Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ

УНИВЕРСИТЕТ»

Разработка политики информационной

безопасности маркетинговой компании

Подготовил:

студент 3 курса 6 группы ФИТ

Соколовский Д.В.

Минск 2023

**Оглавление**

[**Введение** 3](#_Toc63810197)

[**1 Актуальность политики безопасности** 5](#_Toc63810198)

[**2 Основные определения** 7](#_Toc63810199)

[**3 Описание структуры предприятия** 9](#_Toc63810200)

[**4 Главные угрозы** 13](#_Toc63810201)

[**5 Угрозы, риски, уязвимости** 15](#_Toc63810202)

[**6 Разработка мер защиты** 19](#_Toc63810203)

[**Вывод** 22](#_Toc63810204)

# **Введение**

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.

Под информационной безопасностью (далее ИБ) следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Не секрет, что дела с обеспечением ИБ в большинстве белорусских компаний обстоят не недостаточно хорошо. Общение со специалистами и результаты статистических исследований только укрепляют это мнение. Множество организаций регулярно терпят убытки, связанные с нарушением ИБ, не способны оценить ущерб или хотя бы обнаружить многие из этих рушений. Тем более речь о реализации в современных организациях полноценной процедуры управления рисками ИБ не идет. Большинство специалистов-практиков даже не берутся за эту "непосильную" задачу, предпочитая руководствоваться при решении проблем ИБ исключительно собственным опытом и интуицией. Убытки от нарушений ИБ могут выражаться в утечке конфиденциальной информации, потере рабочего времени на восстановление данных, ликвидацию последствий вирусных атак и т.п. Убытки могут также выражаться и вполне конкретными "круглыми суммами", например, когда дело касается мошенничества в финансовой сфере с использованием компьютерных систем. ИБ можно обеспечить только в случае комплексного подхода. Разрешение каких-то отдельных вопросов (технических или организационных) не решит проблему ИБ в целом, а вот как раз этого главного принципа большинство сегодняшних руководителей не понимают и вследствие чего являются жертвами злоумышленников.

Политика информационной безопасности (далее ПИБ) организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Адекватный уровень информационной безопасности в состоянии обеспечить только комплексный подход, предполагающий планомерное использование как программно-технических, так и организационных мер защиты на единой концептуальной основе. При этом организационные меры играют первостепенную роль. Эффективность самых сложных и дорогостоящих механизмов защиты сводится к нулю, если пользователи игнорируют элементарные правила парольной политики, а сетевые администраторы нарушают установленные процедуры предоставления доступа к ресурсам корпоративной сети. В основе организационных мер защиты информации лежат политики безопасности. От их эффективности в наибольшей степени зависит успешность любых мероприятий по обеспечению информационной безопасности.

# **Актуальность политики безопасности**

В настоящее время компаниям просто необходимо использовать информационные ресурсы и технологии. Сейчас тема информационной безопасности очень актуальна для маркетинговых компаний.

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.

Так основными целями политики ИБ являются защита информации учреждения и обеспечение его эффективной работы при осуществлении деятельности.

Общее руководство обеспечением ИБ маркетинговой компании должен осуществлять ее директор.

Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет сотрудник, отвечающий за функционирование автоматизированной системы и выполняющий функции администратора информационной безопасности (далее администратор информационной безопасности).

Сотрудники кампании обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования политики безопасности и других документов ИБ.

Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная система управления ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для учреждения.

Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия возможным атакам, а также программно-технических и организационных решений, позволяющих минимизировать возможные потери от технических аварий и ошибочных действий персонала.

Задачами разработки ПИБ являются:

1. описание центра системы управления информационной безопасностью маркетинговой компании;
2. реализация антивирусной защиты;
3. информирование об инцидентах в области ИБ;
4. политика учетных записей;
5. политика предоставления доступа к информационному ресурсу;
6. управление доступом к средствам вычислительной техники, программам и данным;
7. проведение ремонтных и восстановительных работ.

# **Основные определения**

Информационная (информационно-вычислительная) система – это организационно упорядоченная совокупность документов, технических средств и информационных технологий, реализующая информационные (информационно-вычислительные) процессы.

Информационные процессы – процессы сбора, накопления, хранения, обработки (переработки), передачи и использования информации.

Информационные ресурсы – отдельные документы или массивы документов в информационных системах.

