Учреждение образования

«Белорусский государственный технологический университет»

**Основы информационной безопасности**

**Лабораторная работа №3**

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

Выполнил:

Студент 2 курса 2 группы ФИТ

Мойсеёнок Денис

Преподаватель:

Ржеутская Надежда Викентьевна

Минск 2025

**Цель:** разработать проект политики информационной безопасности бизнес-компании.

Контрольные вопросы:

1. Что такое политика безопасности?

Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

2. Что означают метки безопасности?

Метки безопасности используются для реализации принудительного управления доступом с субъектами и объектами. Метка субъекта описывает его благонадежность, метка объекта - степень закрытости, содержащейся в нем информации. Согласно "Оранжевой книге", метки безопасности состоят из двух частей – уровня секретности и списка категорий.

3. Какие работы производятся по обеспечению режима информационной безопасности?

–  определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания;

–  оценка рисков;

–  выбор контрмер, обеспечивающих режим ИБ;

–  управление рисками;

–  аудит системы управления ИБ;

–  выработка политики безопасности.

4. Какие практические шаги осуществляются для определения политики информационной безопасности?

Этап 1. Выбор национальных и международных руководящих документов, и стандартов в области информационной безопасности и формулирование на их базе основных требований и положений политики информационной безопасности компании, включая:

– управление доступом к средствам вычислительной техники (СВТ), программам и данным, а также антивирусную защиту;

– вопросы резервного копирования;

– проведение ремонтных и восстановительных работ;

– информирование об инцидентах в области информационной безопасности и пр.

Этап 2. Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности компьютерных информационных систем (КИС). Уровень защищенности в соответствии с зарубежными стандартами может быть минимальным (базовым) либо повышенным. Этим уровням защищенности соответствует минимальный (базовый) или полный вариант анализа информационных рисков.

Этап 3. Структуризация контрмер по защите информации по следующим основным уровням: административному, процедурному, программно-техническому

Этап 4. Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере информационной безопасности. Назначение периодичности проведения совещаний по тематике информационной безопасности на уровне руководства, в том числе периодического пересмотра положений политики информационной безопасности, а также порядка обучения всех категорий пользователей информационной системы в области информационной безопасности. Известно, что выработка политики безопасности организации – наименее формализованный этап. Однако в последнее время именно здесь сосредоточены усилия многих специалистов по защите информации.

Этап 5. Определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания. На этом этапе определяются границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности строится именно в этих границах.

5. Что является основой программно-технического уровня для обеспечения безопасности?

Основой программно-технического уровня являются следующие механизмы безопасности:

− идентификация и аутентификация пользователей;

− управление доступом;

− протоколирование и аудит;

− криптография;

− экранирование;

− обеспечение высокой доступности и т. д.

Вариант 15: Интернет-магазин

**Введение**

Современные интернет-магазины представляют собой сложные информационные системы, обрабатывающие большие объемы данных, включая персональные данные клиентов, платежную информацию, сведения о заказах и складских запасах. В условиях растущего числа кибератак и мошеннических действий защита этих данных становится критически важной задачей.

Развитие цифровых технологий способствует не только расширению возможностей электронной коммерции, но и увеличению потенциальных рисков. Утечки данных, атаки злоумышленников, вирусные программы и внутренние ошибки сотрудников могут привести к серьезным финансовым и репутационным потерям. Кроме того, нарушение законодательства о защите персональных данных может повлечь за собой юридическую ответственность.

Основная цель политики информационной безопасности интернет-магазина — минимизировать угрозы, обеспечить защиту критически важных данных и создать надежную систему противодействия возможным инцидентам. Для этого необходимо разработать комплексную стратегию, охватывающую технические, организационные и юридические аспекты безопасности.

Данный документ содержит основные положения политики информационной безопасности интернет-магазина, анализирует потенциальные угрозы, рассматривает меры их предотвращения и способы быстрого реагирования на инциденты. Реализация данной политики позволит повысить уровень доверия со стороны клиентов, обеспечить бесперебойную работу компании и минимизировать риски, связанные с утечками и несанкционированным доступом к данным.

**Описание структуры бизнес-компании**

Выбранная компания – интернет-магазин, специализирующийся на продаже бытовой электроники. Деятельность магазина охватывает полный цикл взаимодействия с клиентами, начиная от приема заказов и заканчивая их доставкой. Для обеспечения эффективной работы интернет-магазина сформирована организационная структура, включающая несколько ключевых подразделений:

1. Администрация

Отвечает за общее руководство компанией, стратегическое планирование, управление финансами и развитие бизнеса. В задачи администрации входит контроль над соблюдением внутренних регламентов, анализ рынка, взаимодействие с партнерами и инвесторами.

