизованного доступа.
* Знать способы выявления ненормального поведения конкретных систем, последовательность дальнейших действий, точки контакта с ответственными лицами.
* Знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

Реакция на нарушения режима безопасности.

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

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

На заводе должен быть человек, доступный 24 часа в сутки (лично, по телефону или электронной почте), отвечающий за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности.

Для недопущения повторных нарушений необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику. Каковы источники зловредного кода? Какие пользователи имеют обыкновение выбирать слабые пароли? На подобные вопросы и должны дать ответ результаты анализа.

Очень важными являются программно-технические меры, которые образуют последний и самый важный рубеж информационной защиты. Основную часть ущерба наносят действия легальных пользователей, по отношению к которым операционные регуляторы не могут дать решающего эффекта. Главные враги - некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Физическую защиту, целесообразно необходимости, поручить интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещения сотрудников и по пространству предприятия, и по информационному пространству. Это вторая причина, объясняющая важность программно-технических мер.

В случае умышленного нарушения информационной безопасности выражающуюся в утере, хищении, уничтожении, модификации информации, внесении программ-вирусов, осуществлении действий, в результате которых наносится ущерб информационной целостности организации и раскрытие конфиденциальной информации сотрудники данного учреждения согласно Закону привлекаются к ответственности в зависимости от нанесенного ущерба от административной ответственности до лишения свободы сроком до 10 лет.

**3. Экономическая часть**

Отдел АСУ ЗАО завода ЛИТ укомплектован современным сетевым оборудованием и оргтехникой необходимыми для устойчивой стабильной работы всех подразделений завода в целом, финансово-экономической и административно-хозяйственной деятельности. Защита информации отдела АСУ от злоумышленников и разрушающих программных средств находится на высоком уровне и практически не имеет прорех. Поэтому задачей моей дипломной работы является расчет минимизации затрат на обслуживание ЛВС завода и ее защиту от разрушающих программных средств.

Расчет затрат на обслуживание локальной сети

Таблица 3.1. Расчет затрат на обслуживание локальной сети и плановый ремонт рабочих станций

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование оргтехники | Количество | Цена за ед. руб. | Сумма руб. |
| Обеспечение антивирусными программами | 1 | 1200 | 1 200 |
| Плановый ремонт рабочей станции  (за 1 месяц) | 4 | 250 | 1 000 |
| Сопровождение кабельных линий связи | 3500 м | 2 | 7 000 |
| Сопровождение сети  (за 1 месяц) рабочей станции | 36 | 120 | 4 320 |
| Сопровождение сети  (за 1 месяц) сервера | 2 | 450 | 900 |
| ИТОГО: |  |  | 14 420 |

Таким образом общие затраты (Змаш) на плановый ремонт и обслуживание ЛВС и ее компонентов и программного обеспечения общей стоимостью: Змаш = 14 420 (рублей)

Расходы на оплату труда специалистов

Сумма затрат определяется как произведение временных затрат (t1+t2+t3+t4+t5+t6) и среднечасовой оплаты труда разработчика (ЗПсрч).

Затраты труда на подготовку описания задачи (t1) точной оценке не поддаются, так как это связано с творческим характером работы.

Принимаем t1 = 10 час

Все остальные виды затрат труда можно выразить через условное число клиентов сети.

Рассчитаем t2 - затраты труда на исследование и решение задачи.

t2 = Укс \* Куз / Ккл \* К

где:

Куз – коэффициент увеличения затрат труда, вследствие недостаточно точного описания задачи, последующих уточнений и дополнений

(Куз = 1,2...1,5; принимаем Куз ср = 1,35)

К – коэффициент, учитывающий квалификацию разработчика в зависимости от стажа работы:

|  |  |
| --- | --- |
| до 2-х лет | 0,8 |
| от 2-х до 3-х лет | 1,0 |
| от 3-х до 5-и лет | 1,1...1,2 |
| от 5-х до 7-и лет | 1,3...1,4 |
| свыше 7 лет | 1,5...1,6 |

Ккл - среднее количество клиентов сети, подлежащих настройке в один час (принимаем среднее значение клинетов Ккл = 5).

