МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №1**

Выполнила студентка 3 курса 4 группы Смелова В.В.

Проверила: Копыток Д.В.

Минск 2021

# **Обоснование актуальности, цели и задачи разработки ПИБ в Интернет-магазине**

Актуальность разработки политики информационной безопасности для Интернет-магазина объясняется необходимостью создания механизма управления и планирования информационной безопасности. Также ПИБ позволяет совершенствовать следующие направления деятельности магазина:

* упорядочивание бизнес-процессов;
* обеспечение соответствия с правовыми нормами;
* улучшение имиджа и деловой репутации.

Цель системы обеспечения информационной безопасности — создание и постоянное соблюдение в Интернет-магазине условий, при которых риски, связанные с нарушением безопасности информационных ресурсов магазина, постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска.

Основными задачами деятельности по обеспечению информационной безопасности Интернет-магазина являются:

* своевременное выявление, оценка и прогнозирование источников угроз информационной опасности, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования систем магазина;
* снижение рисков магазина, связанных с использованием информационных технологий;
* создание условий для максимальной автоматизации выполнения различных операций и исключения ручных операций при условии минимизации рисков;
* своевременное выявление новых угроз;
* контроль состояния информационной безопасности на всех этапах жизненного цикла автоматизированных информационных систем;
* минимизация потерь магазина при реализации угроз информационной безопасности;
* обеспечение жизнедеятельности Интернет-магазина и безопасности его информационных ресурсов в условиях форс-мажорных обстоятельств (экономические и политические кризисы, природные и техногенные катастрофы, террористические угрозы и пр.);
* оптимизация затрат на обеспечение информационной безопасности;
* защита от вмешательства в процесс функционирования систем магазина посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
* разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам магазина — обеспечение доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей;
* обеспечение аутентификации пользователей, имеющих допуск в информационные сети и участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
* защита от несанкционированной модификации используемых в системах магазина программных средств, а также защиту систем от внедрения несанкционированных программ, включая компьютерные вирусы;
* защита информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

# **Объекты защиты**

Основными объектами защиты системы информационной безопасности в Интернет-магазине:

* информационные ресурсы, содержащие служебную тайну и конфиденциальную информацию, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Интернет-магазина, независимо от формы и вида ее представления;
* работники Интернет-магазина и его пользователи;
* информационная инфраструктура, включающая системы хранения, обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;
* Интернет-магазин как web-приложение – исходный код, база данных, сервер, соединение между клиентом и сервером;
* информационные процессы, связанные с денежными транзакциями и иными банковскими операциями.
* Любые информационные системы, используемые в отделах магазина: бухгалтерского учета, система отслеживания курьерских доставок, информационная система юридического отдела и др.

# **Основные угрозы и их источники**

Любое лицо, имеющее логический или физический доступ к информационным ресурсам и компонентам соответствующих информационных технологий (программному обеспечению и данным, средствам вычислительной техники, коммуникационному оборудованию и каналам связи) может являться потенциальным злоумышленником. При этом предполагается возможность сговора сотрудника магазина с внешним злоумышленником, но не сговор двух и более сотрудников магазина.

Целью злоумышленника является получение контроля над информационным ресурсом, приводящего к нарушению его доступности, целостности или конфиденциальности.

Для достижения целей злоумышленник может использовать все экономически соизмеримые с потенциальным ущербом способы проведения атак на всех уровнях архитектуры информационных систем.

Источниками угроз информационным ресурсам Интернет-магазина являются:

* внешние и внутренние злоумышленники;
* ошибочные действия персонала или пользователя;
* вирусные атаки;
* отказы и сбои оборудования и программного обеспечения;
* недостаточная надежность банковских транзакций;
* недостаточная защищенность соединения;
* отсутствие противовирусной защиты;
* недочеты в конфигурациях безопасности баз данных и серверов;

# **Оценка угроз, рисков и уязвимостей**

Цель оценивания рисков состоит в определении характеристик рисков для Интернет-магазина и его ресурсов. На основе этих данных будут выбраны необходимые средства управления информационной безопасностью.

Для оценки рисков необходима шкала для численной оценки рисков от несанкционированного доступа (НСД) к информационным ресурсам магазина, которая представлена в таблице 4.1.

Таблица 4.1 – Условная численная шкала для оценки ущерба

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Последствий нет |
| 1 | Незначительные последствия |
| 2 | Минимальные последствия |
| 3 | Допустимые последствия |
| 4 | Значительные последствия |
| 5 | Высокая степень существенности последствия |

Следующим этапом является непосредственная оценка рисков с использованием ранее созданных шкал для оценки ущерба и вероятностно-временной. Оценка рисков Интернет-магазина представлена в таблице 4.3.

