Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Разработка и внедрение политики безопасности маркетинговой компании

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Содержание**

[**ВВЕДЕНИЕ** 3](#_Toc128469411)

[**1. Объект защиты** 4](#_Toc128469412)

[**1.1. Описание структуры организации** 4](#_Toc128469413)

[**1.2. Внутренняя структура организации** 4](#_Toc128469414)

[**1.3. Обзор объектов и субъектов информационных отношений** 6](#_Toc128469415)

[**1.3.1. Объекты информационных отношений** 6](#_Toc128469416)

[**1.3.2. Субъекты информационной безопасности** 6](#_Toc128469417)

[**2. Основные угрозы и их источники** 7](#_Toc128469418)

[**2.1. Естественные угрозы** 7](#_Toc128469419)

[**2.2. Искусственные угрозы** 7](#_Toc128469420)

[**2.3. Преднамеренные угрозы** 7](#_Toc128469421)

[**2.4. Непреднамеренные угрозы** 8](#_Toc128469422)

[**2.5. Внешние угрозы** 8](#_Toc128469423)

[**2.6. Внутренние угрозы** 8](#_Toc128469424)

[**3. Оценка угроз, рисков и уязвимостей** 9](#_Toc128469425)

[**3.1. Оценка ущерба организации** 9](#_Toc128469426)

[**3.2. Оценка вероятности реализации угрозы** 10](#_Toc128469427)

[**3.3. Оценка рисков** 10](#_Toc128469428)

[**4. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов** 12](#_Toc128469429)

[**4.1. Методы средств защиты** 12](#_Toc128469430)

[**4.1.1. Несанкционированный доступ преступных группировок** 12](#_Toc128469431)

[**4.1.2. Несанкционированный доступ третьих лиц на рабочее место** 13](#_Toc128469432)

[**4.1.3. Санкционированный доступ сотрудников** 13](#_Toc128469433)

[**4.1.4. Человеческий фактор** 13](#_Toc128469434)

[**ЗАКЛЮЧЕНИЕ** 14](#_Toc128469435)

# **ВВЕДЕНИЕ**

В современном мире хранение и использование информации имеет важную значимость. Как в маленьких, так и в больших организациях и учреждениях информация необходима для нормального функционирования. Так, лучшим средством для обеспечения надёжности и безопасности информации является разработка политики безопасности.

Политика информационной безопасности – 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.

Разработка политики информационной безопасности является необходимым фактором для функционирования маркетинговой компании. Компания, используя различные средства хранения информации, содержит множество конфиденциальных данных как о клиентах, так и о внутренних делах компании. Нарушение информационной безопасности, утечка, потеря хранящихся данных может привести к необратимым последствиям.

В связи с этим необходимо выделить следующие цели и задачи для разработки политики информационной безопасности:

Цели:

* сохранение конфиденциальности критичных информационных ресурсов
* обеспечение непрерывности доступа к информационным ресурсам
* защита целостности информации
* предотвращение или снижения ущерба от угроз и рисков

Задачи:

* разработка концепций, стандартов, инструкций, процедур и планов мероприятий
* описание структуры маркетинговой компании
* обзор всех возможных объектов и субъектов информационных отношений
* выявление основных угроз и их источников
* оценка угроз, рисков и уязвимостей

1. **Объект защиты**
   1. **Описание структуры организации**

В организациях для распределения полномочий и обязанностей существует организационная структура. Распределение полномочий и обязанностей позволяет наиболее эффективность достичь целей организации, целесообразно и продуктивность распределять усилия сотрудников и подразделений, обеспечивать взаимозаменяемость сотрудников.

Для организации деятельности предприятие формирует организационную структуру, в рамках которой персонал выполняет предназначенные ему функции, совокупное исполнение которых дает возможность достичь целей управления.

Организационная структура определяется следующими характеристиками:

* Функции;
* Организационные звенья;
* Иерархия.

