Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

**«Разработка политики информационной безопасности**

риэлтерской компании»

Студент: Герман А.Е.

ФИТ 2 курс 4 группа

Преподаватель: Барковский Е. В.

Минск 2022

**Введение**

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.

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

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 под хода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Разработанная и утвержденная документация должна включать в себя следующие разделы:

* перечисление объектов, в отношении которых устанавливается режим информационной безопасности, их ранжирование по значимости и требуемой степени защиты;
* описания технологий, применяемых для обеспечения сохранности информации;
* перечень действующих и потенциальных угроз информационной безопасности, описание степени их серьезности и реализуемости;
* описание внешних и внутренних субъектов, которые могут стать источниками потенциальной угрозы;
* описание понятия инцидента информационной безопасности, процедур уведомления о его возникновении;
* описание применяемых организационных мер, действий сотрудников компании по обеспечению информационной безопасности;
* описание выбранной политики защиты от вирусных атак, программ-вредителей, возможных действий хакеров;
* описание системы резервного копирования важных данных, ее периодичности, моделей хранения – на дисках, на посторонних серверах;
* описание того, в каком порядке будут проводиться аварийные и восстановительные работы при повреждении аппаратной части в случае пожара, проблем с электросвязью или по иным причинам, повлекшим за собой гибель компьютеров, носителей информации или самих баз данных;
* план мероприятий по постоянному поддержанию готовности системы к работе, ее обновлению при изменении правил сертификации или степени значимости угроз.

Целью политики является регламентирование единых подходов и требований по обеспечению информационной безопасности сотрудниками компании, а также государственными органами и организациями, иными юридическими лицами и индивидуальными предпринимателями в рамках оказания им услуг риэлтерской компанией.

Достижение указанной цели предполагает решение следующих задач:

* реализация требований законодательства государства в части информационной безопасности информационных систем и мер контроля их защищенности;
* определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований политики, в том числе с использованием программных, программно-аппаратных средств технической и криптографической защиты информации, а также посредством принятия соответствующих внутренних нормативных и организационно-методических документов информационной безопасности риэлтерской компании;
* своевременное выявление и оценка причин, условий и характера угроз информационной безопасности и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов информационной безопасности;
* планирование, реализация и контроль эффективности использования защитных мер и средств защиты информации, создание механизма оперативного реагирования на угрозы информационной безопасности;
* реализация программ по осведомленности и обучению сотрудников (работников) компании о возможных факторах рисков информационной безопасности и мерах противодействия.

**Описание структуры риэлтерской компании**

Структура риэлтерской компании (далее – компания) – это форма организации её внутренних элементов: подразделений, управлений и служб**.**

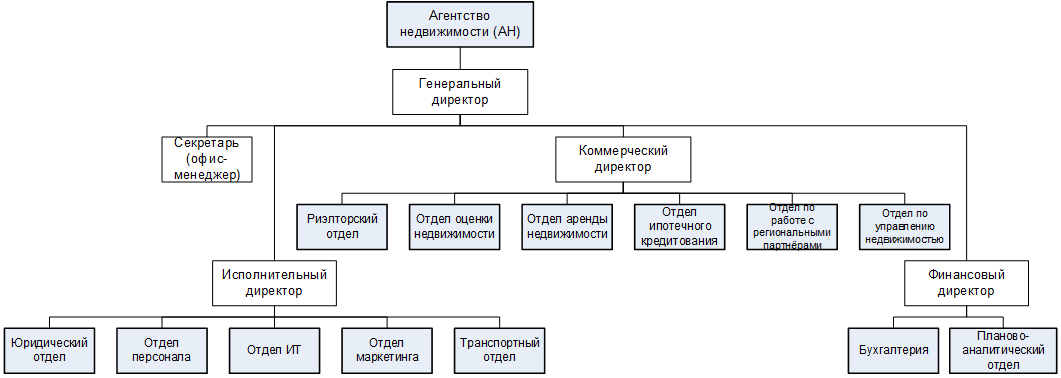
Среди внутренних аспектов работы компании особенно важными оказываются:

* Основные направления деятельности:
* совершение сделок купли продажи, дарения, обмена жилых и нежилых помещений;
* продажа жилых и нежилых помещений с аукциона и на конкурсной основе;
* сдача в аренду жилых и нежилых помещений, земельных участков, находящихся в собственности юридических и физических лиц;
* заключение договоров купли продажи жилья е пожизненным содержанием собственника и др.
* Масштаб деятельности компании: один или несколько близких городов, представительства в регионах страны, международные структуры;
* Важнейшие категории клиентов: частные лица, юридические лица.

К внешним условиям относятся:

* Указания владельцев компании;
* Правовые особенности оказания риэлтерских услуг.

В практике стран с развитой рыночной экономикой принята трехступенчатая классификация субъектов управления компании в зависимости от объема их распорядительных полномочий.

