МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий   
Кафедра информационные системы и технологии   
Специальность 1-40 01 01 «Программное обеспечение информационных технологий»   
Специализация Программирование интернет-приложений

**Проект информационной безопасности метрополитена**

Выполнил студент Козловский Д. В.

(Ф.И.О.)

Преподаватель Блинова Е.А.

(Ф.И.О.)

Минск 2018

**ВВЕДЕНИЕ**

**Цель работы** - разработать проект политики информационной безопасности бизнес-компании.

Развитие и рост предприятий очень тесно связан с ростом ИТ-инфраструктуры и информационных систем, сложность и масштабы которых постоянно растут, порождая при этом новые виды угроз, уязвимостей и рисков, которые прямым образом влияют на деятельность организации.

Возникновение проблем в информационной безопасности организации приводит как к финансовым, так и к репутационным потерям. Важная задача руководства – предотвратить эти угрозы, минимизировать риски и обеспечить должный уровень безопасности ИТ-инфраструктуры предприятия.

Основой мер административного уровня, то есть мер, предпринимаемых руководством организации, является политика безопасности.

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Любая защитная мера есть компромисс между снижением рисков и удобством работы пользователя. Таким образом, политика выполняет две основные функции:

* определяет безопасность внутри организации;
* определяет место каждого служащего в системе безопасности.

Оглавление

[ОБЩИЕ ПОЛОЖЕНИЯ 5](#_Toc506967285)

[ОЦЕНКА РИСКОВ 6](#_Toc506967286)

[РАЗРАБОТКА МЕР ЗАЩИТЫ 8](#_Toc506967287)

[Меры обеспечения безопасности. 8](#_Toc506967288)

[Формирование политики безопасности 9](#_Toc506967289)

[Организационное обеспечение информационной безопасности 10](#_Toc506967290)

[СТОИМОСТЬ МЕРОПРИЯТИЙ ВО ВНЕДРЕНИЮ ЗАЩИТЫ ПРЕДПРИЯТИЯ ОТ ВОЗМОЖНЫХ УГРОЗ 12](#_Toc506967291)

[ВЫВОД 13](#_Toc506967292)

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика разработана в соответствии с законодательством РБ и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов

1.2. Настоящая Политика является документом, доступным любому сотруднику ит - предприятия и пользователю его ресурсов, и представляет собой официально принятую руководством систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности.

1.3. Руководство ит - предприятия осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования ит деятельности, а также развития реализуемых ит технологий и ожиданий клиентов предприятия и других заинтересованных сторон. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества предприятию обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

1.4. Требования информационной безопасности, которые предъявляются предприятиеем, соответствуют интересам (целям) деятельности предприятия и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере предприятия имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности. Факторы рисков в информационной сфере предприятия составляют значимую часть операционных рисков предприятия, а также имеют отношение и к иным рискам основной и управленческой деятельности предприятия.

## ОЦЕНКА РИСКОВ

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Существуют различные подходы к оценке рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Процесс оценивания рисков содержит несколько этапов.

1. Идентификация ресурса и оценивание его количественных показателей (определение негативного воздействия).
2. Оценивание угроз.
3. Оценивание уязвимостей.
4. Оценивание существующих и предполагаемых средств обеспечения.
5. Оценивание рисков.

На основании оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для нормальной работы организации и имеющие определенную степень уязвимости, считаются подверженными риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

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 ИБ.

При оценивании рисков учитывается:

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

* количественными (например, стоимостные);
* качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный);
* их комбинацией.

Вероятность того, что угроза реализуется, определяется следующими факторами:

* привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;
* технические возможности угрозы, используемые при умышленном воздействии со стороны человека;
* вероятность того, что угроза реализуется;
* степень легкости, с которой уязвимость может быть использована.

Все риски, связанные с производством гофротары, можно поделить на внутренние и внешние.

К внутренним рискам относятся:

* утрата сведений о пакете заказов и общей информации о заказчиках;
* ознакомление работниками комбината посторонних лиц с конфиденциальной информацией о заказах, а также об отчётах должностных лиц на предприятии;
* недоступность информации о заказах, о дневном задании по причине неисправности оборудования;
* отсутствие контроля процесса производства;
* низкая квалификация работников производства.

К внешним рискам относятся:

* взлом базы данных технологов производства гофротары;
* кража стандартов производства и технологических карт.

В результате воздействия угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности:

* финансовые потери, связанные с утечкой или разглашением защищаемой информации;
* финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
* ущерб от дезорганизации деятельности и потери, связанные с невозможностью выполнения им своих обязательств;

## РАЗРАБОТКА МЕР ЗАЩИТЫ

## Меры обеспечения безопасности.

Все меры обеспечения безопасности компьютерных систем подразделяются на:

* правовые (законодательные);
* морально-этические;
* организационные (административные);
* физические;
* технические (аппаратурные и программные).

Законодательные (правовые) меры защиты. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и Политика информационной безопасности использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

Морально-этические меры защиты. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

Организационные (административные) меры защиты. Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Физические средства защиты. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Технические (программно-аппаратные) средства защиты. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав информационных систем и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

## Формирование политики безопасности

Политика служит методологической основой для формирования и реализации программы создания системы информационной безопасности.

В целом для функционирования системы информационной безопасности с учетом положений Политики должны быть разработаны и приняты (с учетом необходимого обновления) следующие документы:

* классификация (анализ) рисков информационной безопасности;
* внутренний документ о порядке отнесения сведений к конфиденциальной информации;
* перечень сведений, составляющих конфиденциальную информацию;
* организационно-распорядительные документы, регламентирующие порядок и правила обеспечения сохранности конфиденциальной информации в рамках каждой функциональной задачи и соответствующей ей автоматизированной системы.