Существует три типа организационных структур:

* Функциональная оргструктура основана на разделении всех звеньев по функциональному признаку;
* В дивизиональной структуре принципиально важным является выделение подразделений по продуктовому признаку, а функция используется только как признак группировки;
* Матричная структура, идея которой заключается в том, чтобы выделить институт менеджеров, ответственных за проект или работу с клиентом, а уж они для решения своих задач смогут привлечь специалистов из любых подразделений.
  1. **Внутренняя структура организации**

Рассмотрим подробнее внутреннюю структуру маркетинговой компании, её отделы.

Генеральный директор – главный орган управления маркетинговой компании, который должен играть ведущую роль в переориентации компании на интересы потребителей и спрос на рынке.

Договорный отдел – выполняет расчёт и проверку стоимости работ и готовит договора с заказчиками и субподрядчиками.

Отдел сбыта – отдел, который занимается формированием сбытовой политики. К его функциям относятся разработка методов поощрения покупок, воздействие на структуру, скорость и объемы продаж, реализация своей продукции в целях получения большой денежной выручки.

Рекламный отдел – отдел, который занимается проведением определённых мероприятий в сфере коммуникаций и реализацией выбранной маркетинговой стратегии.

Отдел исследования рынка и цен – отдел, который выявляет и изучает потребительский спрос, собирает и систематизирует экономическую и коммерческую информацию о возможных рынках сбыта, выявляет новых рыночных ниш.

Отдел контроля маркетинга – отдел, который занимается регулярным и комплексным изучением маркетинговой деятельности компании: сравнивает запланированные результаты с реальными показателями, выявляет отклонение от основных задач.

Финансовый отдел – отдел, который отвечает за управление финансовыми аспектами компании и обеспечение ее финансовой стабильности.

Юридический отдел – отдел, который занимается юридическим сопровождением деятельности организации: правовое сопровождение бизнеса, составление договоров, участие в судебных разбирательствах.

IT-отдел – отдел, который занимается обеспечением работоспособности и поддержкой информационной инфраструктуры предприятия. Он отвечает за планирование, установку, настройку, обслуживание и модернизацию всех компьютерных систем, программного обеспечения, сетей и коммуникационного оборудования организации.

Структура маркетинговой организации представлена на рисунке 1.1

****

Рисунок 1.1 – Структура маркетинговой компании

* 1. **Обзор объектов и субъектов информационных отношений**

В данном разделе будут рассмотрены все основные объекты и субъекты информационных отношений, для защиты который должны быть приняты меры по обеспечению информационной безопасности.

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.

* + 1. **Объекты информационных отношений**

Обеспечение безопасности объектов информационных отношений при разработке политики безопасности является одной из основных задач. В маркетинговой компании можно выделить следующие объекты информационной безопасности:

* Аппаратные средства: комплектующие, блоки бесперебойного питания, офисное оборудование, сетевое оборудование, средства коммуникаций, периферийная техника, диски, дискеты, материалы;
* программные средства: электронные таблицы, прикладные пакеты, средства мультимедиа, средства проектирования ПО;
* информационные продукты, базы данных;
* информационные услуги: консалтинговые, учебные, внедренческие, сопроводительное, ремонтные, посреднические, торговые, рекламные, интерактивные, телекоммуникационные;
  + 1. **Субъекты информационной безопасности**

Не менее важным является обеспечение безопасности субъектов информационных отношений при разработке политики безопасности. В маркетинговой компании можно выделить следующие объекты информационной безопасности:

* сотрудники организации, имеющие доступ к информации
* пользователи услуг маркетинговой компании
* рыночные посредники
* аппаратные средства: компьютеры.

1. **Основные угрозы и их источники**

Одной из главных целей разработки политики информационной безопасности является классификациях всех возможных типов угроз, а также оценка рисков возникновения этих угроз.

Угрозы безопасности можно разделить на внутренние и внешние, преднамеренные и непреднамеренные, искусственные и естественные. Наиболее частой целью для утечки в маркетинговой компании является база данных клиентов

* 1. **Естественные угрозы**

К естественны угрозам относятся вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.