Таблица 4.3 – Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб \* Вероятность) |
| Взлом логинов/паролей пользователей | 4 | 0,5 | 2 |
| Перехват банковских транзакций | 5 | 0,6 | 3 |
| DOS-атака | 4 | 0,5 | 2 |
| Внедрение вирусного ПО | 5 | 0,4 | 2 |
| SQL-инъекции | 5 | 0,2 | 1 |
| Подделка межсайтовых запросов | 5 | 0,1 | 0,5 |
| Несанкционированный доступ к административным ресурсам | 5 | 0,3 | 1,5 |
| Аппаратные отказы | 5 | 0,4 | 2 |
| Колебания напряжения | 2 | 0,5 | 1 |
| Вредоносное программное обеспечение | 5 | 0,4 | 2 |
| Технические неисправности сетевых компонентов | 1 | 0,2 | 0,2 |
| Ненадлежащее использование ресурсов | 2 | 0,1 | 0,2 |
| Программные сбои | 3 | 0,4 | 1,2 |
| Итого | 51 | 4,4 | 18,6 |

Таким образом, можно сделать выводы, что наиболее уязвимыми активами являются персональные данные и настройки безопасности приложения, а также аппаратное и программное обеспечение.

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

# **Назначение и распределение ролей, обеспечение доверия к персоналу**

«Ролевое» управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах.

Роли формируются с учетом принципа минимальности полномочий.

Ни одна роль не должна позволять пользователю проводить единолично критичные операции.

Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных системах без непосредственного доступа к данным.

В критичных системах по решению владельца информационного ресурса может вводиться роль администратора информационной безопасности автоматизированной системы, в функции которого входит подтверждение прав и полномочий пользователей, заведенных в системе ее администратором.

Должностные обязанности сотрудников и трудовые договоры предусматривают обязанности персонала по выполнению требований по обеспечению информационной безопасности.

Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным нарушениям, доводятся до всех сотрудников Университета под роспись.

# **Управление доступом к информационным ресурсом и регистрация**

Все информационные ресурсы Интернет-магазина идентифицируются, категорируются и имеют своих владельцев.

Доступ к информационным ресурсам всем сотрудникам магазина предоставляется только на основании документально оформленных заявок, согласованных с их владельцами. По умолчанию определяется отсутствие доступа.

Доступ к информационным ресурсам не предоставляется (прекращается) в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения сотрудника.

Проводится периодический формальный контроль соответствия согласованных и реальных прав доступа к информационным ресурсам текущему статусу пользователя.

Прямой доступ пользователей к базам данных не предоставляется.

Доступ к открытым ресурсам магазина осуществляется без авторизации пользователей.

Регистрация пользователя Интернет-магазина осуществляется с предоставлением реальной электронной почты либо телефонного номера. Успешная регистрация подтверждается высланным кодом/ссылкой/письмом для активации аккаунта.

Доступ к ресурсам, подразумевающий защищаемые операции, осуществляется только после авторизации пользователя, прошедшего проверку надежности.

Журналы аудита действий пользователей и администраторов автоматизированных систем должны быть информативны‚ защищены от модификации и храниться в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов, связанных с нарушением информационной безопасности.

# **Управление жизненным циклом автоматизированных систем**

Процедуры по обеспечению информационной безопасности предусматриваются на всех стадиях жизненного цикла автоматизированных систем: при разработке (приобретении), эксплуатации, модернизации, снятии с эксплуатации.

Разработка, тестирование автоматизированных систем отделяются от эксплуатации.

Разработчики программного обеспечения не допускаются к его промышленной эксплуатации.

Разработка и тестирование программного обеспечения проводятся на выделенных физически или логически средствах вычислительной техники (виртуальные серверы), не использующихся для промышленной эксплуатации автоматизированных систем.

В контрактах со сторонними разработчиками на поставку систем предусматривается их ответственность за наличие в системах скрытых недокументированных возможностей, ведущих к ущербу для Интернет-магазина, а также соблюдение условий конфиденциальности.

Все изменения, вносимые в автоматизированные системы, контролируются и документируются. Дистрибутивные комплекты и исходные тексты систем собственной разработки, а также дистрибутивные комплекты приобретаемых систем хранятся в ИТ-Управлении.

В состав документации на критичные автоматизированные системы в обязательном порядке входит документация по обеспечению ее информационной безопасности.

Ввод автоматизированных систем в эксплуатацию производится только после их аттестации на соответствие предъявленным требованиям по информационной безопасности. Не допускается эксплуатация автоматизированных систем, не прошедших аттестации или имеющих не устранённые критичные замечания.

При выводе автоматизированной системы из эксплуатации или замене входящего в ее состав оборудования осуществляется принудительное удаление информации с соответствующих машинных носителей и из памяти компьютеров за исключением ведущихся в установленном порядке контрольных архивов электронных документов.

# **Антивирусная защита**

Каждый сотрудник Интернет-магазина обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать СИБ при подозрениях на вирусное заражение.

Антивирусная защита обеспечивается использованием специализированного программного обеспечения на production-сервере приложения.

Для снижения влияния человеческого фактора, исключения возможности отключения или отсутствия обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится централизованно автоматизированном режиме. При этом обеспечивается минимально возможный период обновления.

