Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа №1

**Разработка и внедрение политики безопасности**

**IT-компании**

Студента: Чистякова Ю.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

**Оглавление**

[Введение 3](#_Toc32993865)

[Обоснование актуальности 4](#_Toc32993866)

[Описание структуры организации 5](#_Toc32993867)

[Основные угрозы и их источники 8](#_Toc32993868)

[Оценка угроз, рисков и уязвимостей 10](#_Toc32993869)

[Разработка мер защиты 11](#_Toc32993872)

[Вывод 14](#_Toc32993873)

# **Введение**

В нынешнее время все компании нуждаются в информационных технологиях для того, чтобы выдерживать конкуренцию в условиях повсеместного использования высокотехнологичных решений. Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры.

Жизнь современного общества немыслима без информационных технологий. Программные средства обслуживают банковские системы, распределяют энергию, следят за расписанием поездов. Они обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса о разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Однако именно высокая степень автоматизации порождает риск снижения личной, информационной и государственной безопасности, делая ее чрезвычайно уязвимой.

Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, Конституции, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

# **Обоснование актуальности**

Любой компании, ведущей свой бизнес, приходится работать с информацией везде и всегда, как при планировании долгосрочных стратегических задач, так и при рутинных канцелярских делах. В процессе бурного развития науки и техники появилось немало методов и средств работы с информацией, порой настолько сложных, что применение их, их адаптация к специфике конкретной компании и условий, в которых она находится, сейчас уже является отдельным классом задач, решаемых специализированными ИТ организациями.

Каждая фирма имеет дело с внешними и внутренними источниками информации, с выполнением таких операций, как сбор информации, ее первичная обработка, отображение, кодирование и декодирование, преобразование, запоминание (хранение), передача, защита. В средних и тем более крупных по размеру компаниях осуществление вышеуказанных операций немыслимо без применения информационных технологий. Под информационными технологиями здесь понимаются: обычные средства; средства на основе вычислительной техники; методы связи.

В век высоких технологий компаниям просто необходимо использовать информационных ресурсы и технологии. Согласно исследованиям, многие IT-компании практически не защищены от кражи и утери конфиденциальных данных. Сейчас, как никогда, тема информационной безопасности актуальна для компаний.

Новые технологии позволяют собрать клиентскую базу, анализировать и структурировать ее, а также изучать кейсы, создавать базы стандартных ответов в типичных ситуациях и передавать их потребителям IT услуг.

Как правило, в IT фирмах отсутствует разработанная политика информационной безопасности, используются минимальные средства защиты и не нанимаются сотрудники, отвечающие за информационную безопасность. Все это приводит к рискам утечки конфиденциальной информации, потере репутации и последствиям раскрытия хранимой конфиденциальной информации. В числе наиболее важных мер по обеспечению информационной безопасности является аудит информационной безопасности, создание документа, регулирующего процесс обеспечения информационной безопасности, настройку систем защиты, проведения тренинга среди сотрудников, страхование рисков во всех сферах.

# **Описание структуры организации**

В большинстве случаев кажровый состав IT отдела включает в себя сотрудников следующих профилей:

* + специалист по сетевому обеспечению;
  + системный аналитик;
  + программист;
  + системный администратор;
  + специалист по поддержке пользователей;
  + руководитель отдела ИТ;
  + веб-мастер.

Специалист по сетевому обеспечению определяет возникающие в ходе работы сети проблемы; анализирует требования пользователей; координирует процесс наладки и поддержки сетевого оборудования; обеспечивает совместимость программного и аппаратного сетевого обеспечения; готовит бюджет в подотчетной сфере и обеспечивает эффективное использование ресурсов; руководит менее квалифицированным техническим персоналом.

Системный аналитик проводит анализ требований пользователей для определения конфигурации программного и аппаратного обеспечения; готовит технические спецификации, технические отчеты по поддержке программного и аппаратного обеспечения; проводит анализ комплексных вопросов программирования касательно модификации кода уже существующих программ и создания кода для новых программ.

Программист решает комплексные вопросы программирования, касающиеся модернизации, модификации уже существующего кода либо создания нового кода; готовит графики и диаграммы рабочего процесса; устанавливает последовательность проведения операций по вводу и компьютерной обработке данных; контролирует проведение тестирования и отладки программного обеспечения.

