МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Белорусский государственный технологический университет»

Кафедра информационных технологий

Разработка политики информационной безопасности для подразделения автоуправления «Северстальресурс» в г. Варкуте

«Учёт ремонта и ТО автотранспорта»

Выполнила:

Студент 2 курса, 2 группы

Факультета ИТ

Глушнева Екатерина

Преподаватель:

Бракович Андрей Игоревич

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Минск 2015

Содержание

[Цели и задачи 2](#_Toc414364725)

[Введение 3](#_Toc414364726)

[Информационные ресурсы и пользователи системы 4](#_Toc414364727)

[Горизонтальная модель сети 6](#_Toc414364728)

[Общие меры безопасности 6](#_Toc414364729)

[Методы борьбы с утерей информации 11](#_Toc414364730)

[Вертикальная модель 12](#_Toc414364731)

[Заключение 18](#_Toc414364732)

[Список литературы 19](#_Toc414364733)

# **Цели и задачи**

Целью данной работы является разработка политики информационной безопасности для системы "Учёт ремонта и ТО автотранспорта", разрабатываемой для подразделения автоуправления "Северстальресурс" в г. Воркуте. Система создается для автоматизации процесса ведения, контроля, учета ремонта и технического обслуживания автотранспортного хозяйства. В данной работе будет: проведен анализ информации, циркулирующей в автоматизированной информационной системе, обоснован выбор класса защищенности для разрабатываемой системы, приведены примеры по предотвращению угроз, проведено горизонтальное проектирование, разработаны организационные мероприятия.

# **Введение**

Безопасность данных означает их конфиденциальность, целостность и доступность. Критерии безопасности данных могут быть определены следующим образом: конфиденциальность данных предполагает их доступность только для тех лиц, которые имеют на это соответствующие полномочия. Целостность информации предполагает ее неизменность в процессе передачи от отправителя к получателю. Под доступностью можно понимать гарантию того, что злоумышленник не сумеет помешать работе законных пользователей. В частности, в задачу обеспечения доступности входит исключение возможности атак, вызывающих отказ в обслуживании.

# **Информационные ресурсы и пользователи системы**

База данных создаваемой системы будет содержать данные конфиденциального характера, требующие жесткого контроля при доведении сведений до служб, которые имеют право на использование такой информации. В связи с этим информацию и систему в целом необходимо защитить от нанесения ущерба в результате сознательных либо случайных противоправных действий, такие как неправомерный доступ, уничтожение, модифицирование, блокирование, копирование, распространение, а также иные действия в отношении такой информации.

Ниже перечислены данные, которые будут использоваться в данной системе:

* Информация о наличии подвижного состава автотранспортного хозяйства;
* Факты выполненных работ по ремонту и техническому обслуживанию (ТО) автотранспорта;
* Показатели количества обслуживания за месяц и рабочий день;
* Простой автомобилей в ТО, ремонте и его ожидании;
* Планирование работ по ТО и ремонту подвижного состава.

К выделенным ресурсам в подсистеме "Учета ремонта и ТО автотранспорта" имеют доступ следующие группы пользователей:

**Начальник управления** и **главный инженер** (осуществляет общее руководство производством через непосредственно подчиненного ему начальника производства) имеют право только на просмотр всех данных, выпуск отчетов;

**Начальник производства** (руководит всеми работами по ТО и ремонту подвижного состава) имеет право на просмотр данных, выпуск отчетов;

**Диспетчер производства** (оперативное руководство производством работ на постах обслуживания и ремонта автотранспорта) имеет право на просмотр, редактирование и ввод данных;

**Инженер планового отдела**получает необходимые выходные данные системы;

**Системный администратор**, наделяет пользователей (группы пользователей) необходимыми для работы правами, имеет право на просмотр журнала событий (регистрационный журнал) системы, обязан делать резервные копии системы.

Рассмотрим правила разграничения доступа всех пользователей информационной системы (Таблица 1).

