Белорусский государственный технологический университет

Факультет информационных технологий

Кафедра Программной Инженерии

Практическое занятие №2

По дисциплине «Основы информационной безопасности»

На тему **«Разработка политики информационной безопасности бизнес-компании»**

Выполнил:

Студент 2 курса 3 группы

Шутро А.С.

Преподаватель: Ржеутская Н.В.

Минск 2023

**Введение**

В настоящее время обеспечение информационной безопасности является одним из ключевых аспектов успешной деятельности любой компании. В рамках данного проекта была разработана политика информационной безопасности для бизнес-компании, которая имеет профсоюзную организацию в своей структуре.

В рамках проекта были рассмотрены следующие аспекты: описание структуры профсоюзной организации, оценка рисков, связанных с обработкой и хранением конфиденциальной информации профсоюза, разработка мер защиты и выводы.

Описание структуры бизнес-компании позволило определить основные участники процесса обработки и хранения конфиденциальной информации профсоюзной организации. Оценка рисков позволила выявить возможные угрозы и уязвимости, связанные с обработкой и хранением конфиденциальной информации профсоюза. Разработка мер защиты позволила определить конкретные действия, которые необходимо предпринять для минимизации рисков и обеспечения безопасности конфиденциальной информации профсоюзной организации.

Выводы, полученные в результате разработки политики информационной безопасности, позволяют компании обеспечить безопасность конфиденциальной информации профсоюзной организации, снизить риски утечки и несанкционированного доступа к информации, а также соблюдать требования законодательства в области защиты персональных данных. Реализация данной политики позволит компании повысить свою репутацию и доверие со стороны клиентов и партнеров, а также снизить риски финансовых потерь и ущерба для бизнеса.

**Описание структуры профсоюзной организации**

Профсоюзная организация - это некоммерческая организация, которая представляет интересы работников в отношениях с работодателями и государством. Она может включать в себя различные отделы и подразделения, такие как отделы юридической поддержки, финансового управления, организации мероприятий и т.д.

Структура бизнес-компании, которая имеет профсоюзную организацию в своей структуре, может быть организована следующим образом:

* Руководство компании - это высшее звено управления, которое отвечает за разработку стратегии и принятие решений по вопросам информационной безопасности.
* Отдел информационной безопасности - это структурное подразделение, которое отвечает за разработку и реализацию политики информационной безопасности, а также за контроль и мониторинг ее выполнения.
* Профсоюзная организация - это структура, которая представляет интересы работников компании и обеспечивает их социальную защиту. В рамках данного проекта, профсоюзная организация также является объектом защиты информации.
* Отдел IT-технологий - это структурное подразделение, которое отвечает за разработку и поддержку информационной инфраструктуры компании, а также за обеспечение безопасности информационных систем.
* Отдел кадров - это структурное подразделение, которое отвечает за управление персоналом компании, включая профсоюзную организацию.
* Отдел юридических вопросов - это структурное подразделение, которое отвечает за юридическую поддержку компании, включая вопросы информационной безопасности и защиты данных.

В рамках данного проекта, мы будем сосредоточены на разработке политики информационной безопасности для профсоюзной организации, которая является частью структуры бизнес-компании.

**Оценка рисков**

Для профсоюзной организации, как и для любой другой организации, существуют риски в области информационной безопасности. Они могут включать в себя утечки конфиденциальной информации, кибератаки, вирусы и другие угрозы. Для оценки рисков необходимо провести анализ уязвимостей и потенциальных угроз, а также определить вероятность их возникновения и последствий.

