МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Разработка и внедрение политики безопасности интернет-магазина

Студент: Евсеенко В. П.

ФИТ 3 курс 4 группа

Преподаватель: Савельева М. Г.

Минск 2025

Содержание

[Введение 3](#_Toc191469930)

[1 Объекты защиты 4](#_Toc191469931)

[1.1 Описание структуры организации 4](#_Toc191469932)

[1.2 Объекты и субъекты ИВС 5](#_Toc191469933)

[1.2.1 Объекты ИВС 5](#_Toc191469934)

[1.2.2 Субъекты ИВС 5](#_Toc191469935)

[2 Основные угрозы и их источники 6](#_Toc191469936)

[2.1 Естественные угрозы 6](#_Toc191469937)

[2.2 Искусственные угрозы 6](#_Toc191469938)

[2.3 Преднамеренные угрозы и непреднамеренные 6](#_Toc191469939)

[2.4 Внутренние угрозы 7](#_Toc191469940)

[2.5 Внешние угрозы 7](#_Toc191469941)

[3 Оценка угроз, рисков и уязвимостей 9](#_Toc191469942)

[4 Меры, методы и средства обеспечения требуемого уровня защищённости информационных ресурсов 12](#_Toc191469943)

[Выводы и предложения 15](#_Toc191469944)

# **Введение**

Актуальность обеспечения информационной безопасности будет присутствовать всегда, особенно интернет-магазинам, они предоставляю услуги по продаже товаров или услуг через интернет, подвергаются многочисленным угрозам, включая кибератаки, утечку личных данных клиентов, нарушение целостности и доступности информации, что может привести к потерям как финансовым, так и репутационным. В условиях постоянно меняющихся технологий и угроз информационная безопасность является ключевым фактором для обеспечения стабильной работы магазина, защиты персональных данных клиентов и соблюдения законодательства.

Цель разработки информационной безопасности:

* обеспечение конфиденциальности, целостности и доступности информации в интернет-магазине;
* защита от внешних и внутренних угроз, включая хакерские атаки, фишинг, вирусы, утечку данных и другие;
* устранение уязвимостей в системе безопасности и защита от потенциальных рисков;
* снижение финансовых и репутационных рисков.

Задачи:

* определить объекты защиты и риски безопасности;
* разработать меры и средства защиты;
* создать план мероприятий по внедрению и обеспечению безопасности;
* разработать систему мониторинга и контроля состояния информационной безопасности.

# **Объекты защиты**

# **Описание структуры организации**

Интернет-магазин представляет собой сложную информационную систему, объединяющую в себе веб-сайт, серверное оборудование, базы данных, системы управления заказами, платежные шлюзы и логистические сервисы.

Основу периметра составляют серверные помещения, где размещаются основные вычислительные и хранилищные мощности, а также облачные сервисы, обеспечивающие гибкость и масштабируемость хранения информации. Наряду с этим, периметр включает в себя зону, предназначенную для размещения веб-серверов, обеспечивающих публичный доступ к сайту магазина, что позволяет изолировать критичные внутренние ресурсы от внешних воздействий. Дополнительным элементом периметра являются точки подключения к платежным системам и партнёрским сервисам, посредством которых осуществляется обмен финансовой и логистической информацией.

Внутренняя структура ИВС характеризуется распределением компонентов по функциональным зонам, обеспечивающим сегментацию и изоляцию критически важных систем. Внутри периметра выделяются отдельные зоны, где, например, расположены серверы баз данных, обрабатывающие конфиденциальную информацию о клиентах и заказах, а также серверы приложений, выполняющие бизнес-логику интернет-магазина. Сервера аутентификации и управления доступом располагаются в отдельном сегменте, что позволяет ограничить доступ пользователей и систем к критическим ресурсам. Также внутренняя структура включает в себя системы мониторинга, резервного копирования и восстановления данных, что позволяет оперативно реагировать на любые инциденты и минимизировать потенциальный ущерб. Все компоненты ИВС взаимодействуют посредством защищенных сетевых каналов, реализующих протоколы шифрования и аутентификации, что обеспечивает целостность и конфиденциальность передаваемой информации. Такой детальный подход к проектированию внутренней структуры позволяет не только обеспечить высокую производительность системы, но и создать эффективные механизмы для обнаружения и нейтрализации угроз.

# **Объекты и субъекты ИВС**

В рамках информационно-вычислительной системы интернет-магазина объектами являются все компоненты информационной системы, имеющие значение для функционирования бизнеса и сохранности данных. Субъектами же выступают все участники, имеющие доступ к информационным ресурсам интернет-магазина, а также те, кто влияет на управление и функционирование системы.

