Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Разработка и внедрение политики безопасности консалтинговой компании

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Оглавление

[ВВЕДЕНИЕ 3](#_Toc129656803)

[1. Объекты защиты 4](#_Toc129656804)

[1.1. Описание структуры организации 4](#_Toc129656805)

[1.2. Объекты и субъекты ИВС 6](#_Toc129656806)

[1.2.1 Объекты ИВС 6](#_Toc129656807)

[1.2.2. Субъекты ИВС 6](#_Toc129656808)

[2. Основные угрозы и их источники 7](#_Toc129656809)

[2.1. Внешние угрозы 7](#_Toc129656810)

[2.2. Внутренние угрозы 8](#_Toc129656811)

[2.3. Преднамеренные угрозы 8](#_Toc129656812)

[2.4. Непреднамеренные угрозы 9](#_Toc129656813)

[2.5. Естественные угрозы 9](#_Toc129656814)

[2.6. Искусственные угрозы 10](#_Toc129656815)

[3. Оценка угроз, рисков и уязвимостей 11](#_Toc129656816)

[4. Меры, методы и средства обеспечения требуемого уровня защищённости информационных ресурсов 14](#_Toc129656817)

[ВЫВОДЫ 15](#_Toc129656818)

# ВВЕДЕНИЕ

Защита информации является критически важной для обеспечения конфиденциальности, целостности и доступности данных. В современном мире, когда информация передается и хранится в цифровом формате, угрозы безопасности стали более распространёнными. Несанкционированный доступ к конфиденциальной информации может привести к утечке личных данных, финансовым потерям, разрушению репутации. И это лишь малая часть проблем, с которыми мы можем столкнуться. Для того, чтобы избежать настолько серьёзные последствия и обеспечить защиту информации, необходимым является разработка политики информационной безопасности.

Политика информационной безопасности — это набор правил, процедур и мер, которые применяются для обеспечения конфиденциальности, целостности и доступности информации в организации. Разработка политики информационной безопасности является одной из ключевых задач для любой успешной компании. Это особенно важно для консалтинговой компании, которая работает с большим объёмом информации, включающей в себя персональные данные клиентов и корпоративные данные. К таким данным относятся:

* информация о клиентах и сотрудниках (ФИО, контактные данные, адреса, дата рождения, трудовой стаж, история должностей, зарплата и прочее);
* финансовые данные (о доходах и расходах клиентов, бухгалтерская отчётность и прочее);
* медицинские данные (информация о состоянии здоровья, диагнозы, рецепты и прочее).

Исходя из этого, можно выделить следующие цели и задачи разработки ПИБ:

Цели:

* обеспечение конфиденциальности информации;
* предотвращение утечек данных;
* защита от вирусов и вредного ПО;
* соответствие нормативным требованиям, установленным законодательством.

Задачи:

* описание структуры компании и ее информационных систем;
* выявление уязвимостей и рисков информационной безопасности компании;
* оценка вероятности возникновения угроз и потенциального ущерба от них;
* разработка мер, методов и средств обеспечения необходимого уровня защищенности информации в компании;
* Разработка процедур и инструкций по обеспечению информационной

безопасности компании.

# Объекты защиты

# Описание структуры организации

Подробно рассмотрим структуру консалтинговой компании. Она представляет собой иерархическую организацию, в которой выделяется несколько уровней управления.

Руководство компании. Этот уровень представлен генеральным директором компании, который является главным руководителем организации и несет ответственность за ее деятельность перед советом директоров и акционерами. Он управляет деятельностью всех подразделений компании и принимает стратегические решения.

Отдел развития бизнеса отвечает за поиск новых клиентов и проектов, а также за удержание существующих клиентов. Он занимается маркетинговыми исследованиями, разработкой бизнес-стратегий, презентациями компании и общением с клиентами.

Юридический отдел обеспечивает юридическую поддержку компании, обрабатывает договоры, участвует в переговорах с клиентами и занимается вопросами интеллектуальной собственности.