Системный администратор производит установку программного и аппаратного обеспечения; осуществляет мониторинг и оптимизацию работы операционных систем вычислительной техники; определяет проблемы в программном обеспечении; анализирует требования пользователя, оценивает дополнительные возможности по улучшению работы программного обеспечения.

Специалист по поддержке пользователя отвечает за установку и проведения диагностики программного и аппаратного обеспечения; предоставляет техническую поддержку и консультации конечным пользователям; несет ответственность за организацию ремонта компьютерной техники; обеспечивает наличие расходных материалов для компьютерной и оргтехники; консультирует пользователей по техническим вопросам.

Руководитель отдела IT руководит любой деятельностью, связанной с обслуживанием вычислительной техники; контролирует процесс подбора, установки, поддержки программного и аппаратного обеспечения; контролиует связи компании с партнерами, предоставляющими услуги в сфере IT; руководит процессом подбора, обучения специалистов отдела, анализирует результаты их деятельности; руководит процессом обучения сотрудников.

На данный момент Интернет в сфере бизнеса является не только средством связи между территориально удаленными подразделениями или разными фирмами, но и средством, с помощью которого можно осваивать новые рынки, предъявив потенциальным клиентам свою визитную карточку – вэб-сайт.

В зависимости от типа вэб-сайта (сайт-визитка, информационный портал, интерактивный портал с Интернет-магазином) количество требуемых специалистов может существенно варьироваться. В самом сложном случае, в отделе IT должны присутствовать:

* PHP/ASP/Perl/JavaScript программист со знанием языка управления базами данных SQL;’
* HTML/CSS/Flash верстальщик;
* Веб-дизайнер, работающий на профессиональном уровне с такими прграммами редактирования растровой и векторной графики, как AdobePhotoshop, CorelDraw;
* Контент-менеджер, отбирающий, редактирующий текстовую и графическую информацию для последующего размещения на сайте;
* Системный администратор по вэб-службам (Apache, cron, sshd, sendmail, mysql);
* Специалист по привлечению посетителей сайта (SEO, регистрация в тематических каталогах, заказ рекламы и ссылок).

Отсюда видно, что задача создания крупного, динамически развивающегося Интернет проекта, который приносил бы ощутимую пользу бизнесу – не из простых. Особенно с учетом того, что критерии качества вэб-сайтов становятся все более строгими с каждым годом. Разработчики программ выполняют первостепенную роль в индустрии IT, так как без развития самого программного обеспечения не может идти речи и о развитии бизнеса дистрибьюторов, интеграторов, специалистов по защите ПО.

На основе изложенной выше градации подчиненнных можно выделить наиболее простой способ организации – линейный. Он используется в небольших компаниях или на начальных этапах развития ИТ: выделяется должность руководителя отдела, в непосредственном подчинении которого находятся несколько ИТ-специалистов. В общем случае возможно представить структуру IT-компании графически (см. рисунок 1). Схема, представленная ниже, является функциональным способом организации подразделения (результат развития линейной структуры).

