|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб × Вероятность) |
| Несанкционированный доступ к базе данных клиентов | 5 | 0,3 | 1,5 |
| Атака с использованием SQL-инъекции | 4 | 0,4 | 1,6 |
| Кража данных платежных карт через фишинг | 5 | 0,2 | 1,0 |
| Атака DDoS на веб-сайт интернет-магазина | 4 | 0,6 | 2,4 |
| Утечка персональных данных из-за утраты устройства | 3 | 0,2 | 0,6 |
| Нарушение работы серверов из-за сбоя оборудования | 3 | 0,5 | 1,5 |
| Нарушение конфиденциальности через неконтролируемый доступ к электронной почте (фишинг) | 4 | 0,5 | 2,0 |
| Злоупотребление сотрудниками интернет-магазина | 3 | 0,1 | 0,3 |
| Итого | 31 | 2,8 | 10,9 |

Интернет-магазин — это веб-платформа, позволяющая пользователям покупать товары или услуги онлайн. Такие магазины предлагают удобные способы поиска товаров, оформления заказов, а также способы оплаты и доставки.

**Актуальность ПИБ для интернет-магазина:**

Интернет-магазины стали важным элементом современного бизнеса, а защита информации — критически важной задачей. Магазины обрабатывают большое количество персональных данных и финансовых транзакций, что делает их уязвимыми для атак. Разработка и внедрение политики информационной безопасности (ПИБ) необходимы для защиты данных клиентов и поддержания доверия к магазину.

**Цели ПИБ**

Целью ПИБ является обеспечение надежной защиты информации в интернет-магазине, поддержание конфиденциальности, целостности и доступности данных, а также выполнение требований законодательства.

**Задачи ПИБ**

1. Защита персональных данных клиентов.
2. Обеспечение безопасности платежей и транзакций.
3. Минимизация рисков утечек данных и атак на сайт.
4. Разработка процедур для защиты от внешних и внутренних угроз.
5. Обучение сотрудников безопасности и защите данных.

**Объекты защиты. Описание структуры**

Структура интернет-магазина:

* Веб-сайт
* Система управления контентом (CMS)
* Серверы и базы данных
* Платежные системы
* Логистическая система
* Система безопасности

Объекты информационной безопасности интернет-магазина:

* Персональные данные
* Финансовые транзакции
* Товары и каталог
* Информационные системы
* Сетевые ресурсы

Внутренняя структура ИВС:

1. Сетевые компоненты
2. Хранение данных
3. Программное обеспечение
4. Процесс управления

**Потенциальные угрозы**

1. Естественные угрозы

* Землетрясения, наводнения и другие стихийные бедствия
* Пожары
* Ураганы

2. Искусственные угрозы

* Системные сбои или ошибки в программном обеспечении
* Уязвимости в программном обеспечении или несанкционированный доступ к внутренним системам
* Нарушения в управлении данными или конфиденциальностью

3. Преднамеренные угрозы

* Кибератаки
* Вредоносное ПО и вирусы

4. Непреднамеренные угрозы

* Ошибки персонала при обработке заказов, который может привести к утрате или недоставке товаров.
* Неосмотрительное обновление программного обеспечения или внедрение новых функций
* Необоснованные изменения в политике безопасности

5. Внешние угрозы

* Конкуренты
* Киберпреступники
* Государственные органы

6. Внутренние угрозы

* Невнимательность сотрудников при работе с клиентскими данными или проведении транзакций
* Преднамеренные действия сотрудников, направленные на кражу данных или уничтожение информации
* Недостаточная защита данных в рамках внутренней инфраструктуры компании

**Меры, методы и средства обеспечения безопасности:**

1. **Технические меры:**
   * **Шифрование данных**: защита клиентской информации и транзакций (SSL/TLS).
   * **Антивирусы и фаерволы**: защита от вирусов, атак и внешних угроз.
   * **Резервное копирование**: регулярное создание резервных копий для защиты от потери данных.
   * **Обновления ПО**: устранение уязвимостей через своевременные обновления.
2. **Организационные меры:**
   * **Политики безопасности**: разработка внутренних регламентов по защите информации.
   * **Обучение персонала**: регулярное обучение сотрудников основам информационной безопасности.
   * **Управление доступом**: ограничение доступа к важной информации.
3. **Контроль и аудит:**
   * **Мониторинг систем**: отслеживание действий пользователей и активности на сайте.
   * **Аудит безопасности**: регулярные проверки и тестирование систем на уязвимости.