*Таблица 1 – правила разграничения доступа всех пользователей информационной системы.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Объект/  Субъект | Инф. о наличии  подвижного состава  автотранс-го х-ва | Факты выполненных  работ по ремонту  и ТО автотран-та | Показатели количества  обслуж-ия за месяц  и рабочий день | Простой автомо-билей  в ТО, ремонте и  его ожидании | Планирование работ  по ТО и ремонту  подвижного состава | Права и группы | Регистр-нный журнал |
| Начальник  управления, главный инженер | П | П | П | П | П | Н | Н |
| Нач.  производства | ПР | ПР | П | П | ПРДУ | Н | Н |
| Диспетчер производства | ПРДУ | ПРДУ | П | П | ПРДУ | Н | Н |
| Инженер планового отдела | П | П | П | П | ПРДУ | Н | Н |
| Сиситемный  админ. | Н | Н | Н | Н | Н | ПРДУ | ПУ |

В данной таблице приведены следующие условные обозначения:

Н – нет доступа; П – просмотр данных; Р – редактирование; Д – добавление данных; У – удаление данных;

# **Горизонтальная модель сети**

**Безопасность ИС** – это комплекс организационно-технических мероприятий. Для того, чтобы более эффективно обезопасить систему, необходимо произвести анализ и выявить, каким угрозам она должна противостоять. Это позволит детально рассмотреть наиболее уязвимые места и решить задачу защиты информации.

## Общие меры безопасности

Ни о какой информационной безопасности системы не может быть и речи, если не соблюдаются основные меры безопасности:

* Обеспечено бесперебойное электропитание сервера;
* Обеспечен нормальный климатический режим работы оборудования;
* В помещении сервера есть пожарная сигнализация, нет вероятности затопления (особенно касается первых и последних этажей);
* Все системные блоки опломбированы и закрыты;
* Особое внимание уделено инструктажу и контролю над уборщиками помещений, строителями и электриками. Эти лица могут по неосторожности нанести ущерб, который не сопоставимо больше умышленного вреда.

1. Физический доступ к основным ресурсам: серверы, активное оборудование

Даная угроза имеет место при бесконтрольном доступе к активному оборудованию. В результате чего злоумышленник может получить доступ к информации, произвести неправомерные действия по отношению к ней или иным образом навредить системе.

Для того, чтобы избежать данную ситуацию, необходимо обеспечить физическую охрану помещения, в котором установлено активное оборудование. Данное помещение должно закрываться на ключ, правом доступа к которому должны обладать лица, имеющие для этого соответствующие полномочия, а на случай экстренной необходимости разработана система оповещения ответственных лиц.

1. Физический доступ к персональному компьютеру пользователя

Персональное место пользователя так же является угрозой. Для усложнения доступа к системе необходимо использовать механизмы аутентификации (аутентификация Windows) и идентификации пользователя.

Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. Обычный способ идентификации - ввод имени пользователя при входе в систему. В свою очередь, система должна проверить подлинность личности пользователя, то есть что он является именно тем, за кого себя выдает. Стандартное средство проверки подлинности (аутентификации) – пароль. Администратор в свою очередь должен позаботиться об эффективности паролей, и соответствующей настройке контроллера домена (служба Active directory).

Иногда возникает такая ситуация, в которой компьютер временно находится без присмотра пользователя. В это время возникает опасность доступа к нему злоумышленника. Для того, чтобы предотвратить эту угрозу, необходимо перевести компьютер в режим ожидания с интервалом в 5 минут, т.е. включить хранитель экрана (screen-saver) c опцией ввода пароля при выходе из этого режима.

1. Прослушивание сетевого трафика

Реализовать такую атаку можно, используя сетевой анализатор. Для предотвращения этой угрозы необходимо использовать сетевые протоколы, поддерживающие защиту от НСД, а также конфиденциальность данных.

Защита от НСД подразумевает способность защитить данные от удаления или изменения, как случайного, так и преднамеренного; конфиденциальность – способ сокрытия информации, часто для этого используют кодирование. Для этих целей применяется технология Open SSL, которая обеспечивает кодирование канала связи между сервером и клиентом. Для гарантии целостности данных SSL использует МАС-коды (Message Authentication Code). При создании МАС - кода хеш-функция применяется к объединению самого сообщения и некоторых секретных данных, известных только доверенным сторонам (автору и получателю сообщения). Для проверки МАС - кода получатель вычисляет хеш, применяя хеш-функцию к данным и секретным данным. Если результат совпадает с МАС - кодом, прилагаемым к сообщению, можно считать, что данные не изменились.

Чтобы качественно защитить ресурсы следует задействовать такой механизм управления доступом, как ACL (Access Control List - списки управления доступом). Необходимо провести настройку "строгих" ACL на коммуникационном оборудовании и выполнить привязку MAC - адресов (Media Access Control) сетевых интерфейсов к коммутатору. При выполнении привязки к конкретному порту коммутатора доступ будут иметь только компьютеры с конкретными адресами сетевых интерфейсов. Устройства с другими сетевыми картами уже не смогут получить доступ к портам данного коммутатора.