Укс = У \* Ксл \* (1 + Ккор)

где:

Укс – условное число клиентов сети,

У – предполагаемое число клиентов сети (принимаем У = 11),

Ксл – коэффициент сложности сетевой архитектуры

(Ксл=1,25-2,0; принимаем Ксл ср = 1,6),

Ккор – коэффициент коррекции сетевой архитектуры в ходе разработки

(Ккор = 0,05-1,0; принимаем Ккор ср = 0,5).

Укс = 10 \* 1,6 \* (1 + 0,5) = 24

Затраты труда на исследование решения задачи (t2):

t2 = Укс \* Куз \* К / Ккл

t2 = 24 \* 1,35 \* 1,2 / 5 = 7,776 (час)

Рассчитаем t3 - затраты труда на исследование сетевой архитектуры:

t3 = Укс \* К / (3…5)

t3 = 24 \* 1,2 / 4 = 7,2 (час)

Рассчитаем t4 - затраты труда на настройку сети – вычисления аналогичны предыдущим: принимаем t4 = 7,2 (час).

Рассчитаем t5 - затраты труда на отладку:

t5 = Укс \* К / (1…3)

t5 = 24 \* 1,2 / 2 = 14,4 (час)

Затраты на подготовку документации (t6):

t6 = t61 + t62, где:

t61 - затраты труда на подготовку документации в рукописи,

t62 – затраты на оформление документации.

t61 = Укс \* К / 14 = 24 \* 1,2 / 14 ≈ 2,057 (час)

t62 = 0.75 \* t61 = 0.75 \* 2,057 ≈ 1,543 (час)

итак:

t6 = 2,057 + 1,543 = 3,6 (час)

Таблица 3.2. Расчет временных и материальных затрат на установку, настройку и обслуживание сети

|  |  |  |
| --- | --- | --- |
| Виды затрат | Временные затраты, часы | Сумма затрат,  рубли |
| Затраты труда на подготовку и описание задачи (t1) | 10 | 506,00 |
| Затраты труда на исследование и решение задачи (t2) | 7,776 | 393,47 |
| Затраты труда на исследование сетевой архитектуры (t3) | 7,2 | 364,32 |
| Затраты труда на настройку (t4) | 7,2 | 364,32 |
| Затраты труда на отладку (t5) | 14,4 | 728,64 |
| Затраты на подготовку документации (t6) | 3,6 | 182,16 |
| ИТОГО (Зпр): | 50,176 | 2 538,91 |

Определение среднечасовой оплаты труда разработчика

ЗПсрч = ОК / ( Др \* Дпр )

где:

ОК – оклад разработчика (8 500 руб.),

Др – среднемесячное число рабочих дней (21 день),

Дпр – продолжительность рабочего дня (8 час).

ЗПсрч = 8500 / 21 \* 8 ≈ 50,60 (руб/час)

Общие затраты определяются как сумма общих затрат (Змаш) на приобретение недостающего для организации локальной информационной сети оборудования и программного обеспечения и затрат (Зпр) на установку, настройку и обслуживание сети.

Зобщ = Змаш + Зпр

Зобщ = 14 420 + 2 538,91 ≈ 16 959 (руб)

Таким образом из расчетов видно, что затраты для обслуживания ЛВС и ее компонентов ЗАО завода ЛИТ относительно небольшие. Вместе с тем положительный эффект от поддержания вычислительной системы в состоянии готовности предотвратить попытки хищения, модификации, либо подмены информации, значительный.