Для осуществления технической политики в области обеспечения информационной безопасности необходимо разработать и реализовать комплекс мероприятий:

* по обеспечению технической и программной защиты информации в автоматизированных системах;
* по оснащению важнейших объектов и помещений средствами и системами защиты и контроля.

В процессе создания системы безопасности необходимо предусмотреть приоритеты реализации наиболее важных и актуальных направлений обеспечения безопасности, с учетом выделяемых финансовых ресурсов.

В целях достижения оптимального уровня информационной безопасности следует:

* иметь в наличие внутренний документ, определяющий порядок определения сведений, составляющих конфиденциальную информацию и требования к организации их защиты, включающие описание процедур отнесения сведений к категории конфиденциальных и, в случае необходимости, в установленном порядке вносить в него изменения и дополнения;
* определять полный перечень и возможные угрозы нарушения конфиденциальности информации и классифицировать их по вероятности возникновения исходя из принятой типовой модели нарушителя;
* с учетом действующих мер и средств защиты проводить оценку риска утечки конфиденциальной информации;
* разработать и внедрить систему обеспечения безопасности информации (систему защиты информации), направленную на снижение уровня риска, включающую комплекс организационных мер и технических средств;
* на постоянной основе проводить обучение и повышение квалификации персонала в области информационной безопасности;
* проводить периодический контроль эффективности и адекватности принимаемых мер защиты информации.

## Организационное обеспечение информационной безопасности

Задачи обеспечения безопасности информационных ресурсов решаются следующими организационными методами:

* разработкой и осуществлением разрешительной системы допуска работников к работам с документами и сведениями конфиденциального характера;
* установлением единого порядка хранения и обращения конфиденциальной информации (документов, носителей информации);
* координацией работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи.

При работе основными организационными мерами в плане достижения информационной безопасности являются:

* заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности и сохранность конфиденциальной информации;
* проведение периодического обучения и повышения квалификации работников производства в области информационной безопасности.

Система распределения обязанностей между отдельными работниками может в значительной мере способствовать повышению общего уровня информационной безопасности. Этого можно достичь следующими методами:

* минимизация данных, доступных работникам. Каждый работник должен знать только те детали процедур обработки данных, которые необходимы ему для выполнения своих обязанностей. Организация технологического процесса сбора и обработки информации и планирование помещений должны по мере возможности исключать или сводить к минимуму контакты персонала в процессе выполнения работ. Каждый работник должен знать все о своей работе и связанных с нею ограничениях, а также четко представлять последствия нарушения этих ограничений;
* разделение полномочий и дублирование контроля. Временные или вновь принятые работники, а также работники, проходящие обучение, стажировку, практику не должны самостоятельно выполнять ответственные задания.

Административные меры защиты информации предполагают:

* обеспечение физической сохранности гофроагрегатов и дополнительного оборудования;
* организацию контроля доступа и режима выполнения работ персоналом подразделения информационных технологий;
* инспектирование правильности и полноты выполнения персоналом подразделения информационных технологий мер по обеспечению сохранности необходимых дубликатов файлов, библиотеки программ, оборудования системы;
* практическую проверку функционирования отдельных мер защиты: предотвращения недозволенных изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;
* проверку машинных и ручных протоколов выполнения работ со стороны пользователей.

## СТОИМОСТЬ МЕРОПРИЯТИЙ ВО ВНЕДРЕНИЮ ЗАЩИТЫ ПРЕДПРИЯТИЯ ОТ ВОЗМОЖНЫХ УГРОЗ

Сформированный бюджет службы безопасности можно рассмотреть на уровне упрощенной модели как совокупность трех составляющих компонент (см. рисунок 1). Всю деятельность по защите информации можно условно разделить на:

1) мероприятия административно-организационные;

2) мероприятия технические;

3) действия, направленные на ликвидацию последствий воздействия негативных факторов или форс мажорных обстоятельств.

Суммарные ежегодные затраты на информационную безопасность можно рассчитать по формуле :

ЗИБ = Зо + Зт + Зл , где

ЗИБ – ежегодные суммарные затраты на безопасность, руб.

Зо – за­траты на административно-организационные мероприятия, руб.

Зт – за­траты на технические мероприятия, руб.

Зл– затраты на ликвидацию последствий, руб.

Зо  - включают в себя годовой фонд оплаты труда, представительские расходы, расходы на аналитическую и оперативную деятельность, вообще все, что не включается в прямые затраты на приобретение и эксплуатацию материально-вещественного инструментария безопасности. Зт  - затраты формируемые за счет технического перевооружения и приобретения\эксплуатации материальных фондов. Зл  - резервный фонд, закладываемый на случай обстоятельств не преодолимой силы.

## ВЫВОД

В данном проекте была разработана и рассмотрена политика информационной безопасности на примере ит - предприятия. Важно управлять информационной системой в целом и механизмами безопасности в особенности. Упомянутые меры безопасности должны опираться на общепринятые стандарты, быть устойчивым к сетевым угрозам, учитывать специфику отдельных сервисов. В ходе создания данного проекта были рассмотрены следующие пункты: была рассмотрена структура информационной безопасности ит - предприятия, были рассмотрены и оценены различные риски, а так же были предусмотрены и разработаны меры защиты информации.

Руководство компании заявляет своё одобрение настоящей Политики, которая будет объявлена, распространена, внедрена, а так же будет поддерживаться на всех уровнях данной компании.

Политика информационной безопасности компании является общедоступным документом, который может предоставляться всем заинтересованным сторонам.