К естественным угрозам в маркетинговой компании можно отнести электрические, магнитные, электромагнитные и ионизирующие помехи

* 1. **Искусственные угрозы**

Искусственные угрозы – угрозы, вызванные деятельностью человека. К искусственным угрозам можно отнести следующее;

* несанкционированные доступ к программным средствам, базам данных третьими лицами или сотрудниками компании;
* Заражение компьютерных систем компании вирусами сотрудниками либо иными лицами;
* Доступ к программный средствам, базам данных сотрудниками, не имеющие достаточной квалификации;
* Человеческий фактор.
  1. **Преднамеренные угрозы**

Преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т. п.) действия легально допущенных к информационным ресурсам пользователей (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), которые приводят к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности компонентов информационной системы. К преднамеренным угрозам можно отнести следующее:

* Деятельность преступных организаций, формирований или же отдельных лиц со злым умыслом;
* Ошибки, допущенные при разработке компонентов информационной системы и системы её защиты, ошибки в программном обеспечении.
  1. **Непреднамеренные угрозы**

Непреднамеренные (ошибочные, случайные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований безопасности информации и другие действия сотрудников компании (в том числе сотрудников, отвечающих за обслуживание и администрирование компонентов корпоративной информационной системы), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности маркетинговой компании.

К большинству непреднамеренных угроз относится к человеческому фактору. Человеческий фактор – это совокупность специфических для человека физических, психических и поведенческих свойств, которые могут повлиять на его надёжность и работоспособность в некоторых ситуациях.

* 1. **Внешние угрозы**

Внешние дестабилизирующие факторы влияют:

На программные средства (ПС):

* неквалифицированные пользователи;
* несанкционированный доступ к ПС с целью модификации кода.

На аппаратные средства:

* электромагнитные и ионизирующие излучения;
* недостаточная квалификация обслуживающего персонала.
  1. **Внутренние угрозы**

Внутренние дестабилизирующие факторы влияют:

На программные средства (ПС):

* некорректный исходный алгоритм;
* неправильно запрограммированный исходный алгоритм.

На аппаратные средства (АС):

* системные ошибки при постановке задачи проектирования
* отклонения от технологии изготовления комплектующий изделий и АС в целом
* нарушение режима эксплуатации, вызванное состоянием АС.

1. **Оценка угроз, рисков и уязвимостей**

Риск – вероятность возникновения негативного события, которое нанесёт ущерб организации, так же можно представить как произведение ущерба угрозы на вероятность её возникновения.

При оценке риска учитывается следующее:

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

Потенциальное негативное воздействие на деятельность организации можно определять количественно, качественно или их комбинацией.

По показателю негативного воздействия можно определить наиболее значимые угрозы и на основе этого подготавливать приоритетные меры, методы и средства защиты информационных ресурсов.

Так, одним из вариантов является создание шкалы оценки ущерба для компании.

* 1. **Оценка ущерба организации**

Для оценки возможного ущерба маркетинговой компании создаётся численная шкала с величиной ущерба от 0 до 5. Благодаря численной шкале можно просчитать риски для каждой потенциальной угрозы. Численная шкала предоставлена в таблице 3.1.

Таблица 3.1 – Численная шкала оценки ущерба маркетинговой компании

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб компании |
| 1 | Ущерб от атаки есть, но он незначителен, основные операции и положение компании на рынке не затронуты |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время компания терпит убытки, но его положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные потери на рынке и в прибыли. От компании уходит ощутимая часть клиентов |
| 4 | Потери очень значительны, компания на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы |
| 5 | Компания прекращает существования |

* 1. **Оценка вероятности реализации угрозы**

Помимо оценивая оценивания ущерба, так же необходимо учитывать и вероятность их происшествия. Вероятность того, что угроза реализуется, определяется на основе следующих факторов:

* 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.