Информационные активы – информационные системы, информационные средства, информационные ресурсы.

Информационные средства – программные, технические, лингвистические, правовые, организационные средства, используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Администратор информационной безопасности – сотрудник учреждения, осуществляющий контроль за обеспечением защиты информации, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Анализ риска – систематическое использование информации для определения источников и оценки риска.

Объект – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).

Субъект – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

Доступ – специальный тип взаимодействия между объектом и субъектом, в результате которого создается поток информации от одного к другому.

Атака – попытка несанкционированного преодоления защиты системы.

Несанкционированный доступ (НСД) – доступ к информации, устройствам ее хранения и обработки, а также к каналам передачи, реализуемый без ведома (санкции) владельца и нарушающий тем самым установленные правила доступа.

Защита информации – организационные, правовые, программно-технические и иные меры по предотвращению угроз информационной безопасности и устранению их последствий.

Безопасность информации – защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Безопасность любого ресурса информационной системы складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности, также могут быть включены другие, такие как аутентичность, подотчетность, надежность; или иначе: информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности информации или средств ее обработки: конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия; целостность компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права; целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени; доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

# **Описание структуры предприятия**

Эффективность управления деятельностью зависит оттого, насколько грамотно сформирована организационная структура управления и насколько она соответствует цели деятельности организации.

Маркетинг для организации должен представлять управленческий процесс, нацеленный на увеличение доходов собственников компании посредством создания устойчивых отношений с прибыльными потребителями и защиты этих отношений устойчивыми отличительными преимуществами. Известный американский специалист по менеджменту П. Друкер писал: «Необходимо поставить специалиста по маркетингу в начале, а не в конце производственного цикла и интегрировать маркетинг в каждую фазу бизнеса... Маркетинг должен оказывать воздействие на проектирование, планирование выпуска, экономический анализ, равно как и на распределение, сбыт и предоставление услуг по продукту».  Иными словами можно сказать, что фирма достигла современного уровня маркетинга только тогда, когда маркетинг стал основой всей ее деятельности.

Основные задачи и функции маркетинга в компании можно представлены в  таблице 3.1.

Таблица 3.1. – Функции и задачи маркетингового отдела

|  |  |
| --- | --- |
| Функции | Задачи |
| Формирование рыночной стратегии фирмы | * Анализ и прогнозирование: потребностей и спроса; конъюнктуры рынка; факторов конкурентного преимущества фирмы; качества и ресурсоемкости аналогичных товаров конкурентов. * Анализ связей фирмы с внешней средой * Прогнозирование воспроизводственных циклов товаров фирмы. * Анализ и прогнозирование организационно-технического уровня производства конкурентов и фирмы. * Прогнозирование: объемов рынков по сегментам; лимитных цен на будущие товары; конкурентоспособности будущих товаров на конкретных рынках. * Разработка и экономическое обоснование мероприятий, направленных на обеспечение конкурентоспособности будущих товаров. * Окончательный выбор целевых рынков на  год * Разработка нормативов конкурентоспособности будущих товаров. |
| Реализация концепции маркетинга | * Согласование структуры и содержания системы менеджмента фирмы. * Участие в проектировании организационной и производственной структуры фирмы. * Участие в разработке положений и должностных инструкций фирмы. * Входной маркетинговый контроль (на соблюдение концепции маркетинга) всей нормативно-методической и технической документации, разрабатываемой фирмой. * Разработка, согласование и утверждение руководством фирмы Плана мероприятий по реализации концепции маркетинга в деятельности фирмы на период. * Участие в анализе внешнеэкономической деятельности фирмы * Согласование цен на выпускаемые товары * Согласование долгосрочных контрактов и договоров. Установление схемы обратной связи по стадиям жизненного цикла товаров |
| Стратегическая реклама и стимулирование сбыта товара | * Определение целей рекламы * Определение методов, правил и средств рекламы * Формирование стратегии стимулирования сбыта товаров и роста прибыли |
| Обеспечение маркетинговых исследований | * Разработка структуры службы маркетинга фирмы * Информационное обеспечение и создание нормативной базы маркетинговых исследований * Кадровое обеспечение исследований * Обеспечение техническими средствами * Обеспечение внутренних и внешних связей службы маркетинга фирмы |

Из данной таблицы можно выделить следующие основные задачи маркетинговой деятельности:

        исследование, анализ и оценка потребностей реальных и потенциальных потребителей;

        маркетинговое обеспечение разработки новых товаров и услуг фирмы;

        анализ, оценка и прогнозирование состояния и развития рынков, включая исследование деятельности конкурентов;

        формирование ассортиментной политики фирмы;

        разработка ценовой политики фирмы;

        сбыт продукции; коммуникации.