Отдел финансов и управления рисками отвечает за финансовое планирование и анализ, управление бухгалтерской отчетностью, управление рисками и обеспечение финансовой стабильности компании.

Отдел кадров занимается наймом, обучением и управлением персоналом компании. Он также отвечает за разработку политики компании в области управления персоналом, включая оплату труда, стимулирование и мотивацию сотрудников.

Отдел IT отвечает за информационные технологии компании, включая разработку и поддержку информационных систем, сетевой инфраструктуры, безопасности и обеспечения бесперебойной работы ИВС.

Отдел продаж отвечает за поиск и привлечение новых клиентов, разработку коммерческих предложений, заключение договоров и контроль за их исполнением. Он состоит из менеджеров по продажам, которые работают с клиентами, и специалистов по маркетингу, занимающихся анализом рынка и разработкой стратегии продаж.

Отдел управления персоналом занимается подбором и наймом новых сотрудников, организацией обучения и развития персонала, разработкой системы мотивации и оценки результатов работы сотрудников. Он состоит из HR-менеджеров и специалистов по персоналу.

Отдел управления проектами отвечает за планирование, контроль и управление проектами консалтинговой компании. Он состоит из проектных менеджеров и проектных команд, которые занимаются реализацией проектов.

Отдел управления информационными технологиями занимается разработкой и поддержкой информационных систем компании, а также обеспечением их безопасности. Он состоит из IT-менеджеров, администраторов и разработчиков.

Отдел бухгалтерии и финансов занимается учетом финансовой деятельности компании, разработкой бюджета, финансового анализа и отчетности. Он состоит из бухгалтеров, финансовых аналитиков и контролеров.

Отдел юридической поддержки занимается вопросами правовой поддержки деятельности компании, разработкой договоров, юридическим консультированием и представительством интересов компании в суде. Он состоит из юристов и юридических консультантов.

Отдел качества занимается контролем и обеспечением качества услуг, предоставляемых компанией. Он состоит из специалистов по контролю качества, менеджеров по работе с клиентами и аналитиков.

Каждый отдел имеет своего руководителя, который отчитывается перед генеральным директором компании. Все отделы взаимодействуют друг с другом и координируют свои действия для достижения общих целей.

Пример структуры консалтинговой компании представлена на рисунке 1.1.

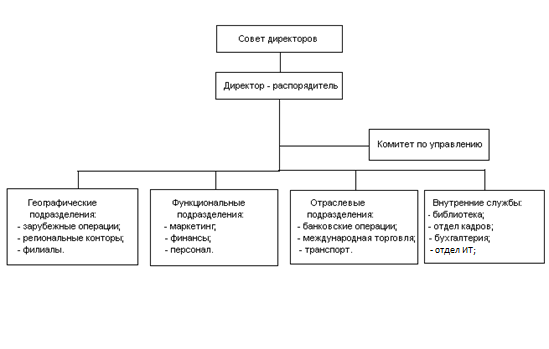


Рисунок 1.1 – Пример структуры консалтинговой компании

# Объекты и субъекты ИВС

Объекты информационно-вычислительной системы — это все компоненты и элементы ИВС, которые используются для обработки, хранения и передачи информации. Субъекты информационных отношений в ИВС — это люди или группы людей, которые используют ИВС для выполнения своих задач.

# 1.2.1 Объекты ИВС

В консалтинговой компании можно выделить следующие объекты информационно-вычислительной системы, которые необходимо защищать:

* сеть;
* серверы;
* сетевые ресурсы;
* системы управления персоналом;
* электронная почта;
* системы управления клиентскими отношениями (CRM);
* базы данных.

В целом, объекты ИВС для консалтинговой компании включают в себя все устройства и системы, которые используются для обработки, хранения, передачи и управления информацией.