Численная шкала реализации угрозы предоставлена в таблице 3.2.

Таблица 3.2 – Численная шкала реализации угроз

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события |
| 0 | Данный вид угрозы 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 |

* 1. **Оценка рисков**

На основании таблиц 3.1 и 3.2 можно составить таблицу рисков. На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем, например 5.

Далее в каждой строке таблица проверяется, превышен ли порог. Если превышен, то данная атака должна рассматриваться с точки зрения одной из первоочередных целей разработки политики безопасности.

На таблице 3.3 предоставлена оценка рисков.

Таблица 3.3 – таблица оценки рисков маркетинговой компании

|  |  |  |  |
| --- | --- | --- | --- |
| Описание угрозы | Ущерб | Вероятность | Риск |
| Устаревание оборудования | 2 | 0,1 | 0,2 |
| Несанкционированный доступ хакеров к личным данным клиентов компании | 4 | 0,1 | 0,4 |
| Заражение компьютеров систем вирусами сотрудниками компании | 2 | 0,2 | 0,4 |
| Перебои в работе электричества в следствии несанкционированного доступа | 3 | 0,2 | 0,6 |
| Несанкционированный доступ и копирование личных данных сотрудниками компании | 4 | 0,2 | 0,8 |
| Непреднамеренные ошибки из-за человеческого фактора | 1 | 0,5 | 0,5 |
| Доступ к данным компании неквалифицированными сотрудниками | 1 | 0,3 | 0,3 |
| Проникновенные третьих лиц | 3 | 0,2 | 0,6 |
| Нарушение режима эксплуатации аппаратных средств, в следствии чего те ломаются | 2 | 0,2 | 0,4 |
| Ошибки в алгоритмах ПО, которые влияют на их работу в целом | 1 | 0,4 | 0,4 |
| DDOS веб-сайта компании | 3 | 0,2 | 0,6 |
| Создание поддельных копий веб-сайта компании | 2 | 0,3 | 0,6 |
| Использование адресов почты, схожих с адресом компании в целях получения личных данных клиентов | 3 | 0,3 | 0,6 |
| Кража данных от почт сотрудников | 4 | 0,1 | 0,4 |
| **Итого** |  |  | **7** |

По итогам данных из таблицы оценки рисков, оценка рисков превышает допустимый уровень. Это означает, что необходимо разработать дополнительные меры по уменьшению рисков возникновения угроз.

1. **Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

В данном разделе будут рассмотрены меры, методы и средства, которые необходимо применять для снижения вероятностей или их полного устранения.

В связи с этим можно выделить следующее:

* План обучения персонала разработанной политике информационной безопасности;
* Правила и принципы работы с средствами хранения данных;
* Алгоритмы действий по организации информационной безопасности;
* Конкретные действия для защиты информации;
* Алгоритмы действий на случаи восстановительных работ
* Алгоритмы действий на случаи нарушения политики информационной безопасности.
  1. **Методы средств защиты**

В данном разделе будут рассмотрены те или иные методы по обеспечению требуемого уровня защищённости информационных ресурсов.

* + 1. **Несанкционированный доступ преступных группировок**

Несанкционированный доступ хакеров к информации и системам предприятия может привести к серьезным последствиям, таким как утечка конфиденциальных данных, нарушение работы систем и программ, а также финансовые потери. Для предотвращения этого необходимо принимать следующие меры:

* Использование защитных программ и устройств: предприятие должно использовать антивирусные программы, брандмауэры и другие средства защиты от хакерских атак;
* Авторизация и аутентификация: для доступа к системам и информации предприятия необходимо использовать механизмы авторизации и аутентификации, такие как пароли;
* Обучение сотрудников: сотрудники должны быть обучены правилам безопасности информации, методам защиты от хакерских атак и действиям в случае возникновения подозрительной ситуации.
* Мониторинг: предприятие должно проводить мониторинг своих систем и информации, чтобы обнаруживать подозрительную активность и своевременно реагировать на возможную угрозу.
  + 1. **Несанкционированный доступ третьих лиц на рабочее место**