В обязательном порядке должна осуществляться физическая охрана помещения, в котором расположено коммуникационное оборудование, предусматривающая контроль доступа в помещение посторонних лиц.

1. Подмена сетевых объектов

Данный вид угрозы можно описать следующим образом: злоумышленник выдает себя за другого пользователя или подменяет настоящей сервер подложным. Опасность подмены объектов обычно подразумевает подмену пользователя (получение доступа к аутентификационным данным, что также является разглашением информации), процесса (замена процесса подложным, это также опасность модификации данных). Реализация данной угрозы возможна при использовании ненадежных методов аутентификации.

Для решения этой проблемы необходимо произвести привязку MAC-адресов (Media Access Control) к конкретным портам активного оборудования. Используемые сетевые протоколы должны поддерживать защиту от НСД, а также конфиденциальность данных. Избежать подмены сервера поможет схема аутентификации, которая позволит клиентскому ПО выполнять проверку подлинности сервера. Подобная конфигурация клиентов должна быть определена корпоративной политикой предприятия.

1. Использование ненадежного программного обеспечения

Самое узкое место любой сети. Программное обеспечение серверов, рабочих станций, маршрутизаторов и т. д. написано людьми, следовательно, оно практически всегда содержит ошибки. Чем выше сложность подобного ПО, тем больше вероятность обнаружения в нем ошибок и уязвимостей. Большинство из них не представляет никакой опасности, некоторые же могут привести к трагическим последствиям, таким, как получение злоумышленником контроля над сервером, неработоспособность сервера, несанкционированное использование ресурсов (хранение ненужных данных на сервере, использование в качестве плацдарма для атаки и т.п.). Большинство таких уязвимостей устраняется с помощью пакетов обновлений, регулярно выпускаемых производителем ПО. Своевременная установка таких обновлений является необходимым условием безопасности сети.

1. Заражение вирусами

Вирусы представляют собой небольшие программы, при своем запуске дописывающие себя к другим программам, чтобы уже при их, запуске, производить новые, более опасные действия. В настоящее время компьютерный вирус распространяется либо через электронную почту, либо при переносе информации на съемных носителях. Для того чтобы избежать заражения вирусами, было решено установить антивирусную программу Symantec Antivirus. При получении какой- либо информации на электронном носителе эта машина используется как карантинная, т.е. именно на ней носитель проверяется на наличие вирусов и только после этого информацию можно предоставлять в локальную сеть. Так же необходимо убрать с клиентских компьютеров оборудование для считывания информации с электронных носителей (CD-дисководы, флоппи-диски), опечатать USB-порты.

1. Технические сбои оборудования

Работа кабельной системы состоящей из неэкранированной витой пары пятой категории и экранированной витой пары.

К отказам в работе сети приводят неисправности кабельной системы - это обрывы кабеля, короткое замыкание и физическое повреждение соединительных устройств. Большие неприятности могут доставлять электромагнитные наводки различного происхождения, например, от излучения бытовых электроприборов, стартеров ламп дневного света и т.п., поэтому используется сетевой кабель STP. Для определения таких характеристик как затухание и перекрестные наводки используются сканеры сетевого кабеля – приборы, предназначенные для установления не только причины, но и места повреждения кабельной системы. Сканер посылает в кабель серию коротких электрических импульсов и для каждого импульса измеряет время от подачи импульса до прихода отраженного сигнала и его фазу. По фазе отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). А по времени задержки – расстояние до места повреждения. Если кабель не поврежден, то отраженный импульс отсутствует.

Защита при отключении электропитания

При кратковременном отключении электроэнергии, признанной мерой защиты информации является в настоящее время установка источников бесперебойного питания. Подобные устройства, различающиеся по своим техническим и потребительским характеристикам, могут обеспечить питание всей сети или отдельного компьютера в течение промежутка времени, достаточного для восстановления работы электросети или записи информации на магнитные носители.

1. Человеческий фактор

Также разглашению или порчи информации может послужить человеческий фактор, а именно: уволенные или недовольные сотрудники, промышленный шпионаж, халатность, низкая квалификация.