# 1.2.2. Субъекты ИВС

Защищать необходимо не только различные источники информации, но и тех, кто может этими объектами воспользоваться. В консалтинговой компании можно выделить следующие субъекты, требующие обеспечения информационной безопасности:

* сотрудники компании, а также устройства, которые они используют;
* рабочие станции, которыми пользуются сотрудники;
* администраторы ИВС, которые управляют сетевой инфраструктурой, настраивают программное обеспечение и обеспечивают безопасность системы;
* клиенты, которые предоставляют конфиденциальные данные консалтинговой компании для анализа и обработки;
* партнеры и поставщики, которые имеют доступ к информации о бизнес-процессах и технологиях компании;
* злоумышленники, которые могут попытаться получить несанкционированный доступ к информации или навредить системе;
* государственные органы и регуляторы, которые могут потребовать доступ к информации компании в соответствии с законодательством.

Все эти субъекты могут оказать влияние на безопасность ИВС и требуют соответствующих мер по защите информации.

# Основные угрозы и их источники

При разработке политики информационной безопасности для консалтинговой компании необходимо произвести классификацию всех возможных типов потенциальных угроз и оценить риски их возникновения.

Говоря об угрозах, они могут иметь внутреннее или внешнее происхождение, быть естественными или искусственными, а также непреднамеренными или преднамеренными.

Рассмотрим потенциальные угрозы, с которыми может столкнуться консалтинговая компания.

# Внешние угрозы

Внешние угрозы — это различные факторы, события и процессы, которые находятся за пределами компании и могут негативно повлиять на ее бизнес-операции, финансовые показатели и репутацию.

Для консалтинговой компании внешние дестабилизирующие факторы могут быть следующими:

* Угрозы безопасности информации: неквалифицированные пользователи, несанкционированный доступ к ПС с целью модификации кода, угрозы кибербезопасности (хакерские атаки, вирусы, фишинг и другие мошеннические схемы);
* Угрозы природного характера: внешние климатические условия, неблагоприятные природные условия;
* Технические угрозы: электромагнитные и ионизирующие помехи, перебои в электроснабжении;
* Угрозы социально-психологического характера: нарушение этики и профессионального поведения сотрудников, которое может негативно сказаться на репутации и имидже компании.

# Внутренние угрозы

Внутренние угрозы — это различные факторы, связанные с деятельностью и поведением внутри компании, которые могут негативно повлиять на ее бизнес-операции, финансовые показатели и репутацию.

К внутренним угрозам для консалтинговой компании относятся:

* Нарушение правил доступа и безопасности информации сотрудниками компании: нарушение политики паролей, отсутствие многофакторной аутентификации, неправомерный доступ к конфиденциальной информации, несанкционированное использование учетных данных других сотрудников;
* Недостаточная безопасность сети и инфраструктуры: несанкционированный доступ к сетевым ресурсам, уязвимости в системах защиты, отсутствие мониторинга сети и обнаружения инцидентов, неправильная конфигурация сетевых устройств;
* Неправомерное использование корпоративных ресурсов: использование компьютеров и сети компании для личных целей, работа с конфиденциальной информацией других клиентов, нарушение правил использования программного обеспечения;
* Нарушение процедур безопасности при обработке и хранении конфиденциальной информации: отсутствие шифрования данных, неправильное хранение паролей и другой конфиденциальной информации, небезопасная передача конфиденциальной информации по сети, несанкционированный доступ к конфиденциальной информации.

Консалтинговые компании должны иметь стратегию по защите от внутренних угроз и принимать меры по обеспечению безопасности своих систем, клиентов и данных, регулярно проводить анализ уязвимостей и тестирование на проникновение для выявления возможных слабостей в системах безопасности и устранения их.

# Преднамеренные угрозы

Преднамеренные угрозы могут быть вызваны многими факторами, включая мотивацию для получения выгоды, политические или идеологические мотивы, или просто желание нанести вред. Независимо от мотивации, результатом таких угроз могут быть утечки данных, нарушения безопасности и повреждения ИВС. кража конфиденциальной информации: сотрудники компании могут украсть или скопировать конфиденциальную информацию, чтобы продать ее конкурентам или использовать в личных целях.