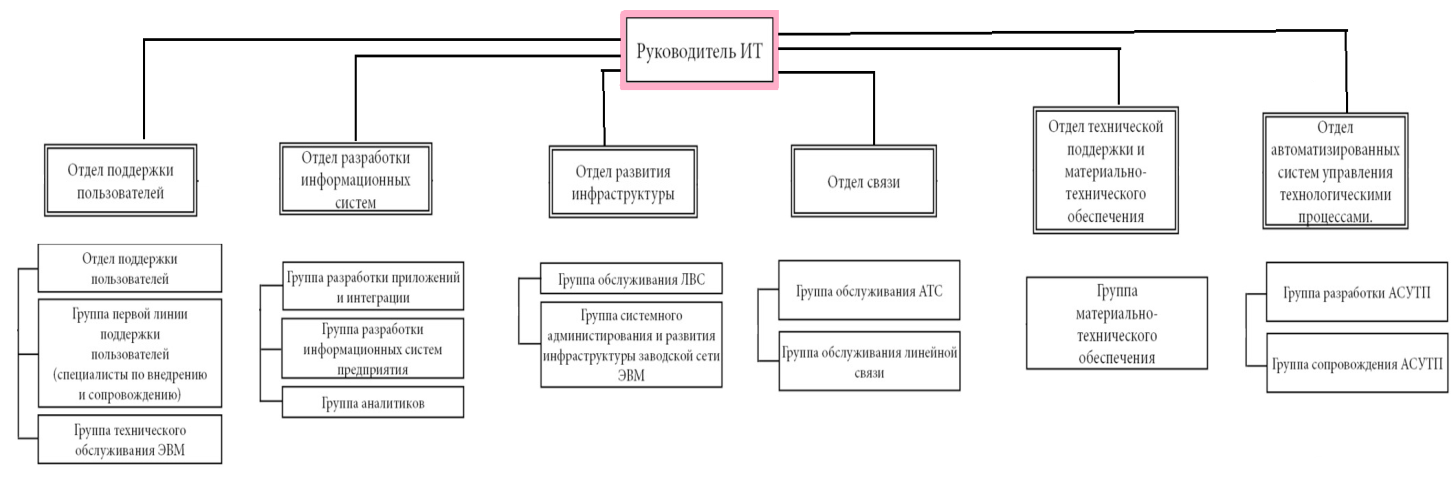


Рисунок 1 – Структура IT-компании

Минусом такой организационной структуры является увеличение руководящего состава в ИТ-структуре, усложнение администрирования распределенных информационных систем, так как получается, что за различные части этой системы отвечают сотрудники разных «дивизионов». Чтобы частично разрешить второй недостаток, используются также смешанные структуры, где основные ИТ-подразделения организуются на дивизиональной основе, но существуют отдельные подразделения ИТ, сохраняющие функциональную организацию, например, служба поддержки, организованная в центральном офисе, является единой для всех филиалов.

# **Основные угрозы и их источники**

В зависимости от критерия классификации, угрозы информационной безопасности IT-компании можно условно разделить на следующие основные подтипы:

* естественные и искусственные;
* преднамереннные и непреднамеренные;
* внешние и внутренние.

К естественным угрозам относят природные явления, которые не зависят от человека: ураганы, наводнения, пожары; угроза отключения электричества, что приведет к сбою незавершенных операций и потере данных; угроза возникновения неправильной адрессации пакетов.

Искусственные угрозы зависят непосредственно от человека. К ним относятся угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ, и попадания в офис.

Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличии от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри IT-компании. Результат реализации этого вида угроз – потери денежных средств, интеллектуальной собственности и доверительной репутации компании.

Источниками внутренних угроз являются сотрудники организации, программное обеспечение и аппаратные средства. Такие угрозы могут проявлятся в следующих формах:

* ошибки пользователей и системных администраторов;
* нарушения сотрудниками организации установленных регламентов сбора, обработки, передачи и уничтожения информации;
* отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся: компьютерные вирусы и вредоносные программы; организации и отдельные лица; стихийные бедствия. Формами проявления внешних угроз являются:

* заражение компьютеров вирусами или вредоносными программами; несанкционированный доступ (НСД) к корпоративной информации;
* информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;
* действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;
* аварии, пожары, техногенные катастрофы.

По степени преднамеренности проявления (случайные и преднамеренные):

* случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия, ошибки пользователей и т.п.).
* преднамеренные (умышленные действия, например, шпионаж, диверсия, перехват информации, хакерские атаки, фальсификация документов и т.п.)

По размерам наносимого ущерба:

* общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба).
* локальные (причинение вреда отдельным частям объекта безопасности).
* частные (причинение вреда отдельным свойствам элементов объекта безопасности).
* по степени воздействия на информационную систему:
* пассивные (структура и содержание системы не изменяются).
* активные (структура и содержание системы подвергается изменениям).

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:

* информационные;
* программные;
* физические;

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* хищение информации из архива, отделов и баз данных;
* нарушение технологии обработки информации;
* противозаконный сбор и использования;
* использование информационного оружия.

К программным угрозам относятся

* использование ошибок и «дыр» в ПО;
* компьютерные вирусы и вредоносные программы;

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи;
* хищение носителей информации;
* хищение программных или аппаратных ключей и средств криптографической защиты данных;
* воздействие на персонал (шантаж, нападение).

