Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Разработка и внедрение политики безопасности логистической компании

Студент: Касперович А. С.

ФИТ 3 курс 6 группа

Преподаватель: Блинова Е. А.

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

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.

Концепция политики информационной безопасности (ИБ) разрабатывается в соответствии с законодательством по информа ционной безопасности Республики Беларусь, соответствующими нормативными документами министерства или ведомства, к кото рому относится организация или учреждение, а также решениями Оперативно-аналитического центра при Президенте Республики Беларусь (см. п. 2.2 в книге [1]).

Обеспечение ИБ на предприятиях и в учреждениях, как правило, является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач. Значимость систематической целенаправленной деятельности по обеспечению ИБ становится тем более высокой, чем выше степень автоматизации бизнес-процессов. Значимость обеспечения ИБ в некоторых случаях может определяться наличием в общей системе информационных потоков предприятия сведений, составляющих не только коммерче скую, но и государственную тайну, а также другие виды конфиден циальной информации: сведения, составляющие банковскую тайну, различные виды персональных данных, в том числе врачебная тайна, интеллектуальная собственность компаний-партнеров и т. п.

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 логистической компании, которая работает с большим объёмом информации, включающей в себя персональные данные клиентов и корпоративные данные.

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.

1. **Объекты защиты. Описание структуры организации (учре ждения), 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.**

**Отделы:**

* Руководство компании

### **Операционный отдел**

### **Коммерческий отдел**

### **Финансовый и бухгалтерский отдел**

### **IT-отдел**

### **Отдел кадров**

### **Юридический отдел**

### **Отдел безопасности**

### **Обслуживающий персонал**

**Работники:**

**Генеральный директор** – отвечает за стратегическое развитие, финансовую стабильность и ключевые решения компании.

**Исполнительный директор** – контролирует операционные процессы, взаимодействие между отделами, оптимизацию логистических цепочек.

**Финансовый директор** – управляет финансами компании, бюджетированием, расчетами с контрагентами.

**Операционный директор (или руководитель логистики)** – координирует работу подразделений, связанных с перевозками, складским учетом, таможенным оформлением.

**Логисты** – планируют маршруты, распределяют грузы, работают с клиентами и перевозчиками.

**Специалисты по складской логистике** – контролируют приемку, хранение, комплектацию и отгрузку товаров.

**Водители-экспедиторы** – занимаются транспортировкой грузов, контролируют загрузку и выгрузку.

**Грузчики** – выполняют погрузо-разгрузочные работы на складе.

**Директор по продажам** – отвечает за развитие клиентской базы и привлечение заказчиков.

**Менеджеры по продажам** – ищут новых клиентов, ведут переговоры, заключают договоры.

**Главный бухгалтер** – контролирует бухгалтерский и налоговый учет.

**Бухгалтеры** – занимаются расчетами с контрагентами, налогами, заработной платой.

**IT-директор** – разрабатывает и поддерживает информационные системы компании.

**Программисты и системные администраторы** – обеспечивают бесперебойную работу логистического ПО, баз данных и внутренних сервисов.

**HR-директор** – отвечает за подбор, мотивацию и обучение персонала.

**Специалисты по подбору персонала** – занимаются наймом сотрудников.

**Юристы** – оформляют договоры, разрешают споры, обеспечивают соблюдение законодательства.

**Начальник службы безопасности** – следит за сохранностью грузов, транспорта, складов.

**Охранники** – обеспечивают физическую охрану территории и имущества.

**Технический персонал** – занимаются ремонтом и обслуживанием автопарка и складской техники.

**Уборщики** – поддерживают чистоту в офисах и складских помещениях.

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

### Естественные и искусственные

**Естественные:**

* Воздействие стихийных сил (наводнения, пожары и т. п.)
* Воздействие мощных электромагнитных и электрических помех (промышленных и природных)

**Искусственные:**

* Действия внутреннего или внешнего злоумышленника
* Наблюдение за источниками информации
* Подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов
* Перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений
* Разглашение информации компетентными людьми
* Утеря носителей информации
* Несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре
* Сбои и отказы в аппаратуре сбора, обработки и передачи информации
* Отказы системы электроснабжения
* Проникновение на территорию непроверенных лиц
* Взлом навигационной системы
* Угроза психологического здоровья работников

### Преднамеренные и непреднамеренные

**Преднамеренные:**

* Действия внутреннего или внешнего злоумышленника
* Наблюдение за источниками информации
* Подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов
* Перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений
* Разглашение информации компетентными людьми
* Несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре
* Проникновение на территорию непроверенных лиц
* Взлом навигационной системы