**Заключение**

В ближайшее время прогресс в области развития средств вычислительной техники, программного обеспечения и сетевых технологий даст толчок к развитию средств обеспечения безопасности, что потребует во многом пересмотреть существующую научную парадигму информационной безопасности. Основными положениями нового взгляда на безопасность должны являться:

1. исследование и анализ причин нарушения безопасности компьютерных систем;
2. разработка эффективных моделей безопасности, адекватных современной степени развития программных и аппаратных средств, а также возможностям злоумышленников и разрушающих программных средств;
3. создание методов и средств корректного внедрения моделей безопасности в существующие вычислительные системы, с возможностью гибкого управления, безопасностью в зависимости от выдвигаемых требований, допустимого риска и расхода ресурсов;
4. необходимость разработки средств анализа безопасности компьютерных систем с помощью осуществления тестовых воздействий (атак).

В условиях современной суверенизации государств и субъектов Российской Федерации, продолжающихся военных конфликтов, попыток территориальных, экономических и др. притязаний государств друг к другу, растущей угрозы терроризма в отношении отдельных граждан и государственных структур особенно остро встали проблемы надежной защиты информации в особые периоды управления важными государственными объектами, включая вычислительные системы. Это требует дальнейшего развития теории и практики обеспечения информационной безопасности в локальных сетях предприятий, повышения надежности применения современных систем обработки конфиденциальной информации в условиях обострения информационной войны (борьбы).

Широкая информатизация обществ, внедрение компьютерной технологии в сферу управления объектами государственного значения, стремительный рост темпов научно-технического прогресса наряду с положительными достижениями в информационных технологиях, создают реальные предпосылки для утечки конфиденциальной информации.

В дипломной работе, основной целью которой являлось разработка общих рекомендаций по защите информации в локальной сети отдела АСУ ЗАО завода ЛИТ и разработка пакета руководящих документов по обеспечению безопасности информации, получены следующие результаты:

1. Рассмотрены основные пути защиты от несанкционированного доступа к информации циркулирующей в системах обработки данных.
2. Произведена классификация способов и средств защиты информации.
3. Детально осуществлен анализ методов защиты информации в локальных вычислительных сетях.
4. Рассмотрены основные направления защиты информации в ЛВС.
5. Разработаны концепция безопасности локальных вычислительных сетей ЗАО завода ЛИТ и вопросы обеспечения безопасности при групповой обработке данных в службах и подразделениях завода.
6. Осуществлена выработка политики безопасности ЗАО завода ЛИТ.
7. Рассмотрен порядок управления доступом к информации в локальной сети с способы повышения безопасности и защиты данных в ЛВС.

В перспективе рассматривается возможность разработки общих рекомендаций по защите информации локальных сетей для подобных организаций, заводов, учреждений, и создание типовой инструкции по обеспечению безопасности информации в системах обработки данных.

**Список литературы**

1. Сбиба В.Ю, Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб: Питер, 2008.
2. Костров, Д.В. Информационная безопасность в рекомендациях, требованиях, стандартах. 2008.
3. Доля А.В. Внутренние угрозы ИБ в телекоммуникациях. 2007.
4. Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ.
5. Биячуев, Т.А. Безопасность корпоративных сетей. – СПб: ГУ ИТМО, 2004.
6. С.Вихорев, Р.Кобцев Как определить источники угроз. – Открытые системы. 2002.
7. Федеральный закон «Об информации, информатизации и защите информации».
8. Президент Российской Федерации. Указ от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».
9. В.Гайкович, А.Першин, Безопасность электронных банковских систем. - Москва, «Единая Европа», 2004.
10. В.Левин, Защита информации в информационно-вычислительных системах и сетях. - «Программирование», 2004.
11. Л.Хофман, «Современные методы защиты информации», - Москва, 2005.
12. П.Зегжда, «Теория и практика. Обеспечение информационной безопасности». - Москва, 2006.
13. Гостехкомиссия России. «Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения», - Москва, 1992.
14. Журналы "Защита информации" №№ 1-8 изд. КОНФИДЕНТ, С-Пб.

**Приложения**

Приложение 1. Структурная схема локальной сети ЗАО завод ЛИТ