Проникновение третьих лиц в информационные системы и данные предприятия может привести к утечке конфиденциальных данных, нарушению бизнес-процессов и значительным финансовым потерям. Чтобы предотвратить такие ситуации, необходимо принимать соответствующие меры:

* Авторизация и аутентификация: для доступа к системам и информации предприятия необходимо использовать механизмы авторизации и аутентификации, такие как пароли;
* Ограничение доступа: предприятие должно ограничить доступ к информации и системам только тем сотрудникам, которым это необходимо для выполнения своих рабочих обязанностей.
* Мониторинг: мониторинг информационных систем и данных помогает обнаруживать и реагировать на подозрительную активность, которая может указывать на попытку проникновения третьих лиц.
  + 1. **Санкционированный доступ сотрудников**

Утечка данных от сотрудников может привести к серьезным последствиям для компании, включая ущерб репутации, правовые последствия и потерю доверия клиентов. Для предотвращения таких ситуаций необходимо принимать следующие меры:

* Мониторинг: мониторинг доступа к конфиденциальной информации и контроль за действиями сотрудников помогает обнаруживать и реагировать на подозрительную активность, которая может указывать на возможную утечку данных.
* Соблюдение процедур: установление строгих правил и процедур для обработки, хранения и передачи конфиденциальной информации помогает предотвратить случайную или намеренную утечку данных. Важно также регулярно проверять соответствие сотрудников этим процедурам.
  + 1. **Человеческий фактор**

Люди могут оказывать как положительное, так и отрицательное влияние на организацию, в зависимости от своих знаний, навыков, опыта, мотивации, поведения и других факторов. Отрицательное влияние человеческого фактора может проявляться, например, в виде ошибок, несоответствий процедурам и правилам работы с информацией, несоблюдении политик безопасности, утечке конфиденциальной информации и т.д. Поэтому для обеспечения безопасности и эффективности работы организации важно принимать меры по уменьшению отрицательного влияния человеческого фактора и повышению квалификации и компетенции сотрудников.

* + 1. **Почты сотрудников и клиентов**

Атака на почту клиентов и сотрудников может иметь серьезные последствия для компании, а также для ее клиентов и партнеров. Следующие меры могут предотвратить это:

* Двухфакторная аутентификация;
* Использование антивирусного ПО;
* Оповещение клиентов о необходимости проверки правильности почты;
  + 1. **Аппаратные средства**

Аппаратные средства играют ключевую роль в функционировании компании и выход из строя может пагубно повлиять на всю её работу. Для предотвращения этого следует выделить следующие меры:

* Регулярная проверка аппаратных средств на правильное функционирование;
* Обновление аппаратных средств в случае устаревания;
* Резервная копия данных;
* Обеспечение надлежащих условий работы и хранения.
  + 1. **Веб-сайт**

Веб-сайт имеет хоть и не ключевую роль в функционировании компании, но тем не менее, важную. В случае прекращения работы веб-сайта компания может потерять часть новых клиентов. Для предотвращения этого следует выделить следующие необходимые меры:

* Использование безопасных протоколов;
* Регулярное обновление ПО;
* Защиты от DDOS-атак;
* Фильтрация ввода данных.

**ЗАКЛЮЧЕНИЕ**

Была разработана политика информационно безопасности для маркетинговой компании, которая полностью отражает концепцию, стандарты, инструкции, процедуры и планы мероприятий.

Данная политики информационной безопасности обеспечивает доступность, целостность и конфиденциальность информационных ресурсов.

Данная политика информационной безопасности реализует все поставленные задачи.

Так же данная политика информационной безопасности должна быть применена на всех уровнях маркетинговой компании с инструкциями, мерами и планами, который были предоставлены выше. Благодаря данной политике компания сможет избежать большинства угроз и сможет снизить риски их возникновения.