# **1.2.1 Объекты ИВС**

К конкретным объектам ИВС интернет-магазина будут относиться:

* цифровые данные;
* финансовые транзакции;
* веб-сервер;
* бумажные документы
* физическая инфраструктура;
* облачные сервисы;
* базы данных;
* персональная информация.

Обобщая, объектами ИВС являются как виртуальные, так и материальные компоненты. При этом каждый объект требует индивидуального подхода к защите, поскольку степень его уязвимости и потенциальная ценность для бизнеса могут существенно различаться.

# **1.2.2 Субъекты ИВС**

Не только источники информации, но и внешние участники играют важную роль в формировании общего информационного поля организации, поэтому обеспечение безопасности информации требует комплексного подхода, учитывающего как внутренние, так и внешние аспекты. В интернет-магазине следующие субъекты, которым необходимо обеспечение информационной безопасности:

* консультанты интернет-магазина, а также устройства, которые они используют;
* руководство ИВС;
* клиенты интернет-магазина
* разработчики и администраторы веб-приложения;
* поставщики услуг.

Все субъекты, участвующие в информационных отношениях, должны строго соблюдать установленные правила и процедуры безопасности, что позволяет минимизировать риски несанкционированного доступа и утечки конфиденциальных данных.

# **Основные угрозы и их источники**

При анализе угроз для интернет-магазина важно учитывать их происхождение, характер намеренности и источник воздействия. В первую очередь угрозы можно разделить на внутренние и внешние. Рассмотрим потенциальные угрозы, с которыми может столкнуться консалтинговая компания.

# **Естественные угрозы**

Естественные угрозы обусловлены природными катаклизмами, такими как землетрясения, пожары, наводнения или ураганы. Несмотря на отсутствие злого умысла, их последствия могут быть крайне разрушительными: повреждение физической инфраструктуры, утрата данных и длительный простой критически важных сервисов.

Для противодействия таким угрозам организации разрабатывают планы аварийного восстановления, используют резервное копирование данных и распределяют критичные системы по географически удаленным площадкам.

# **Искусственные угрозы**

Искусственные угрозы, напротив, порождаются деятельностью человека и охватывают как преднамеренные атаки, так и непреднамеренные ошибки. Преднамеренные искусственные угрозы включают целенаправленные действия злоумышленников, направленные на получение несанкционированного доступа, изменение или уничтожение информации, а также саботаж деятельности интернет-магазина. Непреднамеренные искусственные угрозы часто связаны с человеческим фактором, таким как ошибки при обновлении программного обеспечения, неправильная настройка систем безопасности или небрежное обращение с конфиденциальными данными.

Такие ошибки могут создать уязвимости, которые впоследствии могут быть использованы злоумышленниками для проведения атак. Интернет-магазин должен принимать меры по защите своих систем, информации клиентов и данных о транзакциях, 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.

# **Преднамеренные угрозы и непреднамеренные**

Преднамеренные внутренние угрозы :

* атака на базу данных клиентов;
* подделка сайта интернет-магазина с целью обмана покупателей;
* взлом платежного шлюза;
* DDoS-атака на веб-сервер магазина;
* SQL-инъекция в систему обработки заказов;
* эксплуатация уязвимости в API мобильного приложения;
* социальная инженерия для получения доступа к административным данным;
* атака на мобильное приложение интернет-магазина;
* манипуляция рейтингами и отзывами на сайте;
* нарушение работы логистической системы вследствие кибератаки;
* физическая кража или повреждение серверного оборудования.

Непреднамеренные угрозы со стороны внутренних субъектов часто обусловлены человеческим фактором — ошибками при работе с данными, неправильной конфигурацией систем или невнимательностью, что может привести к случайной утечке информации или повреждению критических данных:

* утечка коммерческой информации;
* сбой работы облачной инфраструктуры;
* неправильная настройка межсетевого экрана;
* внедрение вредоносного ПО через фишинговое письмо сотрудника.