**Организационная структура**

Можно выделить следующие виды организационных структур службы маркетинга.

Функциональная организация – организационная структура управления, в которой деятельность специалистов в подразделении маркетинга организована, исходя из функций маркетинга, которые они выполняют (маркетинговые исследования, сбыт, реклама и т.д.). Структура функционального типа целесообразна для предприятий, у которых количество товаров и рынков невелико.

Функциональная организация является наиболее простой, однако ее эффективность падает по мере роста номенклатуры выпускаемых продуктов и расширение числа рынков сбыта. Это обусловлено тем, что в функциональной организации отсутствует лицо (кроме самого руководителя подразделения маркетинга), отвечающее за маркетинг отдельных продуктов в целом или за маркетинговую деятельность на определенных рынках. Данную структуру характеризует слабая гибкость стратегии, так как она ориентирована на достижение текущей эффективности, а не на внедрение нововведений.

Товарная организация. Для предприятий, выпускающих большое количество разнообразных товаров, требующих специфических условий производства и сбыта, целесообразна организация маркетинга по товарному принципу. Данная структура имеет ряд достоинств. Управляющий по определенному товару координирует весь комплекс маркетинга по этому товару и быстрее реагирует на возникающие на рынке проблемы. Такая маркетинговая структура обходится дороже, чем функциональная, поскольку требуется больше расходов по оплате труда из-за увеличения количества работников, поэтому организация службы маркетинга по товарному принципу распространена только на крупных предприятиях, где объем продаж каждого товара достаточен для того, чтобы оправдать неизбежное дублирование в работе.

Рыночная организация. Для предприятий, продающих свою продукцию на разных рынках, где наблюдаются неодинаковые товарные предпочтения, а товары требуют специфического обслуживания, целесообразна организация маркетинга по рынкам.

Региональная (географическая) организация. На предприятиях, выпускающих продукцию, покупаемую многими регионами, в каждом из которых целесообразно учитывать специфику потребления этой продукции, маркетинговые структуры могут быть организованы по регионам.

Функционально-товарная организация – организационная структура управления маркетингом, в которой функциональные маркетинговые службы предприятия вырабатывают и координируют осуществление некоторых единых целей для предприятия. В то же время за разработку и реализацию стратегии и планов маркетинга для определенного продукта или группы продуктов отвечает управляющий продуктом. Он также формулирует для функциональных маркетинговых служб предприятия задания в области маркетинга определенных товаров и контролирует их выполнение.

Товарно-рыночная организация реализуется, как правило, в матричной форме, когда имеются как управляющие отдельными товарами, так и управляющие отдельными рынками. Продуктовые управляющие планируют объем продаж и прибыль для своих продуктов, контактируют при этом с управляющими отдельными рынками с целью определения возможного объема продаж. Управляющие отдельными рынками, в свою очередь, отвечают за развитие прибыльных рынков для существующих и потенциальных товаров организации. Применяются организациями, выпускающими разные продукты, реализуемые на многих, сильно отличающихся рынках. Достоинством данной организации маркетинга является то, что уделяется внимание каждому продукту и каждому рынку. Однако, данная организация увеличивает управленческие затраты, не обладая достаточной организационной гибкостью и порождает конфликты.

# **Главные угрозы**

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

* антропогенные,
* техногенные,
* природные.

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как 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. Источники угроз могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.
* Внутренние угрозы могут проявляться 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.

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).

Специфические угрозы безопасности:

1. возможность отключения электричества, что приведет к сбою незавершенных операций и потере данных;
2. угроза возникновения неправильной адресации пакетов;
3. угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ, и попадания в офис и на склад предметов, способных нанести ущерб;
4. угроза доступа в эксплуатационный отдел, могут быть нарушены эксплуатационные планы;
5. угроза доступа в ИТ-отделе.