Рис. 1. Организационная структура агентства недвижимости,  
в виде графической схемы (верхний уровень)

**Высшее руководство (дирекция)** – в его компетенцию входит принятие основополагающих решений по поводу целевых установок и политики компании, подбор и расстановка кад­ров, руководство нижестоящими управленческими подразделениями.

**Среднее руководство (руководители отделов)** осуществляет управление отдельными сферами деятельности компании, регулирование процесса работы, руководство подчиненными служащими, подготовку принятия решений для дирекции.

**Низшее руководство (руководители отдельных групп)** распределяет задания и контролирует работу отдельных групп.

Основным структурными информационными объектами компании являются:

* + - * базы данных компании, хранящая информацию о продаже и покупке недвижимости; участниках продажи и покупки недвижимости; объектах недвижимости; об активах компании и ее деятельности; личные данные контрагента компании: адрес, семейное положение, место работы, дата рождения, наличие или отсутствие судимостей и т.д.;

Основными ресурсами информационной системы риэлтерской фирмы, подлежащие защите, являются сервера, хранящие информацию о компании и её клиентах, архивы документов, портативные носители информации и т.д.

Система критериев оценки ценности информационных систем компании сводится к оценке важности того или иного информационного объекта и к оценке возможных последствий нарушения целостности информации и несанкционированного к ней доступа. Особой защите подлежат носители информации, содержащие персональную информацию клиентов/потенциальных клиентов компании.

Список потенциальных угроз информационным системам компании:

* несанкционированный доступ к базам данных риэлтерской фирмы;
* различного рода атаки на серверы, на которых расположены ресурсы компании;
* несанкционированный доступ к архивам документов о имуществе клиентов и т.д.

**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.

Ценность информационных ресурсов компании характеризуется возможным вредом финансовому положению риэлтерской фирмы, а также понижением её репутационных характеристик. Особой ценностью обладают информационных объекты, содержащие информацию о клиентах компании, их имуществе и производимых с ним операций. Не меньшей ценностью обладают договоры в бумажном и электронном виде.

Значимость определённых угроз зависит от вреда, которые они могут нанести информационным системам и риэлтерской компании в целом. Примеры угроз:

* нарушение целостность информации, хранящейся на серверах;
* получения доступа к информации третьими лицами;
* обнародование секретной или конфиденциальной информации;
* несанкционированный доступ к помещениям, содержащим документы;
* различные стихийные бедствия, приводящие к нарушению целостности здания компании и уничтожения информационных объектов и т.д.

Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень. Обычной областью использования этого уровня являются типовые проектные решения.

Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности осуществления угроз и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

Оценка эффективности существующих или планируемых средств защиты основывается на глубоком анализе истории неблагоприятных для информационной системы компании ситуаций: возникновение серверных атак, конфликтных ситуаций с клиентами, возникших на основе нарушения целостности информации о жилищных объектах и получения третьими лицами доступа к конфиденциальной информации и т.д.

Чтобы определить вероятность выполнения одного из критических сценариев развития, угрожающих целостности информационной системе, ситуаций необходимо оценить привлекательность информационного ресурса как показателя при рассмотрении угрозы от умышленного воздействия со стороны человека:

* договора, документы – высокая ценность;
* справочная информация, база данных клиентской информации – средняя ценность;

Оценка рисков предполагает анализ средств, при помощи которых злоумышленник может навредить информационной системе компании, или стихийных бедствий, который могут стать причиной уничтожения физических носителей информации:

* специально ПО для доступа к серверам;
* вирусы, «трояны», «черви» и другое вредоносное программное обеспечение, способные нанести вред ПО и информационным системам;
* средства взлома сигнализации и различных других защитных систем здания офиса компании;
* ПО для подбора паролей и взлома защищённых информационных объектов и т.д.

**Разработка мер защиты**

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно-техническом уровнях.

**Процедурный уровень**

Можно выделить следующие группы процедурных мер:

* **управление персоналом:**

1. для каждой должности существуют квалификационные требования по информационной безопасности. Таким образом, необходимо ограничить доступ и предоставить достаточно высокий уровень доступа определённым работникам компании.
2. весь рабочий персонал должен быть проинструктирован о возможных угрозах информационной безопасности фирмы;
3. каждый работник должен изучить меры безопасности теоретически и на практике;
4. отдельным работникам доступ к важным бумагам и информационным объектам должен быть ограничен;
5. организация хранения конфиденциальной информации на специальных промаркированных магнитных носителях;
6. организация регламентированного доступа пользователей к работе на ЭВМ, средствам связи и к хранилищам носителей конфиденциальной информации;
7. постоянный контроль за соблюдением установленных требований по защите информации.

* **физическая защита:**

1. установка охранных и охранно-пожарных систем в офисе компании;
2. установка средств охранного телевидения: камеры, экраны наблюдения, зеркальные щиты и т.д.;
3. установка охранного освещения;
4. установка, где присутствует необходимость, ограждений и физической изоляции;
5. установка запирающих устройств на дверные проёмы и двери;
6. установка систем контроля доступа: карты доступа, средства опознавания по отпечаткам пальцев, голосу, почерку, геометрии рук;
7. установка радио-лучевых, радиоволновых и инфракрасных защитных систем: антенн, глушителей и т.д.

