МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №1:**

по дисциплине «Криптографические методы защиты информации»

Тема «Разработка и внедрение политики безопасности организации или учреждения. Маркетинговая компания»

Исполнитель

студентка 3 курса группы 5 Шкода Кристина Михайловна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

Ход работы

*1. Обоснование актуальности, цели и задачи разработки ПИБ в организации (учреждении).*

*1.1. Введение.*

Быстрое развитие технологий и растущая зависимость от цифровых систем сделали информационную безопасность важнейшим аспектом современной деловой активности. Маркетинговые компании собирают, хранят и используют конфиденциальные данные клиентов, поэтому очень важно иметь комплексную политику информационной безопасности (ПИБ). Эта политика будет служить основой для защиты конфиденциальности, целостности и доступности информационных активов и обеспечивать соблюдение компанией соответствующих законов и нормативных актов.

*1.2. Актуальность.*

Маркетинговая индустрия постоянно развивается и все больше полагается на технологии, что увеличивает риск кибератак и утечки данных.

Нарушения информационной безопасности могут привести к финансовым потерям, репутационному ущербу и юридическим последствиям.

Внедрение ПИБ может помочь маркетинговой компании продемонстрировать свою приверженность защите данных клиентов и поддержанию доверия со стороны заинтересованных сторон.

*1.3. Цели*.

Создать комплексную и эффективную программу информационной безопасности, которая защищает конфиденциальность, целостность и доступность информационных активов.

Соблюдение соответствующих законов, нормативных актов и отраслевых стандартов.

Обеспечить, чтобы все сотрудники осознавали свою роль в обеспечении информационной безопасности и следовали передовому опыту.

Постоянно оценивать и повышать эффективность программы информационной безопасности.

*1.4. Задачи*.

Выявить и оценить риски для информационных активов компании.

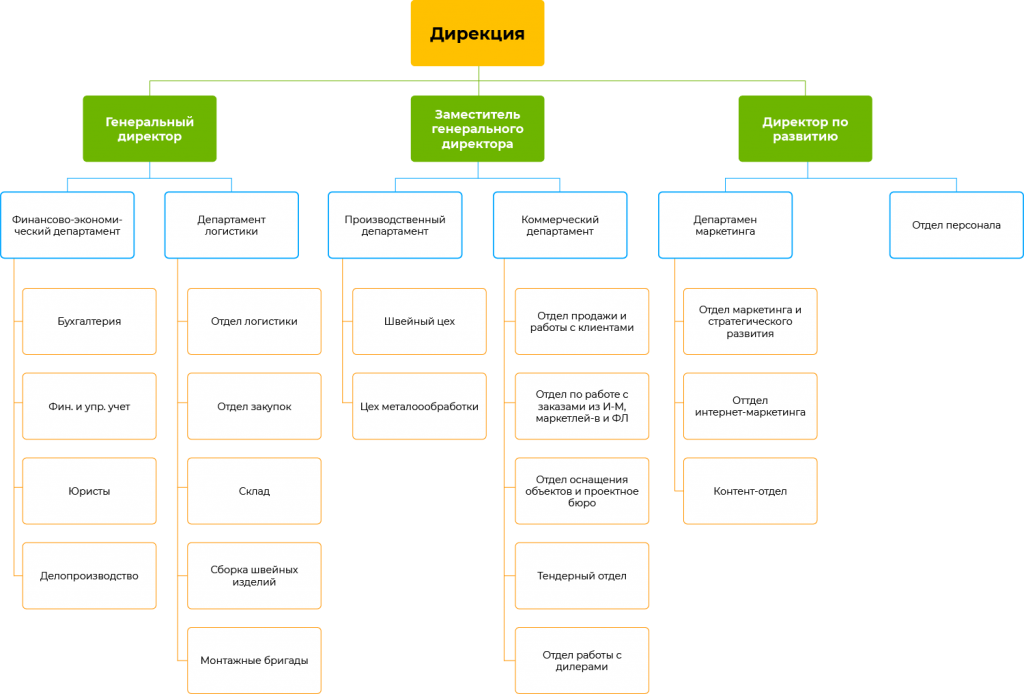
Внедрить соответствующие средства контроля для снижения рисков и обеспечения защиты конфиденциальной информации.

Обеспечить обучение и программы повышения осведомленности сотрудников о лучших практиках информационной безопасности.

Регулярно контролировать и оценивать эффективность программы информационной безопасности.