# **Оценка угроз, рисков и уязвимостей**

Согласно промежуточным результатам исследования, все IT-компании имеют незакрытые критические уязвимости на ПК и серверах, половина – на сетевом оборудовании. 15% компаний не имеют даже минимальной системы защиты, 39% – уязвимы для действий инсайдеров, а 62% – не защищены от внешних угроз. Причинами являются отсутствие шифрования данных; реагирования на инциденты; неразграничение прав доступа; из всех средств защиты присутствуют лишь антивирус и слабые пароли.

На практике это, в частности, означает высокую вероятность взлома; моментальную доступность конфиденциальной информации при утере или выемке устройства, на которой она хранится; неотслеживаемость действий инсайдеров; невозможность узнать и отреагировать на кибератаку.

В частности, нарушение конфиденциальности данных IT-компании зачастую приводит к вымогательству и шантажу, инсайдерской торговле и недобросовестной конкуренции. Это не только нанесет урон репутации – IT фирма понесет ответственность – от финансовой до уголовной.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. 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, стоимостными), качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный) или их комбинацией.

Таблица 1 – Условная численная шкала для оценки ущерба it-компании

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 1 | Раскрытие данных принесет ничтожно малый моральный и экономический ущерб компании |
| 2 | Ущерб от атаки есть, но основные операции и положения затронуты не будут |
| 3 | Значительные финансовые потери и потери доверия со стороны клиента, ощутимая часть которых уйдет |
| 4 | Потери очень значительные, компания теряет свое положение на рынке на период до 2-ух лет. Для восстановления положения потребуются крупные финансовые займы |
| 5 | Компания прекращает существование |

В таблице 1 показаны последствия различной величины ущерба

Можно конкретизировать определение вероятности наступления угрозы ресурсу. Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка ПБ требует учета специфики IT-компании. На таблице 2 приведена шкала вероятности того, что угроза будет реализована.

Таблица 2 – Вероятностно-временная шкала реализации НСД к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Также можно создать таблицу рисков, на этапе анализа которой риски задаюются некоторым максимально допустимым уровнем (порогом). Далее проверятся каждая строка таблицы: превышен или непревышен порог для значения риска, связанного с анализируемой атакой.

Таблица 3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб \* Вероятность) |
| Спам (переполнение почтового ящика) | 1 | 0,4 | 0,4 |
| Копирование жесткого диска из центрального офиса | 3 | 0,1 | 0,3 |
| НСД к корпоративной информации | 4 | 0,2 | 0,8 |
| Мониторинг внутренней работы со стороны специальных служб | 3 | 0,2 | 0,6 |
| Отказы и сбои в работе оборудования | 3 | 0,3 | 0,9 |
| Проникновение на рабочие места не работников отдела, которые имеют туда доступ | 3 | 0,1 | 0,3 |
| Ошибки в работе системных администрторов | 2 | 0,4 | 0,8 |
| Итого | 19 | 1,7 | 32,3 |

Если такое превышение имеет место, данная атака должна рассматриваться с точи зрения одной из первоочередных целей разработки политики безопасности (таблица 3).

# **Разработка мер защиты**

Информационная безопасность it-компаниидолжна обеспечиваться целым комплексом мер, среди которых:

* административно-правовые;
* организационные;
* программно-технические.

Данные меры следует применять совместно. Опираться система защиты должна на управление персоналом компании и контроль над ним. Меры технического характера не менее важны, но не могут существовать в отрыве от организационных мер.

Административные меры безопасности включают в себя разработку внутренних нормативных документов, обеспечивающих информирование сотрудников о системе действий, необходимых для обеспечения информационной безопасности. В it-компании должно быть организовано ознакомление персонала с внутренними нормативными документами.

Служба безопасности it-компанииразрабатывает и предлагает на утверждение руководства политику защиты конфиденциальной информации, который содержит:

* основные принципы защиты конфиденциальной информации в компании;
* контроль исполнения требований законодательства и внутренних документов;
* обязанности каждого сотрудника в части защиты доверенных ему сведений;
* меры ответственности за нарушение положений документа;
* задачи руководства по обеспечению охраны информации;
* проведение профилактических мер при приеме на работу и увольнении работников;
* регламенты обращения с компьютерной техникой и средствами коммуникации;
* контроль соответствия бизнес-процессов требованиям политики;
* реагирование на инциденты, локализацию и минимизацию последствий;
* анализ новых рисков ИБ it-компании;
* определение действий при возникновении чрезвычайных ситуаций.