Конкретными примерами таких угроз для консалтинговой компании являются:

* несанкционированный доступ к системам: сотрудники могут использовать свои привилегии для доступа к информации, которая не относится к их работе, или использовать несанкционированные способы доступа к системам;
* вредоносные действия: сотрудники могут внедрять вредоносные программы на компьютеры и сети компании, чтобы получить доступ к конфиденциальной информации или нарушить работу систем;
* саботаж: сотрудники могут наносить ущерб системам и сетям компании, чтобы причинить ущерб ее бизнесу;
* утечки данных: сотрудники могут неосторожно раскрыть конфиденциальную информацию или утечки могут происходить вследствие несанкционированных действий.

Все эти угрозы могут привести к серьезным последствиям для консалтинговой компании, таким как утечка конфиденциальной информации, нарушение законодательства, потеря доверия клиентов и репутации, а также финансов.

# Непреднамеренные угрозы

В дополнение к преднамеренным угрозам, консалтинговые компании должны учитывать и непреднамеренные. А они, в следующую очередь, могут быть вызваны различными факторами, такими как человеческий, технический, природный и внешний.

Ниже рассмотрим конкретные примеры:

* Человеческий фактор: ошибки и недостатки персонала, например, неправильное использование ПО, нарушение процедур безопасности, утеря данных, неправильная обработка и передача информации.
* Технический фактор: сбои в аппаратной или программной части, возникшие вследствие естественных причин, таких как сбой оборудования, неправильная установка и настройка оборудования.
* Природные катастрофы: пожары, наводнения, землетрясения, ураганы и другие стихийные бедствия, которые могут привести к потере данных и нарушению функционирования информационной системы.
* Внешние атаки: к компьютерным системам могут направляться атаки со стороны злоумышленников с целью получения конфиденциальной информации или нарушения работы системы.

Для того чтобы защититься от непреднамеренных угроз, необходимо внедрить соответствующие меры безопасности, такие как контроль доступа, системы резервного копирования и восстановления данных, защиту от вредоносных программ и др.

# Естественные угрозы

Естественные угрозы для консалтинговой компании можно разделить на три категории:

* Погодные явления: к этой категории относятся наводнения, пожары, ураганы, сильные ветры и т.д. Эти явления могут привести к разрушению зданий и инфраструктуры, прерыванию электроснабжения и связи, а также к потере оборудования и данных.
* Климатический кризис: в эту категорию входят частые и сильные экстремальные погодные явления, вызванные глобальным потеплением, такие как наводнения, лесные пожары и т.д. Это может привести к непредсказуемым последствиям для работы компании, включая сокращение численности сотрудников и потерю данных.
* Геологические процессы: к этой категории относятся землетрясения, извержения вулканов и сейсмические деформации, которые могут привести к нарушению работы компьютерной инфраструктуры, а также к потере данных.

В целом, для защиты от естественных угроз необходимо проводить оценку рисков и разрабатывать соответствующие планы, чтобы быстро восстановить работу компании в случае возникновения ЧС. Также важно обеспечить безопасность данных и резервное копирование информации для предотвращения ее потери в результате естественных катастроф.

# Искусственные угрозы

Искусственные угрозы — это угрозы, связанные с использованием современных технологий и информационных систем, которые могут привести к нарушению безопасности компьютерных систем, сетей и данных, а также к различным видам мошенничества, кражи личных данных, финансовых потерь и т.д.

Консалтинговая компания может столкнуться с различными видами искусственных угроз.

Ниже приведены возможные виды угроз, которые могут возникнуть, а также категории, к которым они могут быть отнесены:

* Кибербезопасность: взлом компьютерных систем, кража конфиденциальных данных, фишинг, распространение вредоносных программ;
* Конкуренция: нарушение авторских прав, незаконное использование технологий, похищение персонала, подделка удостоверений компании;
* Финансы: кража финансовых данных, мошенничество при проведении платежей, сбои в системах онлайн-банкинга, незаконное снятие денежных средств со счетов компании;
* Репутация: негативные отзывы в социальных сетях, распространение ложной информации, утечки конфиденциальных данных клиентов, неправильное представление компании в СМИ;
* Регуляторные вопросы: нарушения в области защиты данных, несоблюдение правил и норм, установленных регулирующими органами, неправильное оформление документации, незаконное использование конфиденциальной информации.