Уволенные и недовольные сотрудники

Данная группа людей наиболее опасна, так как многие из работающих сотрудников могут иметь разрешенный доступ к конфиденциальной информации. Особенную группу составляют системные администраторы, зачатую недовольные своим материальным положением или несогласные с увольнением, они оставляют «черные ходы» для последующей возможности злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д.

Промышленный шпионаж

Это самая сложная категория. Если данные интересны кому-либо, то этот кто-то найдет способы достать их. Взлом хорошо защищенной сети – не самый простой вариант. Воспользовавшись вполне правомерным доступом к данным можно использовать их в своих личных целях.

Халатность

Самая обширная категория злоупотреблений: начиная с не установленных вовремя обновлений, измененных настроек «по умолчанию» и заканчивая несанкционированными модемами для выхода в Internet – в результате чего злоумышленники получают открытый доступ в хорошо защищенную сеть.

Низкая квалификация

Часто низкая квалификация не позволяет пользователю понять, с чем он имеет дело. Из-за этого даже хорошие программы защиты становятся настоящей морокой системного администратора, и он вынужден надеяться только на защиту периметра. Большинство пользователей не понимают реальной угрозы от запуска исполняемых файлов и скриптов и считают, что исполняемые файлы – только файлы с расширением «exe». Низкая квалификация не позволяет также определить, какая информация является действительно конфиденциальной, а какую можно разглашать. В крупных компаниях часто можно позвонить пользователю и, представившись администратором, узнать у него учетные данные для входа в сеть. Выход только один - обучение пользователей, создание соответствующих документов и повышение квалификации.

# **Методы борьбы с утерей информации**

Причины утери информации могут быть разные, будь то физическое повреждение либо непреднамеренное удаление.

Необходимо хранить всю информацию в двух экземплярах:

* На сервере баз данных для повышения надежности работы установлен RAID с чередованием дисков с записью четности на нескольких дисках;
* Создание резервных копий базы данных по расписанию. Необходимую частоту копирования нужно выяснить опытным путем;
* Тщательно расставляются права на все ресурсы, чтобы другие пользователи не могли модифицировать чужие файлы;
* Пользователи хранят ценную информацию в местах известных системному администратору. Если пользователь сохраняет информацию в любых других местах – вся ответственность за сохранность ложиться на пользователя;
* Системный администратор не должен удалять без ведома пользователя никакие «непонятные» папки с компьютера пользователя;
* Перед переустановкой операционной системы следует обязательно копировать все содержимое раздела (на который будет установлена система) на сервер, в другой радел или на CD/DVD.

# **Вертикальная модель**

В данном разделе представлены вопросы обеспечения безопасности согласно семи уровням модели OSI (Open Systems Interconnection Model – стандартная модель взаимодействия открытых систем). В соответствии с концептуальными положениями этой модели процесс информационного обмена в компьютерных сетях можно разделить на семь этапов в зависимости от того, каким образом, и между какими объектами происходит информационных обмен. Эти этапы называются уровнями модели взаимодействия систем.

Канальный уровень

Рекомендации, следование которым позволяет дополнительно защитить компьютерную сеть предприятия средствами канального уровня:

* Администратор должен вести инвентаризационную ведомость соответствия аппаратных и сетевых адресов всех узлов сети предприятия.
* Администратор должен выполнить настройку подсистем, необходимых для реализации разработанной политики защиты. В обязанности администратора входит также отключение неиспользуемых подсистем коммутатора.
* Администратор должен регулярно контролировать соответствие конфигураций коммутаторов разработанной политике защиты.
* Администратор должен вести мониторинг сетевой активности пользователей с целью выявления источников аномально высокого количества широковещательных запросов.
* Администратор должен регулярно выполнять мероприятия, связанные с мониторингом сети, осуществлением профилактических работ по настройке коммутаторов, а также созданием резервных копий конфигураций коммутаторов.
* Администратор должен обеспечить строгий контроль доступа в помещения, в которых расположены коммутаторы и рабочие станции, с которых разрешено управление коммутаторами.

Разбиение сети на различные виртуальные локальные сети (VLAN) необходимо для разграничения трафика. Виртуальной локальной сетью (Virtual LAN, VLAN) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов сети. Технология виртуальных локальных сетей создает мощные барьеры на пути нежелательного трафика из одной сети в другую и позволяет в сети, построенной на коммутато­рах, программным путем создать изолированные группы конечных узлов, между которыми от­сутствует любой трафик, в том числе широковещательный. Поэтому в УАТХ использовано 7 (семь) коммутаторов для эффективной эксплуатации и защиты локальной вычислительной сети (ЛВС).