2. IT-отдел

Обеспечивает бесперебойную работу веб-сайта, баз данных, платежных систем и внутренней корпоративной сети. Основные функции IT-отдела:

* разработка и поддержка веб-платформы интернет-магазина;
* обеспечение безопасности данных и защита от кибератак;
* внедрение новых технологий и модернизация инфраструктуры;
* контроль за соблюдением норм информационной безопасности.

3. Отдел продаж

Взаимодействует с клиентами и поставщиками, обрабатывает заказы, консультирует покупателей и занимается продвижением товаров. Основные задачи:

* управление заказами и клиентской базой;
* формирование ценовой политики и разработка маркетинговых акций;
* анализ спроса и предложения;
* склад и логистика;
* отвечает за прием, хранение, учет и доставку товаров клиентам.

Ключевые функции отдела:

* организация поставок и контроль товарных запасов;
* обеспечение оперативной сборки и отправки заказов;
* взаимодействие с курьерскими службами и транспортными компаниями.

4. Служба поддержки клиентов

Занимается обработкой обращений клиентов, решением вопросов, связанных с возвратами, гарантийным обслуживанием и качеством товаров. Функции отдела:

* консультирование клиентов по работе интернет-магазина;
* рассмотрение претензий и возвратов;
* мониторинг отзывов и обратной связи.

Для эффективного взаимодействия между подразделениями используются внутренние информационные системы, корпоративная сеть и защищенные базы данных. Так как интернет-магазин работает с персональными данными клиентов и платежной информацией, особое внимание уделяется информационной безопасности, защите данных и минимизации рисков несанкционированного доступа.

**Оценка рисков**

Интернет-магазин – это сложная информационная система, которая обрабатывает и хранит значительные объемы данных, включая персональную информацию клиентов, платежные данные и сведения о заказах. Любые сбои в работе системы, утечки информации или кибератаки могут привести к серьезным последствиям, таким как финансовые потери, репутационные риски и юридическая ответственность.

Интернет-магазины сталкиваются с множеством угроз, которые могут повлиять на их работу, безопасность данных и репутацию. Особое внимание необходимо уделить информационным угрозам, так как они могут привести к утечке данных, финансовым потерям и юридическим последствиям.

Основные риски информационной безопасности интернет-магазина:

По виду:

1. Физическая и логическая целостность.

* физическая целостность – уничтожение серверного оборудования, повреждение хранилищ данных (жестких дисков, облачных серверов), атаки на серверные центры;
* логическая целостность – внесение несанкционированных изменений в базу данных товаров, цен, заказов, манипуляции с финансовыми операциями, изменение контента на сайте с целью мошенничества;

1. Конфиденциальность.

* несанкционированный доступ к персональным данным клиентов: ФИО, адреса доставки, номера телефонов, данные банковских карт;
* перехват платежной информации: использование методов фишинга, атак "человек посередине" (MITM), внедрение вредоносных скриптов на страницу оплаты;
* шпионаж со стороны конкурентов: кража данных о продажах, маркетинговых стратегиях, аналитике клиентов.

1. Доступность.

* **DDoS-атаки:** массовая нагрузка на сервер, приводящая к отказу в обслуживании;
* **сбой оборудования или программного обеспечения:** серверные аварии, ошибки в CMS, проблемы с хостингом;
* **злонамеренное блокирование доступа:** удаление критически важных данных, шифрование файлов вирусами-вымогателями.

1. Права собственности.

* **кража интеллектуальной собственности:** нелегальное копирование контента, базы клиентов, уникальных алгоритмов и бизнес-процессов;
* **использование чужих данных в мошеннических схемах:** подмена реквизитов, подделка учетных записей сотрудников.

По происхождению:

1. Случайные угрозы.

* **технические сбои:** ошибки в коде, несовместимость ПО, падение серверов, сбой в работе базы данных;
* **ошибка персонала:** случайное удаление данных, неверные настройки безопасности, утечка информации из-за недостаточного контроля доступа;
* **стихийные бедствия:** пожары, наводнения, перебои в подаче электроэнергии, приводящие к потере данных.

1. Преднамеренные угрозы.

* **хакерские атаки:** взлом системы управления интернет-магазином, внедрение вредоносного кода, обход аутентификации;
* **финансовое мошенничество:** подделка заказов, манипуляции с ценами, кража средств со счетов;
* **социальная инженерия:** мошенничество с использованием человеческого фактора, выманивание паролей у сотрудников или клиентов.

По источникам:

1. Люди.

* **персонал:** утечка данных, саботаж, небрежное обращение с информацией;
* **посторонние лица:** взломщики, конкуренты, мошенники, случайные пользователи, несанкционированно получившие доступ к данным.

1. Технические устройства.