Оценка рисков для проекта политики информационной безопасности бизнес-компании на тему профсоюзной организации может включать следующие аспекты:

* Риск несанкционированного доступа к конфиденциальной информации профсоюзной организации, такой как личные данные членов профсоюза, финансовые отчеты и т.д.
* Риск утечки конфиденциальной информации профсоюзной организации, которая может привести к ущербу для репутации компании и ее отношений с профсоюзной организацией.
* Риск нарушения законодательства в области защиты персональных данных, если компания не соблюдает требования по обработке и хранению личной информации членов профсоюза.
* Риск кибератак со стороны злоумышленников, которые могут попытаться получить доступ к информации профсоюзной организации или использовать ее для проведения кибератак на компанию.
* Риск внутренней угрозы, когда сотрудники компании могут намеренно или ненамеренно нарушить политику информационной безопасности и утечь конфиденциальную информацию профсоюзной организации.

Для уменьшения рисков необходимо разработать и реализовать политику информационной безопасности, которая будет включать в себя меры по защите конфиденциальной информации профсоюзной организации, обучение сотрудников компании правилам безопасности и контроль выполнения политики. Также необходимо регулярно проводить аудит информационной безопасности и обновлять политику в соответствии с изменениями в законодательстве и технологиях.

**Разработка мер защиты**

Разработка мер защиты является одним из ключевых этапов проекта политики информационной безопасности для бизнес-компании, которая имеет профсоюзную организацию в своей структуре. Ниже представлены основные меры защиты, которые были разработаны в рамках данного проекта:

* Ограничение доступа к конфиденциальной информации профсоюзной организации. Для этого были определены роли и права доступа к информации, а также установлены механизмы контроля доступа.
* Шифрование конфиденциальной информации профсоюзной организации. Для этого были выбраны соответствующие алгоритмы шифрования и установлены механизмы шифрования данных.
* Регулярное обновление программного обеспечения и антивирусных программ. Для этого были определены процедуры обновления программного обеспечения и антивирусных программ, а также установлены механизмы контроля обновлений.
* Регулярное проведение аудита информационной безопасности. Для этого были определены процедуры проведения аудита, а также установлены механизмы контроля выполнения рекомендаций по результатам аудита.
* Обучение сотрудников компании правилам информационной безопасности. Для этого были разработаны программы обучения, а также установлены механизмы контроля выполнения обучения.
* Резервное копирование конфиденциальной информации профсоюзной организации. Для этого были определены процедуры резервного копирования, а также установлены механизмы контроля выполнения резервного копирования.
* Установка системы мониторинга и регистрации событий безопасности. Для этого были выбраны соответствующие системы мониторинга и регистрации событий безопасности, а также установлены механизмы контроля выполнения мониторинга и регистрации.

Реализация данных мер защиты позволит компании обеспечить безопасность конфиденциальной информации профсоюзной организации, снизить риски утечки и несанкционированного доступа к информации, а также соблюдать требования законодательства в области защиты персональных данных.

**Выводы**

Разработка политики информационной безопасности для профсоюзной организации является важной мерой для защиты конфиденциальной информации и обеспечения безопасности данных. Она должна включать в себя анализ рисков, разработку мер защиты и обучение сотрудников основам информационной безопасности. Реализация этих мер поможет предотвратить утечки информации и другие угрозы, а также обеспечит надежную защиту данных профсоюзной организации.

В результате разработки политики информационной безопасности бизнес-компании на тему профсоюзной организации были определены риски, связанные с обработкой и хранением конфиденциальной информации профсоюза, а также были разработаны меры по ее защите. Реализация данной политики позволит компании обеспечить безопасность конфиденциальной информации профсоюзной организации, снизить риски утечки и несанкционированного доступа к информации, а также соблюдать требования законодательства в области защиты персональных данных.

Важно отметить, что политика информационной безопасности должна быть постоянно обновляемой и адаптивной к изменяющимся условиям и угрозам. Компания должна регулярно проводить аудиты информационной безопасности и обучать своих сотрудников правилам обработки конфиденциальной информации.

В целом, разработка политики информационной безопасности является важным шагом для обеспечения безопасности конфиденциальной информации профсоюзной организации и защиты интересов ее членов. Компания, следуя данной политике, сможет повысить свою репутацию и доверие со стороны клиентов и партнеров, а также снизить риски финансовых потерь и ущерба для бизнеса.