Консалтинговые компании должны принимать меры по защите своих систем, клиентов и данных, чтобы избежать возможных угроз. Это может включать в себя использование современных методов шифрования данных, установку многофакторной аутентификации и регулярную проверку наличия уязвимостей в системах. Кроме того, компании должны иметь стратегию по реагированию на угрозы и четкий план действий в случае возникновения проблем.

# Оценка угроз, рисков и уязвимостей

Чтобы оценить возможный ущерб, который может быть нанесён консалтинговой компании, воспользуемся шкалой для численной оценки рисков от несанкционированного доступа (НСД) к информационным ресурсам консалтинговой компании. В данной шкале каждой степени ущерба присваивается число от 1 до 5. Числовые значения для оценки ущерба и соответствующие им описания представлены в таблице 3.1.

Таблица 3.1 — Условная численная шкала для оценки ущерба компании

|  |  |
| --- | --- |
| **Величина ущерба** | **Описание** |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб консалтинговой компании |
| 1 | Ущерб от атаки есть, но он незначителен, финансовое положение, а также положение консалтинговой компании на рынке не нарушены |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время консалтинговая компания терпит убытки, но её положение на рынке и количество клиентов изменяются минимально |
| 3 | Значительные финансовые потери, а также потери на рынке. Также ощущаются потери в виде клиентов. |
| 4 | Потери очень значительные, консалтинговая компания теряет своё положение на рынке. Многие клиенты прекращают своё сотрудничество с компанией. Требуются крупные финансовые затраты для восстановления былого положения. |
| 5 | Консалтинговая компания прекращает своё существование |

Пример создания шкалы вероятности того, что угроза будет реализована, приведен в таблице 3.2.

Таблица 3.2 — 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 |

Далее, на основании таблиц 3.1 и 3.2 можно составить таблицу рисков. На этапе анализа таблицы риски задаются некоторым максимально допустимым уровнем. В данном случае это значение 0.5.

Оценка рисков представлена в таблице 3.3.

Таблица 3.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки** | **Ущерб** | **Вероятность** | **Риск** |
| Взлом информационной системы | 5 | 0,3 | 1,5 |
| Фишинг (выманивание паролей) | 3 | 0,4 | 1,2 |
| Использование уязвимости в системе безопасности | 4 | 0,2 | 0,8 |
| Отключение электроэнергии | 2 | 0,2 | 0,4 |
| Обман персонала | 2 | 0,1 | 0,2 |
| Сбои и отказы оборудования | 3 | 0,3 | 0,9 |
| DDoS-атака | 4 | 0,4 | 1,6 |
| Ошибки эксплуатации оборудования | 2 | 0,2 | 0,4 |
| Утечка данных | 3 | 0,3 | 0,9 |
| Вредоносное ПО | 4 | 0,2 | 0,8 |
| Несанкционированный доступ к файлам | 2 | 0,3 | 0,6 |
| SQL-инъекция | 4 | 0,2 | 0,8 |
| Перехват и анализ трафика | 3 | 0,3 | 0,9 |
| Кража/уничтожение оборудования | 5 | 0,1 | 0,5 |
| Спам | 1 | 0,4 | 0,4 |
|  |  | **ИТОГО:** | **11,9** |

Если интегральный риск (итого) превышает допустимый уровень, значит, в системе безопасности набирается множество мелких проблем, которые также нужно решать комплексно. В этом случае из строк таблицы (типов атак) выбираются те, которые «дают» самый значительный вклад в значение интегрального риска. Производится работа по снижению их влияния или полному устранению.

Просматривая таблицу, мы видим, что все описанные интегральные риски не превышают допустимый уровень, что хорошо для компании. Однако суммарный риск от всех угроз превышает допустимый уровень (5).

Таким образом, можно сделать вывод, что система безопасности консалтинговой компании нуждается в доработке. И в первую очередь нужно проработать те угрозы безопасности, которые в таблице получили наибольшую оценку риска (такие как 0,8 и 0,9). А затем уже все остальные.