**Непреднамеренные:**

* Утеря носителей информации
* Воздействие стихийных сил (наводнения, пожары и т. п.)
* Сбои и отказы в аппаратуре сбора, обработки и передачи информации
* Отказы системы электроснабжения
* Воздействие мощных электромагнитных и электрических помех (промышленных и природных)
* Угроза психологического здоровья работников

### Внешние и внутренние

**Внешние:**

* Действия внешнего злоумышленника
* Наблюдение за источниками информации
* Перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений
* Воздействие стихийных сил (наводнения, пожары и т. п.)
* Воздействие мощных электромагнитных и электрических помех (промышленных и природных)
* Проникновение на территорию непроверенных лиц
* Взлом навигационной системы

**Внутренние:**

* Действия внутреннего злоумышленника
* Подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов
* Разглашение информации компетентными людьми
* Утеря носителей информации
* Сбои и отказы в аппаратуре сбора, обработки и передачи информации
* Отказы системы электроснабжения
* Несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре
* Угроза психологического здоровья работников

1. **Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты (воспользуйтесь приве денными в описании таблицами, заполните их).**

Чтобы оценить возможный ущерб, который может быть нанесён логистической компании, воспользуемся шкалой для численной оценки рисков от несанкционированного доступа (НСД) к информационным ресурсам логистической 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 4.1.

Таблица 4.1 — Условная численная шкала для оценки ущерба компании

|  |  |
| --- | --- |
| **Величина ущерба** | **Описание** |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб логистической компании |
| 1 | Ущерб от атаки есть, но он незначителен, финансовое положение, а также положение логистической компании на рынке не нарушены |
| 2 | Финансовые операции не ведутся в течение некоторого времени, за это время логистическая 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, логистическая компания теряет своё положение на рынке. Многие клиенты прекращают своё сотрудничество с компанией. Требуются крупные финансовые затраты для восстановления былого положения. |
| 5 | Логистическая компания прекращает своё существование |

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

Таблица 4.2 — 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 4.1 и 4.2 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 4.3.

Таблица 4.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки** | **Ущерб** | **Вероятность** | **Риск** |
| Сбой и отказ оборудования | 4 | 0,3 | 1,2 |
| Взлом навигационной системы | 4 | 0,2 | 0,8 |
| Использование уязвимости в системе безопасности | 4 | 0,2 | 0,8 |
| Фишинг | 4 | 0,2 | 0,8 |
| Несанкционированный доступ к файлам | 4 | 0,2 | 0,8 |
| Внедрение вредоносного ПО | 4 | 0,2 | 0,8 |
| SQL-иньекция | 4 | 0,2 | 0,8 |
| Отключение электроэнергии | 4 | 0,2 | 0,8 |
| DdoS-атака | 4 | 0,2 | 0,8 |
| Утечка личных данных пользователей | 2 | 0,3 | 0,6 |
| Утечка данных компании | 3 | 0,2 | 0,6 |
| Ошибки эксплуатации оборудования | 2 | 0,3 | 0,6 |
| Обман персонала | 3 | 0,2 | 0,6 |
| Взлом информационной системы | 5 | 0,1 | 0,5 |
| Кража оборудования | 3 | 0,1 | 0,3 |
| Спам-атака | 1 | 0,3 | 0,3 |
| Затопление помещений | 3 | 0,1 | 0,3 |
| Пожар | 3 | 0,1 | 0,3 |
|  |  | **ИТОГО:** | **12,7** |

### Сбой и отказ оборудования

* **Резервное копирование**: Регулярное создание резервных копий данных для их восстановления в случае отказа оборудования.
* **Мониторинг состояния**: Использование систем мониторинга для предсказания и предотвращения отказов оборудования.
* **Планирование обновлений**: Регулярное обслуживание и обновление оборудования.
* **Избыточность**: Использование избыточных систем и компонентов (например, кластеров) для повышения надежности.

### Взлом навигационной системы

* **Шифрование данных**: Использование сильного шифрования для защиты данных навигационной системы.
* **Аутентификация и авторизация**: Применение многофакторной аутентификации и строгой политики доступа.
* **Регулярные обновления**: Установка обновлений и патчей для устранения уязвимостей.
* **Мониторинг и аудит**: Внедрение систем мониторинга и аудита для отслеживания подозрительной активности.