# **Внутренние источники угрозы**

Внутренние угрозы возникают внутри организации и связаны с действиями её сотрудников, подрядчиков или иных доверенных лиц. Эти угрозы могут проявляться как в виде преднамеренных действий, так и случайных ошибок:

* сотрудники, допускающие ошибки или нарушающие правила безопасности.
* недовольные или уволенные работники, намеренно наносящие ущерб.
* ненадежные или устаревшие системы и программное обеспечение.
* неправильная настройка или отсутствие обновлений систем безопасности.
* отсутствие регулярного обучения персонала вопросам информационной безопасности

# **Внешние источники угрозы**

Внешние угрозы исходят из окружения, не контролируемого организацией, и инициируются лицами или группами, не имеющими законного доступа к информационным ресурсам магазина:

* киберпреступники, стремящиеся получить несанкционированный доступ к данным или нарушить работу системы;
* конкуренты, использующие недобросовестные методы для получения коммерческой информации;
* поставщики и партнеры, чьи уязвимости могут повлиять на безопасность интернет-магазина;

Для противодействия внешним угрозам применяются многоуровневые системы защиты: от использования межсетевых экранов и систем обнаружения вторжений до современных методов шифрования и многофакторной аутентификации. Эти меры позволяют не только минимизировать вероятность успешного проникновения, но и обеспечить оперативное реагирование в случае инцидента, ограничивая потенциальный ущерб для бизнеса.

# **Оценка угроз, рисков и уязвимостей**

Чтобы оценить потенциальный ущерб, который может возникнуть в результате несанкционированного доступа к информационным ресурсам интернет-магазина, применяется специализированная оценочная шкала. Каждый уровень ущерба представлен числом от 1 до 5, отражающим степень негативного влияния инцидента на ключевые аспекты бизнеса, включая финансовую устойчивость, оперативную деятельность, репутацию и доверие клиентов. Таблица 3.1 ниже демонстрирует распределение этих уровней ущерба с соответствующими описаниями, адаптированными под специфику работы интернет-магазина.

Таблица 3.1 — Условная численная шкала для оценки ущерба компании

|  |  |
| --- | --- |
| **Величина ущерба** | **Описание** |
| 0 | |  | | --- | | Раскрытие незначительной информации (например, общих метаданных или служебных записей), которое не влияет на операционную деятельность, финансовое состояние и репутацию интернет-магазина. | |
| 1 | |  |  | | --- | --- | |  | Незначительное воздействие, например, мелкие утечки данных, не затрагивающих ключевые клиентские или финансовые сведения, приводящие к минимальным перебоям в работе, которые не влияют на рыночные позиции магазина. | |
| 2 | |  |  | | --- | --- | |  | Кратковременное нарушение работы интернет-магазина (например, временные сбои в работе сайта или системы обработки заказов) или утечка не критичной информации, что вызывает незначительные финансовые потери и временное снижение эффективности работы, но без заметного влияния на лояльность клиентов. | |
| 3 | |  |  | | --- | --- | |  | Значительное нарушение функционирования системы: серьезные перебои в работе интернет-магазина, утечка части критической информации, приводящая к ощутимым финансовым потерям, ухудшению обслуживания клиентов и снижению доверия потребителей. | |
| 4 | |  |  | | --- | --- | |  | Масштабные финансовые и репутационные потери: крупная утечка конфиденциальных данных, длительные простои системы, значительное снижение качества обслуживания и массовый отток клиентов, требующие значительных затрат на восстановление нормального функционирования. | |
| 5 | |  |  | | --- | --- | |  | Катастрофические последствия, приводящие к полной остановке деятельности интернет-магазина: массовая утечка критической информации, полный крах операционной системы, масштабное падение доверия клиентов и потеря позиций на рынке, что может привести к прекращению бизнеса. | |

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 | Событие не наблюдается |
| 0,1 | Реже, чем раз в год |
| 0,2 | Примерно один случай в год |
| 0,3 | Около одного случая в месяц |
| 0,4 | Примерно один случай в неделю |
| 0,5 | Почти ежедневное возникновение инцидента |

Ниже представлена таблица, отражающая анализ рисков для интернет-магазина. В таблице для каждого типа угрозы рассчитывается риск как произведение величины ущерба и вероятности её реализации. Установленный порог максимально допустимого риска для отдельных инцидентов – 0,5, что позволяет выделить критичные направления, требующие немедленного реагирования.

Оценка рисков представлена в таблице 3.3.