*2. Объекты защиты. Описание структуры организации (учреждения), периметра и внутренней структуры ИВС. Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности.*

Структура маркетинговой компании включает следующие основные подразделения:



Периметр маркетинговой компании — это все физические и цифровые активы, системы и информация, принадлежащие компании или используемые ею, включая компьютеры, мобильные устройства, облачные сервисы и другие цифровые носители информации.

К объектам защиты маркетинговой компании относятся:

* Коммерческие тайны компании, такие как информация о контрактах, финансовых отношениях и бухгалтерских данных.
* Коммерческая тайна клиентов и партнеров, включая информацию об их активах, имуществе, платежах и страховых случаях.
* Личные данные сотрудников компании и сотрудников клиентов, включая регистрационные номера автомобилей, водительские права и информацию о кредитных картах;
* Охраняемое помещение.

К числу субъектов маркетинговой деятельности относятся:

* Производители или обслуживающие организация (предприятие или отдельный человек, поставщики, предприятия, обеспечивающие производителя товаров необходимыми ресурсами).
* Конечные потребители (семья или человек приобретающие товары для личного использования).
* Организации - потребители.
* Специалисты по маркетингу (организации или люди).
* Сотрудники
* Посредники (оптовая и розничная торговля, брокеры, маклеры, дилеры, дистрибьюторы).
* Конкуренты - группы лиц или организаций, поставляющих на рынок аналогичные товары и услуги.

Администратор информационной безопасности отвечает за разработку и внедрение мер по защите конфиденциальной информации компании и ее клиентов, а также за обеспечение конфиденциальности, целостности и доступности этой информации. Все сотрудники должны соблюдать политику информационной безопасности компании и принимать соответствующие меры для защиты конфиденциальной информации.

Компания стремится обеспечить безопасность всей информации и будет принимать соответствующие меры для предотвращения несанкционированного доступа, модификации, раскрытия или уничтожения конфиденциальной информации. Компания также будет постоянно контролировать и оценивать свои меры информационной безопасности, чтобы обеспечить их эффективность и актуальность.

*3. Основные угрозы и их источники. Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.*

Маркетинговая компания, как и любая другая организация, уязвима для различных типов угроз, которые могут поставить под угрозу ее работу и повлиять на ее деятельность. Эти угрозы можно разделить на естественные и искусственные, преднамеренные и непреднамеренные, внешние и внутренние.

Естественные угрозы относятся к тем, которые не поддаются человеческому контролю:

* Наводнения;
* Воздействие мощных электромагнитных и электрических помех.

Искусственные угрозы относятся к тем, которые создаются людьми или технологиями:

* Несанкционированное удаленное проникновение посторонних лиц в информационную систему компании и внешние информационные и телекоммуникационные сети общего пользования;
* Недобросовестная конкуренция;
* Социальная инженерия.

Это может происходить по легальным и нелегальным каналам связи и использовать недостатки протоколов обмена, мер безопасности и удаленного доступа к ресурсам.

Преднамеренные угрозы относятся к тем, которые являются преднамеренными и запланированными:

* Фишинг через электронную почту;
* Вирусы, внедренные в файлы электронной почты или USB-носители;
* Несанкционированный доступ к веб-сайту компании.

Непреднамеренные угрозы относятся к случайным:

* Ошибки, допущенные при разработке компонентов информационной системы;
* Сбои программного обеспечения;
* Неисправности технических средств.

Внешние угрозы относятся к тем, которые возникают за пределами компании:

* Перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений;
* Подслушивание конфиденциальных разговоров и акустических сигналов работающего оборудования.

Внутренние угрозы относятся к тем, которые исходят изнутри компании:

* Разглашение информации сотрудниками;
* Несанкционированное распространение информации через поля и электрические сигналы, генерируемые оборудованием.

Компания должна знать об этих потенциальных угрозах и принимать необходимые меры для минимизации их влияния на свою деятельность. Этого можно добиться путем разработки эффективной политики информационной безопасности, обучения сотрудников методам информационной безопасности и привлечения сотрудников службы безопасности и специалистов по информационной безопасности.

*4. Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты.*

В маркетинговой компании оценка рисков должна учитывать ценность информационных ресурсов, таких как данные клиентов, маркетинговые кампании и запатентованные исследования. Необходимо оценить значимость угроз и уязвимостей для этих ресурсов, а также эффективность существующих и планируемых мер защиты. Для этого можно использовать как количественные методы, например, определить стоимость потери доступа к конкретным данным, так и качественные, например, рассмотреть вероятность возникновения различных угроз и их потенциальное влияние на деятельность компании.