Сетевой уровень

Использование в компьютерной сети протоколов сетевого уровня является необходимым условием для обеспечения взаимодействия между узлами сетей с различными канальными протоколами. Важный аспект использования протоколов сетевого уровня - это разграничение доступа к ресурсам внутри сети предприятия

Одной из задач администратора является защита адресного пространства сети от возможности его использования злоумышленником. Частично эту функцию выполняют механизмы маршрутизации, реализованные модулями протокола сетевого уровня. Т.е. осуществление обмена между узлами сетей с различными номерами невозможно без предварительной настройки локальных таблиц маршрутизации узлов этих сетей, либо без внесения изменений в конфигурацию маршрутизатора, осуществляющего обмен пакетами.

Сетевой уровень отвечает за маршрутизацию, т.е. за выбор оптимального пути и доставку пакета данных адресату. На маршрутизаторе происходит объединение VLAN в общую сеть.

Для достижения большего эффекта от такого разбиения сети необходимо использовать листы доступа (ACCESS – листы), которые бы запрещали сетям с конфиденциальной информацией маршрутизироваться в общую сеть, где циркулирует информация общего пользования. В результате использования таких листов доступа, конфиденциальная информация из одного виртуального сегмента никогда не попадёт в сегменты с общедоступной информацией.

Транспортный уровень

Использование свойств транспортных протоколов создает наиболее эффективную преграду деятельности злоумышленника. Здесь для защиты используются признаки, содержащиеся в заголовках сегментов транспортного протокола. Сегмент — блок данных с которыми работает транспортный протокол. Этими признаками являются тип транспортного протокола, номер порта и флаг синхронизации соединения.

Если средствами канального уровня можно защитить аппаратуру компьютерной сети, а протоколы сетевого уровня позволяют разграничить доступ к отдельным хостам и подсетям, то транспортный протокол используется как средство коммуникации сетевых приложений, функционирующих на платформе отдельных узлов. Любое сетевое приложение использует транспортный протокол для доставки обрабатываемых данных. Причем у каждого класса приложений имеется специфический номер транспортного порта. Это свойство может быть использовано злоумышленником для атаки на конкретный сетевой сервис или службу, либо администратором сети для защиты сетевых сервисов и служб.

Администратор формирует политику защиты сети средствами транспортного уровня в виде ведомости соответствия хостов, используемых ими сетевых адресов и доверенных приложений, функционирующих на платформах этих хостов. Формализованная запись содержит:

* Перечень узлов, их символьные имена;
* Соответствующие этим узлам сетевые адреса;
* Перечень используемых каждым узлом транспортных протоколов;
* Перечень сетевых приложений, функционирующих в каждом узле и соответствующие этим приложениям порты транспортного протокола;
* По каждому сетевому приложению необходимо установить, является ли оно потребителем или поставщиком ресурса, т.е. разрешено ли ему инициировать исходящие соединения или принимать входящие.

На данном уровне необходимо организовать списки доступа (ACCESS – листы) аналогичные листам доступа на сетевом уровне, однако, здесь можно указывать не адреса сетей, а адреса конкретных сервисов.

Уровень приложения

Это уровень сетевой модели, отвечающий за взаимодействие пользовательского приложения c сетью. На данном уровне необходимо осуществлять идентификацию (проверку наличия данного пользователя в списке active directory) и аутентификацию Windows (проверку достоверности имени и пароля с помощью сервера — контроллера домена) пользователей. При этом необходимо следить за тем, чтобы пользователи периодически осуществляли смену пароля, причём новый пароль должен значительно отличаться. Беспарольных пользователей в системе быть не должно.

Также на данном уровне необходимо произвести разделение прав доступа пользователей к информации на сервере.

Сюда так же можно отнести поддержку такого механизма как Аудит. Под Аудитом в классе 1Г требований по защите АИС понимается регистрация и учет:

* Входа/выхода субъектов в/из системы (узла сети);
* Выдачи печатных (графических) выходных документов;
* Запуска/завершения программ и процессов (заданий, задач);
* Доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи.

Необходим так же, учет носителей информации, а так же очистка (обнуление) освобождаемых областей ОП ЭВМ и внешних накопителей.