# Меры, методы и средства обеспечения требуемого уровня защищённости информационных ресурсов

Для обеспечения требуемого уровня защищённости информационных ресурсов консалтинговой компании необходимо применять соответствующие меры, методы и средства защиты.

Ниже приведены угрозы, представляющие опасность для консалтинговой компании и приведённые в таблице 3.3, а также способы защиты от них:

* Взлом информационной системы: использование сложных паролей, двухфакторной аутентификации, регулярного обновления систем безопасности, аудита системы на предмет уязвимостей, обучения пользователей правилам безопасности;
* Фишинг (выманивание паролей): обучение пользователей правилам безопасности, использование программ и систем, фильтрующих спам, использование двухфакторной аутентификации, проверка ссылок на подозрительные домены и сайты;
* Использование уязвимости в системе безопасности: регулярное обновление систем безопасности, аудит системы на предмет уязвимостей, использование антивирусных программ, фильтрующих вредоносные программы и уведомляющих о возможной угрозе;
* Отключение электроэнергии: резервирование электроснабжения, использование генераторов электроэнергии, использование ИБП (интерактивных блоков питания), перенос систем на другой объект;
* Обман персонала: обучение персонала правилам безопасности, ограничение доступа к конфиденциальной информации, использование двухфакторной аутентификации, контроль действий персонала;
* Сбои и отказы оборудования: регулярное техническое обслуживание и обновление оборудования, использование резервных систем, быстрое реагирование на возможные сбои и отказы;
* DDoS-атака: использование систем защиты от DDoS-атак, мониторинг сети на предмет аномальной активности, настройка брандмауэра и других систем безопасности для предотвращения атак;
* Ошибки эксплуатации оборудования: обучение персонала правильной эксплуатации оборудования, регулярное техническое обслуживание и обновление оборудования, использование инструкций и руководств для обслуживания оборудования;
* Утечка данных: использование систем защиты данных, ограничение доступа к конфиденциальной информации, шифрование данных, аудит системы на предмет утечек;
* Вредоносное ПО: использование антивирусных программ, обновление систем безопасности, запрет установки непроверенного программного обеспечения;
* SQL-инъекция: использование систем защиты от SQL-инъекций, использование подготовленных запросов к базе данных, фильтрация пользовательского ввода;
* Перехват и анализ трафика: использование систем защиты от перехвата и анализа трафика, шифрование данных, использование защищенных протоколов связи;
* Кража/уничтожение оборудования: использование систем видеонаблюдения и доступа, контроль доступа к помещениям, физическая защита оборудования;
* Спам: использование систем фильтрации спама, обучение пользователей правилам безопасности, использование проверенных почтовых сервисов и программ.

Применение этих мер и методов может снизить вероятность возникновения угроз и защитить информационные ресурсы компании от несанкционированного доступа и других видов атак.

# ВЫВОДЫ

Разработка политики информационной безопасности (ПИБ) — это важный шаг в обеспечении защиты информационных ресурсов организации. Она представляет собой документ, цель которого заключается в определении правил и процедур, которые должны быть реализованы для обеспечения конфиденциальности, целостности и доступности информации, а также защиты от угроз информационной безопасности.

В ходе работы была разработана политика информационной безопасности для консалтинговой компании, которая отвечает современным стандартам и требованиям по защите информации. Были выявлены потенциальные угрозы и уязвимости информационных систем компании, а также разработаны меры и методы обеспечения требуемого уровня защищенности.

Были установлены процедуры по управлению доступом к информации, защите от вредоносных программ, резервному копированию и восстановлению данных, а также меры по обеспечению конфиденциальности информации.

Разработанная политика информационной безопасности должна быть введена на всех уровнях компании и должна подлежать периодическому обновлению и проверке ее эффективности. Были приняты все необходимые меры для защиты информации от возможных угроз и рисков, что обеспечивает надежную защиту информационных ресурсов консалтинговой компании.