Таблица 3.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки** | **Ущерб** | **Вероятность** | **Риск** |
| Атака на базу данных клиентов | 5 | 0,3 | 1,5 |
| Подделка сайта интернет-магазина с целью обмана покупателей | 4 | 0,4 | 1,6 |
| Взлом платежного шлюза | 4 | 0,2 | 1,0 |
| DDoS-атака на веб-сервер магазина | 4 | 0,4 | 1,6 |
| SQL-инъекция в систему обработки заказов | 4 | 0,3 | 1,2 |
| Эксплуатация уязвимости в API мобильного приложения | 3 | 0,2 | 0,6 |
| Неправильная настройка межсетевого экрана | 2 | 0,3 | 0,6 |
| Внедрение вредоносного ПО через фишинговое письмо сотрудника | 3 | 0,2 | 0,6 |
| Социальная инженерия для получения доступа к административным данным | 3 | 0,1 | 0,3 |
| Сбой работы облачной инфраструктуры | 2 | 0,2 | 0,4 |
| Атака на мобильное приложение интернет-магазина | 3 | 0,2 | 0,6 |
| Манипуляция рейтингами и отзывами на сайте | 2 | 0,4 | 0,8 |
| Утечка коммерческой информаци | 4 | 0,3 | 1,2 |
| Нарушение работы логистической системы вследствие кибератаки | 3 | 0,3 | 0,9 |
| Физическая кража или повреждение серверного оборудования | 5 | 0,1 | 0,5 |
|  |  | **ИТОГО:** | **13,4** |

Если суммарный риск превышает допустимый уровень, это означает, что в системе безопасности есть несколько проблем, которые нужно решать комплексно. Из таблицы рисков выделяются угрозы, оказывающие наибольшее влияние на общий риск, и проводится работа по их устранению или снижению воздействия.

Анализ показал, что общий риск выше допустимого уровня, хотя отдельные угрозы не превышают его. Следует сосредоточиться на угрозах с наибольшими значениями риска (например, 1,2 и 1,6) и устранить их в первую очередь, а затем решить остальные проблемы.

Таким образом, необходимо улучшить защиту от наиболее значимых угроз для снижения общего уровня риска.

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

Для обеспечения необходимого уровня защищенности информационных ресурсов интернет-магазина необходимо разработать комплексную программу информационной безопасности (ИБ), которая включает в себя меры, методы и средства защиты на всех уровнях работы организации. Основная цель — минимизировать риски утечек данных, атак и других угроз, обеспечив бесперебойную работу и сохранность информации. В таблице 3.3 представлены основные угрозы для интернет-магазина, и для каждой из них будут предложены соответствующие меры по защите;