**Организационные мероприятия**

Организационные мероприятия для обеспечения защиты информации от утечки, модификации или уничтожения включают:

1. Контроль доступа к СВТ:

* Должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации, особенно в нерабочее время;
* Должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку) и регистрацией их выдачи (приема).

1. Комплект нормативных документов, регламентирующих порядок работы и настройки вычислительной техникой:

* Должна осуществляться регистрация подключения и работы пользователей в сетях передачи данных;
* Должна быть утверждена типовая аппаратная конфигурация СВТ;
* Должен быть утвержден регламент приобретения оборудования.

1. Комплект документов, устанавливающий настройки системного и общесистемного ПО:

* Должен быть утвержден регламент запущенных сервисов на серверном оборудовании и рабочих местах;
* Должна осуществляться регистрация следующих событий:
* Использование идентификационного и аутентификационного механизма;
* Создание и уничтожение объекта;
* Действия по изменению правил разграничения доступа.
* Должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала с помощью тест-программ, имитирующих попытки НСД;
* Должен существовать регламент ведения и хранения контрольного журнала, регистрирующего все чрезвычайные ситуации и события, связанные с нарушением режима безопасности. Кроме отвергнутых попыток входа в системы, целесообразно также регистрировать случаи успешного доступа к ним. Контрольный журнал должен включать следующие данные:
* Дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
* Результат попытки входа: успешная или неуспешная - несанкционированная;
* Идентификатор субъекта, предъявленный при попытке доступа;
* Код или пароль, предъявленный при неуспешной попытке.

Для обеспечения точности контрольных журналов, которые могут потребоваться при расследовании или в качестве свидетельства при наложении дисциплинарных взысканий, необходимо правильно установить системные часы компьютеров. Неточные контрольные журналы могут помешать таким расследованиям и подорвать доверие к такому свидетельству;

Должен быть утвержден регламент антивирусной защиты: определены настройки мониторов для рабочих мест пользователей и администратора, периодичность обновления антивирусных баз.

1. Контроль доступа к объектам системы:

* Должен быть утвержден регламент предоставления прав доступа к информационным ресурсам, определяющий все стадии жизненного цикла управления доступом пользователей – от начальной регистрации новых пользователей до удаления учетных записей пользователей, которые больше не нуждаются в доступе к информационным сервисам. Особое внимание следует уделить необходимости управления процессом предоставления привилегированных прав доступа, которые позволяют пользователям обойти средства системного контроля.
* Должен существовать регламент удаления учетных записей пользователей, которые больше не нуждаются в доступе к информационным сервисам.

1. Комплект документов, регламентирующих механизмы восстановления системы после сбоя и поддержания работоспособности системы:

* Должен быть утвержден перечень критически важного оборудования, находящегося в резерве;
* Инструкция на инсталляцию СУБД;
* Регламент импорта данных;
* Очередность подключения рабочих мест;
* Должен быть установлен регламент конфигурационного управления: подключения новых пользователей, изменения конфигурационных файлов активного оборудования, сетевого оборудования;
* Должен быть утвержден регламент резервного копирования и архивирования, должны создаваться две резервные копии, которые хранятся отдельно от серверного оборудования;
* Должен быть разработан план защиты от непредвиденных обстоятельств, определяющий последовательности действий, необходимых для выхода из различных ситуаций, не предусмотренных процедурами нормального функционирования системы (например, в случае пожара). План защиты от непредвиденных обстоятельств должен включать такие элементы, как:
* Сведения о том, кто является главным ответственным лицом и как можно установить с ним контакт;
* Информация о том, кто и на каком основании принимает решение о возникновении необычной ситуации;
* Технические требования к передаче управления резервным службам, которые могут включать сведения о необходимом дополнительном оборудовании и линий связи;
* Организационные требования в отношении персонала, который осуществляет передачу управления резервным службам;
* Сведения о любых внешних источниках, в которых можно будет получить помощь.

6. Контроль за персоналом включает следующие мероприятия:

* Организация службы безопасности информации, осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;
* Ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
* Получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
* Очистка оперативной памяти клиентских ПК путем перезагрузки после завершения работы пользователя с защищаемыми данными, с удалением файлов с жесткого диска компьютера;
* Должен быть определен регламент реагирования на нарушение безопасности, содержащий описание действий пользователя и администратора при выявлении НСД.

# **Заключение**

Опыт показывает, что для достижения удачных решений по защите информации необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.

# **Список литературы**