При оценке вероятности реализации угрозы необходимо учитывать следующие основные показатели:

Привлекательность информационного ресурса для неавторизованных лиц, таких как конкуренты или злоумышленники, желающие извлечь выгоду из конфиденциальных данных.

Потенциал монетизации ресурса, который может увеличить риск преднамеренного воздействия на человека, например, кибератаки или утечки данных.

Технические возможности субъекта угрозы, которые могут определять вероятность успешной атаки.

Легкость использования уязвимостей, что важно учитывать при оценке потенциального воздействия взлома.

Принимая во внимание эти факторы, маркетинговая компания может лучше понять и определить приоритетность рисков для своих информационных ресурсов и разработать эффективную стратегию безопасности для снижения этих рисков.

Таблица 1. Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (ущерб \* вероятность) |
| Социальная инженерия | 2 | 0,2 | 0,4 |
| DDoS-атака | 3 | 0,1 | 0,3 |
| Атака вредоносного ПО | 3 | 0,3 | 0,9 |
| Фишинговая атака | 3 | 0,3 | 0,9 |
| Программы-вымогатели | 5 | 0,1 | 0,5 |
| Недобросовестная конкуренция | 2 | 0,3 | 0,6 |
| Наводнения | 2 | 0,1 | 0,2 |
| Воздействие мощных электромагнитных и электрических помех | 3 | 0,1 | 0,3 |
| Несанкционированное удаленное проникновение | 3 | 0,2 | 0,6 |
| Ошибки, допущенные при разработке компонентов информационной системы | 4 | 0,2 | 0,8 |
| Сбои программного обеспечения | 3 | 0,3 | 0,9 |
| Неисправности технических средств | 2 | 0,2 | 0,4 |
| Перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений | 2 | 0,1 | 0,2 |
| Подслушивание | 2 | 0,3 | 0,6 |
| Разглашение информации компетентными сотрудниками | 3 | 0,1 | 0,3 |
| Несанкционированное распространение информации через поля и электрические сигналы | 3 | 0,1 | 0,3 |
| Итог |  |  | 8,2 |

*5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения).*

Маркетинговая компания, как и любая другая организация, должна обеспечить безопасность своих информационных ресурсов для защиты своей деятельности и производительности. Для обеспечения требуемого уровня безопасности могут быть реализованы следующие меры, методы и средства:

Административные и правовые меры:

* Разработка и внедрение эффективной политики информационной безопасности;
* Обеспечение соблюдения соответствующих законов и нормативных актов, касающихся информационной безопасности;
* Установление четкой иерархии ролей и обязанностей;
* Проведение регулярных обсуждений и брифингов с сотрудниками.

Организационные меры:

* Обучение сотрудников методам обеспечения информационной безопасности;
* Внедрение четкой и строгой иерархии ролей и обязанностей;
* Наличие экстренной связи каждого сотрудника с полицией и пожарной службой (тревожные кнопки) и четких инструкций для всех сотрудников в случае возникновения чрезвычайной ситуации;
* Защита здания, в котором работают сотрудники (пропускная система по распознаванию лиц, по отпечатку пальца, по карточке, охрана);
* Строгий отбор сотрудников с привлечением полиции в случае необходимости.

Технические меры:

* Защита важной корпоративной почты (двухфакторная аутентификация);
* Защита личных документов, бумажных отчетов путем копирования и переноса информации на электронные носители, а также защита помещений, где хранятся документы;
* Использование новейших мер безопасности (антивирусные продукты, брандмауэры) на персональных компьютерах сотрудников и обязательное использование только лицензионных продуктов;
* Внедрение VPN и шифрования для безопасной связи и хранения данных;
* Регулярное резервное копирование данных;
* Разграничение доступа к финансовому отделу;

Программные и аппаратные меры:

* Гидроизоляция оборудования;
* Обеспечение использования только лицензионного программного обеспечения.

*Заключение.*

Разработка политики информационной безопасности необходима маркетинговой компании для защиты своих информационных активов и сохранения доверия заинтересованных сторон. Установив четкие цели и задачи, компания может гарантировать, что ее программа информационной безопасности является комплексной, эффективной и отвечает соответствующим законодательным и нормативным требованиям.

Применяя меры, соответствующие целям, маркетинговая компания может минимизировать риски опасных воздействий, таких как кража персональных данных, шантажирование вирусом-вымогателем, умышленное отключение света, и их последствия, такие как приостановка работы компании, большой денежный долг.