# **Угрозы, риски, уязвимости**

Оценка информационных рисков компании выполняется по следующим основным этапам:

– идентификация и количественная оценка информационных ресурсов, значимых для работы компании;

– оценивание возможных угроз;

– оценивание существующих уязвимостей;

– оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые уязвимые информационные ресурсы компании подвергаются риску, если по отношению к ним существуют какие-либо угрозы.

При этом информационные риски зависят от:

– показателей ценности информационных ресурсов;

– вероятности реализации угроз для ресурсов;

– эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании.

При оценивании рисков учитываются: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть определены как количественными методами, например, при определении стоимостных характеристик, так и качественными, например, учитывающими штатные или чрезвычайно опасные нештатные воздействия внешней среды.

Условная численная шкала для численной оценки рисков от несанкционированного доступа (НСД) к информационным ресурсам маркетинговой компании приведена в таблице 5.1.

Таблица 5.1 – Условная численная шкала для оценки ущерба маркетинговой компании от НСД

|  |  |
| --- | --- |
| 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 |

Продолжение таблицы 5.1

|  |  |
| --- | --- |
| 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 |

Возможность реализации угрозы оценивается вероятностью ее реализации в течение заданного отрезка времени для некоторого ресурса компании.

При этом вероятность того, что угроза реализуется, определяется следующими основными показателями:

– привлекательностью ресурса, используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

– возможностью использования ресурса для получения дохода, также используется при рассмотрении угрозы от умышленного воздействия со стороны человека;

– техническими возможностями реализации угрозы, используется при умышленном воздействии со стороны человека;

– степенью легкости, с которой уязвимость может быть использована.

Существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

* по расположению источника угроз (внешние, внутренние):
* источниками внутренних угроз являются:
* сотрудники;
* программное обеспечение;
* аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

Ошибки пользователей и системных администраторов; нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации; ошибки в работе программного обеспечения; 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 аспекту информационной безопасности, на который направлены угрозы:

* угрозы [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) (неправомерный доступ к информации);
* угрозы [целостности](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (неправомерное изменение данных);
* угрозы [доступности](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы).

Для фирмы характерно хозяйственное внутриорганизационное управление, так как агентство не является муниципальным и относится к сфере дополнительных услуг. Также в фирме имеет место техническое управление, применяемое для технической поддержки сайта и электронного документооборота.

Шкала вероятности того, что угроза будет реализована, приведена в таблице 5.2.

Таблица 5.2 – Вероятностно-временная шкала реализации несанкционированного доступа 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 |

С помощью приведенных выше таблиц можно рассчитать риски, которым могут быть подвержены компоненты системы. На этапе анализа таблицы риски задаются максимально допустимым уровнем (порогом) – значением 0,5.

Таблица 5.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| Хищение личных данных отдельного клиента сотрудником компании | 1 | 0,1 | 0,1 |
| Хищение клиентской базы сотрудником компании | 2 | 0,1 | 0,2 |
| Хищение личных данных отдельного клиента человеком внешним для компании | 2 | 0,1 | 0,2 |
| Хищение клиентской базы человеком внешним для компании | 2 | 0,1 | 0,2 |
| Удаление базы данных клиентов с главного компьютера | 1 | 0,1 | 0,1 |
| Распространение исследований компании | 2 | 0,1 | 0,2 |
| Ненадежность программ, используемых компании для ведения внутренних процессов | 2 | 0,1 | 0,2 |
| Аппаратные ошибки в настройке локальной сети компании | 3 | 0,1 | 0,3 |
| Программные ошибки в настройке локальной сети компании | 2 | 0,1 | 0,2 |
| Недостаточная квалификация сотрудников | 3 | 0,1 | 0,3 |

# **Разработка мер защиты**

Информационная безопасность маркетинговой 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 маркетинговой компании должно быть организовано ознакомление персонала с внутренними нормативными документами.

Служба безопасности маркетинговой 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 маркетинговой 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 маркетинговой 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):

* 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 маркетинговой 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 клиентов, в первую очередь, привилегированных;
* применение систем криптографической защиты информации;
* обеспечение безотказной работы аппаратных средств;
* мониторинг состояния критичных элементов информационной системы.

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

# **Вывод**

Приведенные меры по защите информации являются примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения информационной безопасности для проведения специальных тестов и экспериментов.

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 главных 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.

Так же, 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.