При невозможности централизованного обновления антивирусного и системного ПО периодичность, сроки и порядок проведения соответствующих мероприятий определяются оценкой имеющихся рисков вирусного заражения критичных информационных ресурсов и техническими возможностями такого обновления.

# **Использование криптографических средств защиты информации**

Применение средств криптографической защиты информации для обеспечения безопасности информационных ресурсов Интернет-магазина и взаимодействия со сторонними организациями производится в соответствии с порядком, установленным государственными уполномоченными органами.

Использование средств ЭП обеспечивает целостность электронного документа и подтверждение авторства подписавшей его стороны и является лучшей практикой организации электронного документооборота при взаимодействии с контрагентами.

Во внутренних системах магазина механизмы криптографического контроля целостности используются в зависимости от результатов оценки рисков информационной безопасности.

Конфиденциальность информации при передаче по публичным сетям и внешним каналам связи обеспечивается обязательным применением шифрования.

Риски, связанные с возможной компрометацией криптографических ключей или доступом к защищаемой информации в обход средств криптографической защиты, должны минимизироваться специальными техническими и организационными мерами.

Уязвимые данные пользователей, такие как логины, пароли, банковские данные, история покупок требуют надежного хранения, подразумевающего их шифрование. Зашифрованные данные, извлеченные из базы данных / хранилища не санкционированно, все еще защищены шифром, так как злоумышленнику недоступны ключи шифрования.

Генерация ключей шифрования должна быть автоматизирована, доступ к этому процессу нежелательно предоставлять лицам даже с самым высоким уровнем ответственности.

Ключи шифрования должны обновляться с учетом частоты появления новых данных и атак злоумышленников.

# **Обеспечение непрерывности бизнеса при сбоях**

Непрерывность критичных процессов при наступлении отказов и сбоев обеспечивается резервированием оборудования, каналов связи, резервным копированием информации, регулярной проверкой их работоспособности и адекватности. Процедуры восстановления после сбоев документируются в соответствующих регламентах и планах.

# **Обеспечение физической безопасности**

Физическая безопасность информационных систем Интернет-магазина сводится к охране серверного помещения – укрепление самого помещения, обеспечение бесперебойным электропитанием, установка камер видеонаблюдения, ограниченный доступ в помещение – вход по пропускам.

Информационная система магазина также включает в себя систему безопасности на складах/помещениях с товаром. Доступ третьих лиц в эти помещения должен быть ограничен, так как хищение товаров несет прямые убытки магазину. Для обеспечения безопасности этих помещений нужно предусмотреть доступ по пропускам, видеонаблюдение, а также защиту журналов поставок и продаж для контроля за количеством товаров и предотвращения краж.

Система оповещения надлежащих органов о пожарах, кражах и других ЧС также входит в комплекс мер по организации безопасности магазина.

**Выводы и предложения**

Таким образом, можно сделать выводы, что наиболее уязвимыми активами являются персональные данные и сведения, содержащие служебную тайну, а также аппаратное и программное обеспечение.

В результате проведенного анализа системы информационной безопасности были выявлены основные угрозы информационной безопасности, произведена оценка риска рисков и выработаны основные меры по защите информации. Кроме того, следует соблюдать ряд общих требований:

* До ввода в эксплуатацию программное обеспечение должно пройти проверку качества.
* Доступ к служебной информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.
* Доступ к открытым ресурсам магазина осуществляется без авторизации пользователя.
* Доступ к операциям, связанным с оформлением заказа и оплатой осуществляется только авторизованным пользователем, прошедшим проверку надежности.
* Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.
* Сотрудники должны проходить регулярное обучение в области информационной безопасности.
* Отдел автоматизации отвечает за определение детальных требований информационной безопасности и контролирует их исполнение в образовательных учреждениях.

Чтобы ограничить доступ к информации, содержащей персональные данные и служебную информацию, необходимо принять следующие меры:

* Специалист автоматизации обеспечивает защиту отдельных файлов и программ от чтения, удаления, копирования лицами, не допущенными к этому.
* Доступ к административным ресурсам магазина открыт лишь лицам с требуемым уровнем ответственности и надлежащей подготовкой.
* Категорически запрещается снимать несанкционированные копии с носителей информации, знакомить с содержанием электронной информации лиц, не допущенных к этому.
* Доступ к персональным данным должен быть описан в «Положения о защите персональных данных»

Для обеспечения физической защиты информации:

* Все объекты критичные с точки зрения информационной безопасности находятся в отдельном помещении, доступ в которое разрешен только сотрудникам, имеющими соответствующее разрешение от руководства компании.
* Вход в помещение осуществляется через дверь, оснащенную замком. Копии ключей находятся на вахте и у обслуживающего персонала.
* Помещение оборудовано вентиляцией и пожарной сигнализацией.
* Ключевые носители, программное обеспечение, документы и прочая конфиденциальная информация хранится в сейфах.
* Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право, находится в помещении в связи с выполнением своих должностных обязанностей.

Для обеспечения безопасности при работе с Интернет:

* Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.
* Сотрудники магазина не должны использовать сеть Интернет для хранения корпоративных данных.
* Специалист автоматизации имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.