МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Белорусский государственный технологический университет»

Кафедра информационных технологий

Практическое занятие №3

Разработка политики информационной безопасности ОАО «Беларуськалий» в г. Солигорске

Выполнила:

Студентка 2 курса, 7 группы

Курносенко Софья Андреевна

Проверил:

Барковский Евгений Валерьевич

Содержание

[Введение 3](#_Toc98452342)

[Оценка рисков 5](#_Toc98452343)

[Разработка мер защиты 6](#_Toc98452344)

[Общие меры безопасности 6](#_Toc98452345)

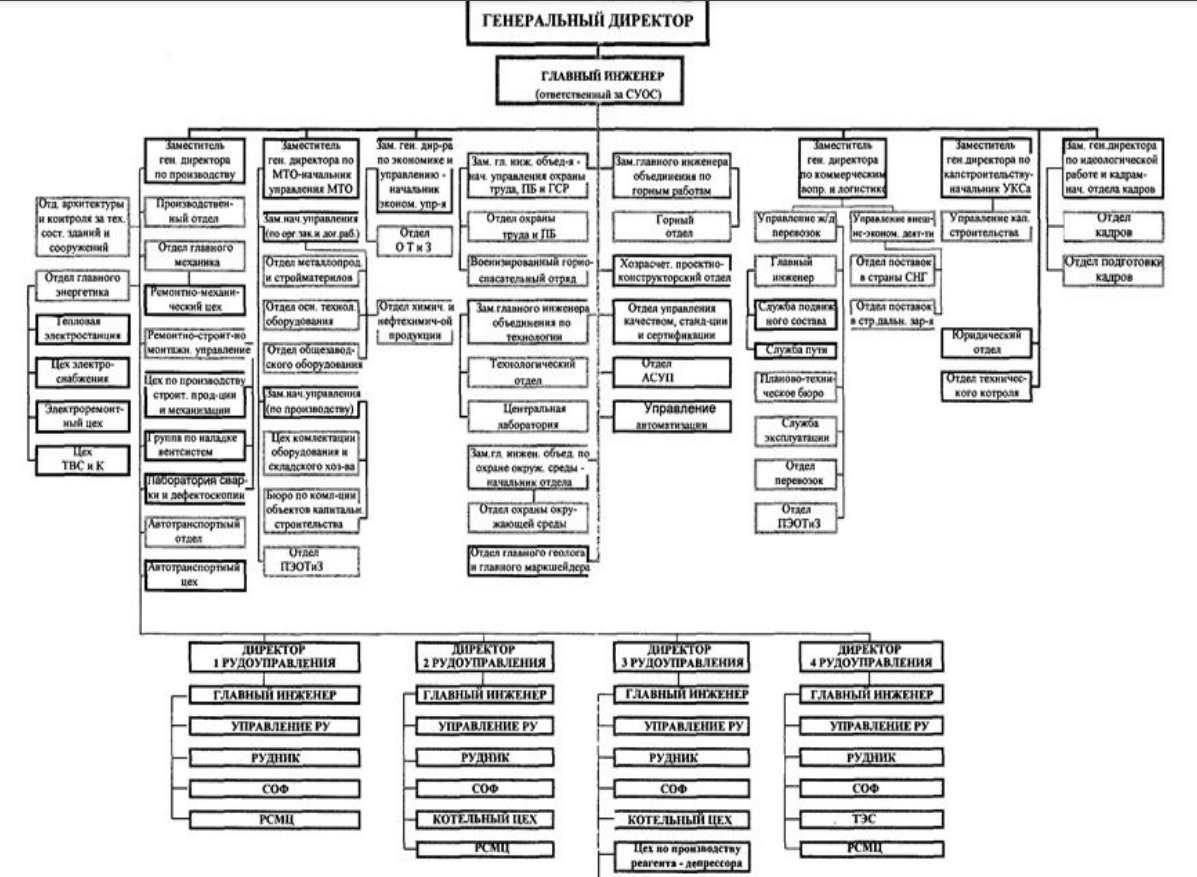
[Заключение 11](#_Toc98452346)

# 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.

**Структура предприятия**

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.



# Оценка рисков

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления информационной безопасностью.

При оценивании рисков учитывается:

• ценность ресурсов;

• оценка значимости угроз;

• эффективность существующих и планируемых средств защиты.

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

* антропогенные,
* техногенные,
* естественные (природные).

Возникновение **антропогенных** угроз обусловлено деятельностью человека. Среди них можно выделить как угрозы, возникающие вследствие непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение **техногенных** угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение **естественных** (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека. К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

# Разработка мер защиты

**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 несопоставимо больше умышленного вреда.

**Возможные угрозы и способы их предостережения:**

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 данной ситуации, 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 (несанкционированного доступа), 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, нужно установить антивирусную программу. 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

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.

8. 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.

# Заключение

Политика безопасности — совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На политике безопасности нельзя экономить, так как данные, которые могут быть подвержены хищению, копированию или изменению, могут стоить дороже, чем ресурсы, потраченные на ее разработку и осуществление.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность и общие меры предосторожностей.

Необходимо иметь в виду, что многие меры защиты требуют достаточно больших вычислительных ресурсов, что в свою очередь существенно влияет на процесс обработки информации.