### Использование уязвимости в системе безопасности

* **Внедрение безопасности на всех уровнях**: Использование защитных мер на уровне сети, приложений и данных.
* **Тестирование на проникновение**: Регулярное проведение тестов на проникновение для выявления и устранения уязвимостей.
* **Обновления и патчи**: Регулярное обновление программного обеспечения для устранения известных уязвимостей.
* **Обучение персонала**: Обучение сотрудников основам кибербезопасности.

### Фишинг

* **Обучение сотрудников**: Проведение регулярных тренингов по распознаванию фишинговых атак.
* **Антифишинговые меры**: Использование специализированных решений для фильтрации и блокировки фишинговых писем.
* **Многофакторная аутентификация**: Применение многофакторной аутентификации для защиты учетных записей.
* **Проверка источников**: Внедрение процедур проверки источников подозрительных писем и ссылок.

### Несанкционированный доступ к файлам

* **Шифрование данных**: Шифрование чувствительных данных на всех уровнях.
* **Контроль доступа**: Применение строгих политик контроля доступа и разграничения полномочий.
* **Аудит и мониторинг**: Внедрение систем мониторинга и аудита для отслеживания доступа к файлам.
* **Многофакторная аутентификация**: Использование многофакторной аутентификации для защиты учетных записей.

### Внедрение вредоносного ПО

* **Антивирусное ПО**: Использование и регулярное обновление антивирусных программ.
* **Сегментация сети**: Разделение сети на сегменты для локализации угроз.
* **Проверка приложений**: Проверка и тестирование приложений перед их установкой.
* **Обучение сотрудников**: Обучение персонала правилам безопасного использования интернета и работы с файлами.

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 логистической компании нуждается в доработке. И в первую очередь нужно проработать те угрозы безопасности, которые в таблице получили наибольшую оценку риска. А затем уже все остальные.

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

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

### Законодательные меры

* **Утечка данных**: соблюдение законодательства о защите данных (например, GDPR), создание политик безопасности и конфиденциальности информации.
* **Обман персонала**: разработка и соблюдение трудового законодательства, регулирующего права и обязанности сотрудников.
* **Кража/уничтожение оборудования**: разработка нормативных актов по защите имущества и оборудования.
* **SQL-инъекция, DDoS-атака, Вредоносное ПО**: принятие законов и норм о кибербезопасности, ответственность за компьютерные преступления.

### Технические меры

* **Сбои и отказы в аппаратуре**: использование резервных систем, регулярное техническое обслуживание и обновление оборудования.
* **Взлом информационной системы**: использование сложных паролей, двухфакторной аутентификации, регулярного обновления систем безопасности, аудита системы на предмет уязвимостей.
* **Использование уязвимости в системе безопасности**: регулярное обновление систем безопасности, аудит системы на предмет уязвимостей, использование антивирусных программ.
* **Несанкционированный доступ к файлам**: использование систем фильтрации спама, двухфакторной аутентификации, проверка ссылок на подозрительные домены и сайты.
* **Фишинг**: использование программ и систем, фильтрующих спам, проверка ссылок на подозрительные домены и сайты.
* **Отключение электроэнергии**: использование резервного электроснабжения, генераторов электроэнергии, ИБП.
* **Вредоносное ПО**: использование антивирусных программ, обновление систем безопасности, запрет установки непроверенного ПО.
* **SQL-инъекция**: использование систем защиты от SQL-инъекций, использование подготовленных запросов к базе данных.
* **DDoS-атака**: использование систем защиты от DDoS-атак, настройка брандмауэра и других систем безопасности.
* **Спам-атака**: использование систем фильтрации спама, проверка почтовых сервисов и программ.
* **Взлом навигационной системы**: шифрование GPS, использование альтернативных систем, контроль доступа.

### Организационные меры

* **Ошибки эксплуатации оборудования**: обучение персонала правильной эксплуатации оборудования, использование инструкций и руководств.
* **Кража/уничтожение оборудования**: использование систем видеонаблюдения и контроля доступа к помещениям.
* **Затопление помещений**: установка датчиков протечек, автоматических клапанов, дублирующих насосов, аварийных заглушек.
* **Пожар**: использование огнестойких материалов, систем пожаротушения, датчиков дыма, проведение аварийных учений.
* **Фишинг**: обучение пользователей правилам безопасности.
* **Обман персонала**: обучение персонала правилам безопасности, контроль действий персонала.
* **Утечка данных**: использование систем защиты данных, шифрование данных, ограничение доступа к конфиденциальной информации.
* **Несанкционированный доступ к файлам**: обучение пользователей правилам безопасности, использование проверенных почтовых сервисов и программ.