Все трудовые договоры должны содержать перечень информации, носящей характер коммерческой, а в самих договорах должны быть предусмотрены меры ответственности за ее разглашение.

Организационные меры безопасности направлены на устранение внутренней угрозы утечки информации и мотивацию сотрудников на соблюдение утвержденных регламентов. Эти меры предпринимаются службой безопасности во взаимодействии с сотрудниками служб управления персоналом.

В числе организационных мер обеспечения информационной безопасности можно назвать следующие:

* установление различных степеней допуска сотрудников к сведениям, содержащим коммерческую тайну;
* ограничение круга лиц, имеющих допуск к конфиденциальной информации it-компании;
* организация порядка использования материальных носителей, установление контроля над копированием и сканированием документов, ограничение доступа сотрудников к внешней электронной почте;
* проведение периодических проверок соблюдения регламентов;
* привлечение специалистов для проведения тренингов по защите информации;
* проведение мероприятий по созданию режима коммерческой тайны;
* внесение в договоры компании с клиентами норм, касающихся обязательств соблюдения последними режима коммерческой тайны в отношении переданной им информации;
* привлечение к ответственности лиц, виновных в разглашении информации.

Иногда система работы с безопасностью информации требует создания в компании специального подразделения, в чьи функции будет входить только эта деятельность.

Также следует учитывать, что при проектировании большинства информационных систем уровень защиты от внешнего проникновения был значительно ниже, чем необходим в настоящее время. Среди организационных мер может быть и их аудит, который установит соответствие современным стандартам.

Технические меры рассчитаны на использование действенных технических средств защиты. Для их реализации используются аппаратные, программные и криптографические средства. Первые предполагают установку систем резервного копирования и защиту от несанкционированного проникновения, вторые отвечают за работу антивирусов и иных защитных программ, третьи обеспечивают шифрование всей хранимой и передаваемой по каналам связи информации. Наиболее часто для защиты информации применяются межсетевые экраны и системы обнаружения вторжений. Технические средства требуют постоянного обновления и модернизации, так как скорость устаревания программных продуктов очень высока.

Технические меры безопасности включают (но не ограничены ими):

* регистрацию, проверку пользователя при помощи капчи;
* построение периметра безопасности защищаемых объектов;
* организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
* организацию противопожарной безопасности складов;
* контроль доступа работников it-компаниив помещения ограниченного доступа;
* использование лицензионного программного обеспечения и сертифицированных средств защиты информации;
* применение комплексной антивирусной защиты;
* использование специальных комплексов ИК (как защита электронных информационных ресурсов, так и защита от утечки по электромагнитным и акустическим каналам);
* обеспечение регулярного резервного копирования информации;
* контроль за правами и действиями пользователей, в первую очередь, привилегированных;
* применение систем криптографической защиты информации;
* обеспечение безотказной работы аппаратных средств;
* мониторинг состояния критичных элементов информационной системы.

Следует провести комплексную оценку с привлечением специализированных людей. Также, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

Комплексное применение современных технических средств в работе службы безопасности it-компании может обеспечить высокий уровень защиты информации от утечек и несанкционированного доступа.

# **Вывод**

Мною были выявлены все возможные угрозы и их источники информационной безопасности в ИТ-компании, а также проанализированы и оценены собранные данные.

На основании этого была разработана концепция, основные элементы политики безопасности для ИТ-компании.

Также были разработаны мероприятия по внедрению разработанной мной политики безопасности на предприятии.

Результаты проделанной работы оформлены в виде описания разработанной политики безопасности а также плана мероприятий по ее реализации.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки, можем выделить следующие рекомендации, следуя которым возможно снизить риски опасного воздействия и их последствий:

* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь офиса с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, баз данных милиции;
* защита серверов компании и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам.
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие в офисе наглядного отображения плана по работе во время чрезвычайных ситуаций.