* **серверы, базы данных, системы хранения:** аппаратные сбои, повреждение жестких дисков, отказ питания;
* **клиентские устройства:** зараженные вирусами компьютеры покупателей, которые могут передавать вредоносные данные в систему.

1. Программные модели и алгоритмы.

* **уязвимости в CMS интернет-магазина:** SQL-инъекции, XSS-атаки, обход аутентификации;
* **ошибки в алгоритмах:** некорректная обработка платежных транзакций, дыры в механизмах защиты данных.

1. Внешняя среда.

* **атмосферные условия:** грозы, перепады напряжения, электромагнитные помехи, влияющие на работу серверов;
* **шумовые сигналы и электромагнитные наводки:** могут привести к повреждению информации на жестких дисках и в оперативной памяти.

Информационные угрозы подразделяется на:

1. Естественные факторы.

* **пожар в серверном центре:** может привести к полной потере данных при отсутствии резервного копирования;
* **наводнение или землетрясение:** повреждение серверного оборудования, уничтожение физических носителей информации;
* **перебои с электроснабжением:** внезапное отключение питания приводит к сбоям в работе базы данных, потере информации.

2. Человеческий фактор.

* **фишинговые атаки:** мошенники могут создать поддельный сайт интернет-магазина и красть логины и пароли пользователей;
* **несанкционированный доступ сотрудников:** администратор с высоким уровнем доступа может преднамеренно изменить базу данных или похитить информацию;
* **слабые пароли и ненадежная аутентификация:** использование слабых паролей сотрудниками и клиентами делает систему уязвимой к взлому;
* **социальная инженерия:** злоумышленники могут выдать себя за представителей техподдержки, чтобы получить доступ к системе.

**Разработка мер защиты**

Интернет-магазин обрабатывает и хранит важные данные, включая личную информацию клиентов, платежные реквизиты, историю покупок и внутренние бизнес-процессы. Любые уязвимости в системе могут привести к утечкам данных, финансовым потерям и ухудшению репутации компании. Поэтому разработка эффективных мер защиты является критически важным этапом обеспечения безопасности интернет-магазина.

1. Защита от угроз физической и логической целостности.

Резервное копирование:

* регулярное создание резервных копий баз данных, логов и конфигурационных файлов;
* хранение копий на нескольких серверах и в облачных хранилищах;
* использование технологии инкрементального и дифференциального бэкапа.

Журналирование и контроль изменений:

* ведение логов изменений данных, действий пользователей и администраторов;
* настройка автоматических уведомлений при попытке модификации критических данных.

Мониторинг целостности данных:

* использование хеш-функций (SHA-256, MD5) для контроля изменений файлов;
* регулярные проверки базы данных на наличие аномалий и повреждений.

Шифрование данных:

* хранение конфиденциальной информации в зашифрованном виде (AES-256);
* применение TLS 1.3 для защиты передачи данных между клиентом и сервером.

Система отката изменений:

* внедрение механизма версионирования, позволяющего быстро восстановить предыдущие версии данных.

2. Защита от угроз конфиденциальности.

Шифрование данных пользователей:

* использование bcrypt или Argon2 для хранения паролей;
* шифрование кредитных карт и других чувствительных данных по стандарту PCI DSS.

Двухфакторная аутентификация (2FA):

* включение дополнительной аутентификации по SMS, e-mail или через приложения (Google Authenticator).

Разграничение доступа:

* ограничение доступа сотрудников к конфиденциальной информации по принципу "минимально необходимого";
* использование ролевой модели управления доступом (RBAC).

Обнаружение утечек данных:

* мониторинг даркнета и баз данных утекших паролей с использованием специализированных сервисов;
* настройка уведомлений при подозрительной активности учетных записей.

Защита сессий пользователей:

* автоматический выход из системы при длительном бездействии;
* использование HttpOnly и Secure-флагов для cookie;
* внедрение защиты от перехвата сессий (Session Hijacking) с помощью уникальных токенов.

3. Обеспечение доступности интернет-магазина.

DDoS-защита:

* использование сервисов защиты от DDoS (Cloudflare, AWS Shield, Imperva);
* ограничение частоты запросов на сервер с одного IP-адреса (Rate Limiting).

Контроль нагрузки на сервер:

* балансировка нагрузки с помощью Nginx или HAProxy;
* автоматическое масштабирование серверов в случае роста нагрузки.

Защита от вредоносного ПО:

* регулярное сканирование сервера на наличие вредоносных файлов (ClamAV, Malwarebytes);
* ограничение прав на выполнение загруженных пользователями файлов.

Использование изолированных контейнеров:

* размещение критических сервисов в контейнерах (Docker, Kubernetes) для предотвращения распространения атак.