* атака на базу данных клиентов: для защиты базы данных клиентов необходимо использовать шифрование всех чувствительных данных, включая личную информацию и платежные реквизиты. Должен быть внедрен многоуровневый доступ к базе данных с разграничением прав доступа и регулярными аудитами безопасности. Также важным элементом защиты является внедрение системы мониторинга, которая позволяет быстро обнаружить несанкционированный доступ и аномальные запросы к базе данных;
* подделка сайта интернет-магазина с целью обмана покупателей: для предотвращения таких атак необходимо использовать сертификаты SSL для всех страниц сайта, чтобы обеспечить шифрование данных между пользователями и сервером. Также важен мониторинг и защита доменных имен (DNS), а также использование двухфакторной аутентификации для пользователей, которые имеют доступ к панели управления сайтом;
* взлом платежного шлюза: для защиты платежной системы следует применять современные технологии защиты транзакций, такие как токенизация данных карт и шифрование всех платежных операций. Также важно регулярно обновлять платежные системы и устранять уязвимости, чтобы предотвратить несанкционированный доступ;
* DDoS-атака на веб-сервер магазина: для защиты от DDoS-атак необходимо использовать специализированные решения для защиты от таких атак, например, внедрение балансировщиков нагрузки, облачных сервисов защиты и специализированных фильтров трафика. Эти меры помогут снизить вероятность перегрузки серверов и предотвратить выход из строя веб-сервера.
* SQL-инъекция в систему обработки заказов: защита от SQL-инъекций предполагает использование подготовленных запросов и параметризированных запросов, что минимизирует возможность внедрения вредоносных SQL команд. Также следует проводить регулярное тестирование и аудит безопасности системы обработки заказов;
* эксплуатация уязвимости в API мобильного приложения: для защиты API мобильных приложений нужно использовать аутентификацию и авторизацию через токены, такие как OAuth, а также зашифрованные каналы связи для передачи данных. Важно регулярно обновлять API и устранять уязвимости, проводя тестирование безопасности;
* неправильная настройка межсетевого экрана: для защиты от угроз, связанных с ошибками в настройке межсетевых экранов, необходимо регулярно проверять и обновлять правила доступа, ограничивать доступ к важным сервисам только для авторизованных пользователей и проводить периодические аудиты настройки фаерволов;
* внедрение вредоносного ПО через фишинговое письмо сотрудника: важно обучить сотрудников распознавать фишинговые письма и использовать решения для защиты от вредоносных программ, такие как антивирусное ПО и фильтрация электронных писем. Также необходимо внедрить систему многослойной аутентификации для сотрудников;
* социальная инженерия для получения доступа к административным данным: чтобы минимизировать риски от социальной инженерии, нужно проводить регулярные тренинги для сотрудников, разрабатывать политику безопасности и внедрять многофакторную аутентификацию для всех административных аккаунтов.
* сбой работы облачной инфраструктуры: для защиты от сбоев облачной инфраструктуры необходимо обеспечить отказоустойчивость и резервирование всех критичных систем. Важно регулярно проводить бэкап данных и иметь план восстановления после сбоев для минимизации потерь в случае инцидентов.
* атака на мобильное приложение интернет-магазина: для защиты мобильных приложений следует использовать шифрование данных, защиту от реверс-инжиниринга, а также обновлять приложения с регулярными исправлениями безопасности. Важно также использовать безопасные каналы связи для передачи данных.
* манипуляция рейтингами и отзывами на сайте: для защиты от манипуляций с отзывами и рейтингами следует внедрить систему аутентификации пользователей, предотвращение фальсификации отзывов через IP-блокировки и алгоритмы выявления подозрительных действий. Также можно использовать механизмы машинного обучения для автоматического выявления поддельных отзывов.
* утечка коммерческой информации: для предотвращения утечек коммерческой информации необходимо внедрить системы контроля доступа и защиту данных с помощью шифрования. Регулярно следует проводить аудит безопасности, а также обучать сотрудников соблюдению корпоративных стандартов безопасности.
* нарушение работы логистической системы вследствие кибератаки: важно интегрировать систему защиты для логистических процессов, включая мониторинг и управление доступом, а также шифрование данных о заказах и маршрутах. При этом необходима интеграция с внешними системами безопасности, чтобы обеспечить защиту от кибератак.
* физическая кража или повреждение серверного оборудования: для защиты оборудования следует использовать системы видеонаблюдения и контролировать доступ в серверные помещения. Также рекомендуется хранить критически важные данные в защищенных дата-центрах, которые имеют физическую защиту и резервирование энергии. Для эффективной защиты интернет-магазина необходимо применить многоуровневый подход, который включает в себя технические средства, такие как системы защиты от DDoS-атак, шифрование данных, использование антивирусных решений, а также организационные меры, включая обучение сотрудников и внедрение строгих процедур доступа. Комбинированное использование этих методов позволит существенно снизить риски и обеспечить надежную защиту от возможных угроз безопасности.

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

# **Выводы и предложения**

Разработка политики информационной безопасности (ПИБ) для интернет-магазина является неотъемлемой частью стратегии защиты его информационных ресурсов и обеспечения безопасности данных клиентов и бизнес-процессов. ПИБ должна быть направлена на создание системы мероприятий, направленных на защиту информации, повышение ее доступности, а также обеспечение целостности и конфиденциальности данных.

В ходе разработки ПИБ для интернет-магазина были выявлены ключевые угрозы и уязвимости, которые могут повлиять на безопасность данных и функционирование бизнес-систем. Рассмотрены потенциальные риски, включая кибератаки, утечку данных, а также внутренние угрозы, такие как ошибки сотрудников и неправильная настройка систем.

Для обеспечения требуемого уровня безопасности были предложены меры по защите данных от несанкционированного доступа, внедрению надежных механизмов аутентификации и шифрования, а также по предотвращению сбоев в работе критических систем. Важными элементами стратегии стали регулярные аудиты безопасности, резервное копирование данных и своевременное обновление программного обеспечения.

Разработанная политика информационной безопасности должна быть интегрирована во все процессы работы интернет-магазина и включать в себя регулярные обучения сотрудников, а также тестирование на предмет уязвимостей. Также важно предусмотреть регулярную актуализацию ПИБ в связи с изменениями в технологиях и возможными новыми угрозами.

Предложения по улучшению безопасности интернет-магазина включают внедрение более эффективных средств защиты от DDoS-атак, усиление контроля доступа к чувствительным данным и расширение использования современных методов защиты мобильных приложений. Также следует усилить контроль за целостностью данных и провести улучшение мер защиты от социальной инженерии.

В заключение, внедрение предложенной политики информационной безопасности поможет минимизировать риски, повысить доверие клиентов и партнёров, а также обеспечить стабильную работу интернет-магазина в условиях растущих угроз информационной безопасности.