* **поддержание работоспособности:**

1. проведение своевременных ревизий защитного оборудования офиса;
2. ежедневный контроль исправности защитного оборудования;

* **реагирование на нарушения режима безопасности:**

1. необходимо назначить несколько рабочих лиц, отвественных за безопасность информационной системы компании;
2. разделение локальных сетей офиса компании на сегменты и своевременной их отключение;
3. необходимо стремится к скорейшей локализации инцидента и выявлению нарушителя;
4. активизация всех защитных систем компании и блокировка доступа ко всем объектам информационной системы;

* **планирование восстановительных работ:**

1. разработка стратегий восстановительных работ;
2. определение перечня возможных аварий;
3. обеспечение информационной системы компании избыточными мерами резервного копирования, хранения копий информации и представления информации в разных видах;
4. заключение соглашений с поставщиками информационных услуг по защите информации;
5. проверка и практическая реализация стратегии восстановительных работ;
6. определение средств штатной работы офиса компании в случае критической ситуации и прорабатывание с персоналом сценариев развития внештатных ситуаций.

**Программно-технический уровень**

Основой программно-технического уровняявляются следующие механизмы безопасности:

* **идентификация и аутентификация пользователей:**

1. установка средств идентификации/аутентификации пользователей (паролей, средств двухфакторной аутентификацией и т.д.);
2. предоставление необходимости подтвердить свою личность в случае подозрительной деятельности пользователя;
3. предоставление необходимости смены пароля или иных средств идентификации/аутентификации в случае длительного их использования или подозрительной деятельности пользователя;

* **управление доступом:**

1. предоставление работникам риэлтерской компании средств контроля доступа за деятельностью пользователей;
2. ограничение доступа к отдельным составляющим информационной системы для отдельных пользователей;
3. полное ограничение и предоставление необходимости в подтверждении прав доступа для пользователей, проявляющих подозрительную активность;

* **протоколирование и аудит:**

1. контроль за действиями пользователя во время пользования информационной системой;
2. протоколирование и ревизия действий пользователей;
3. постоянный аудит работоспособности защитных устройств и систем отдельных информационных объектов;
4. проведение анализа защищённости объектов и процедур по проверке отказоустойчивости защитных систем;

* **криптография:**

1. обеспечение надёжных систем шифрования данных;
2. постоянная разработка и модификация алгоритмов шифрования;
3. аудит секретности шифровальных систем и защищённости алгоритмов шифрования от несанкционированного доступа;

* **экранирование:**

1. установка средств экранирования информационных каналов;
2. мониторинг информационных систем на факт наличия источников утечки информации;
3. установка телекоммуникационных и электроакустических систем экранирования;
4. установка защитного антивирусного программного обеспечения на объекты информационной системы компании.

* **обеспечение высокой доступности:**

1. структуризация элементов информационной системы;
2. апробирование всех процессов и составных частей информационной системы;
3. автоматизация процессов информационной системы;
4. обеспечение модульности архитектуры информационной системы;
5. ориентация на простоту решений при разработке архитектуры информационной системы.

**Выводы**

Правильное составление содержания политики информационной безопасности является важным аспектом построения успешной и защищённой компании. Политика информационной безопасности компании содержит основные инструкции по установке, регулированию и контролю защитных средств.

Политика информационной безопасности помогает основательно подготовить фирму к непредвиденным ситуациям и быстро решить возникшую проблему. Также, она содержит инструкции по информационной безопасности для рабочего персонала риэлтерской компании и может использоваться как пособие для консультации её работников по вопросам данной сферы.

Политика информационной безопасности является одним из звеньев в последовательном ряде решений информационной безопасности, указанное обстоятельство гарантирует должностным лицам и учредителям компании, что система информационной безопасности, построенная в соответствии с концепцией, будет управляемой, экономически обоснованной и соответствующей требованиям бизнеса.

**Ресурсы**

<https://www.businessstudio.ru/articles/article/effektivnaya_model_agentstva_nedvizhimosti_strateg/> - структура риэлтерской компании.

<https://studbooks.net/1838528/ekonomika/organizatsionnaya_struktura_sistema> - структура риэлтерской компании.

<http://g-kvartal24.ru/politika-bezopasnosti/> - политика безопасности риэлтерской компании

<https://studylib.ru/doc/4112870/1.2.-analiz-riskov-informacionnoj-bezopasnosti> - анализ рисков информационной безопасности(ИБ) на реальном примере.

<https://ssbb.ua/proslushka-obnaruzhenie-zashhita/poisk/sposobyi-obespecheniya-informatsionnoy-bezopasnosti/> - методы обеспечения ИБ

<https://searchinform.ru/analitika-v-oblasti-ib/Issledovaniya-v-oblasti-ib/metody-obespecheniya-informatsionnoj-bezopasnosti/> - методы обеспечения ИБ