Автоматическое восстановление после сбоев:

* использование систем резервирования (failover);
* запуск аварийного сервера в случае отказа основного.

4. Защита прав собственности.

Цифровые водяные знаки и скрытые идентификаторы:

* внедрение уникальных невидимых меток в изображения и документы;
* генерация скрытых идентификаторов в коде веб-страниц.

Лицензирование и регистрация прав:

* регистрация товарных знаков и авторских прав на контент;
* включение юридических оговорок о защите интеллектуальной собственности в пользовательском соглашении.

Мониторинг незаконного использования:

* автоматический поиск украденного контента с помощью Google Reverse Image Search, DMCA-такдаунов;
* использование сервисов по защите авторских прав (Copyrighted.com, Copytrack).

5. Защита от человеческого фактора.

Обучение персонала по кибербезопасности:

* проведение регулярных тренингов по распознаванию фишинговых атак;
* создание инструкций по безопасному использованию корпоративных систем.

Разграничение прав доступа:

* ограничение привилегий сотрудников в зависимости от их ролей;
* использование принципа "нулевого доверия" (Zero Trust Security).

Жесткий контроль аутентификации администраторов:

* включение многофакторной аутентификации (MFA);
* запрет на доступ к панели управления без VPN или корпоративного IP.

Мониторинг действий внутри системы:

* логирование всех критических действий пользователей и сотрудников;
* автоматическое оповещение о подозрительных изменениях.

Блокировка учетных записей при подозрительной активности:

* временная блокировка пользователя при нескольких неудачных попытках входа;
* автоматический анализ аномальной активности учетных записей.

6. Защита от естественных факторов.

Защита дата-центров:

* использование дата-центров с защитой от стихийных бедствий;
* наличие резервных источников питания (UPS, генераторы).

Автоматическое резервное копирование:

* настройка ежедневного бэкапа в облако и на отдельные серверы;
* использование Geo-репликации баз данных.

Тестирование системы и кода:

* регулярное проведение тестирования безопасности (penetration testing);
* использование инструментов статического анализа кода (SonarQube, Snyk).

Разработка комплексной системы защиты интернет-магазина требует сочетания организационных, технических и правовых мер. Внедрение современных технологий безопасности, контроль доступа, регулярный аудит и обучение сотрудников помогут минимизировать риски и обеспечить надежную защиту данных клиентов.

Защита интернет-магазина – это не одноразовый процесс, а постоянный цикл мероприятий, включающий мониторинг угроз, обновление систем и адаптацию к новым вызовам в сфере кибербезопасности.

**Вывод**

Создание и управление интернет-магазином требует комплексного подхода к оценке и минимизации рисков, а также разработки эффективных мер защиты. Безопасность бизнеса в онлайн-среде зависит не только от технических решений, но и от организационных, правовых и финансовых аспектов.

Основные выводы:

1. Интернет-магазин подвержен множеству рисков – от кибератак и утечек данных до проблем с логистикой, возвратами и нестабильностью поставок. Финансовые и репутационные потери могут стать критичными, если не учитывать эти угрозы.

2. Комплексный подход к защите – ключ к устойчивости бизнеса. Простые защитные меры (пароли, SSL-сертификаты) уже не способны противостоять современным атакам. Требуется внедрение многоуровневой системы безопасности:

* надежная защита веб-сайта (шифрование данных, защита от SQL-инъекций, использование WAF);
* контроль и разграничение доступа к важным данным;
* обучение сотрудников и клиентов правилам кибербезопасности;
* мониторинг и анализ угроз, регулярное тестирование уязвимостей.

3. Технические меры защиты должны соответствовать современным стандартам. Использование двухфакторной аутентификации, шифрование данных, защита платежных операций и защита от DDoS-атак становятся не просто рекомендациями, а необходимыми условиями работы интернет-магазина.

4. Юридическая защита играет важную роль в бизнесе. Соблюдение законов о защите данных (GDPR, ФЗ-152, PCI DSS) не только минимизирует юридические риски, но и повышает доверие клиентов. Продуманная политика конфиденциальности и пользовательское соглашение позволяют урегулировать возможные споры.

5. Безопасность – это непрерывный процесс. Угрозы в киберпространстве постоянно развиваются, поэтому интернет-магазин должен регулярно проводить аудит безопасности, обновлять программное обеспечение, тестировать свои системы и адаптироваться к новым вызовам.

Интернет-магазин – это сложная система, работающая в высококонкурентной и подверженной рискам среде. Только продуманный и системный подход к защите информации, данных пользователей и финансовых операций позволит создать надежную, безопасную и устойчивую платформу для ведения бизнеса. В долгосрочной перспективе инвестиции в безопасность оправдывают себя, обеспечивая стабильность работы, доверие клиентов и конкурентное преимущество.