МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.03 –	Информационная безопасность автоматизированных систем
Специализация -	Защищенные автоматизированные системы управления

ДИПЛОМНАЯ РАБОТА

на тему

МЕТОДИКА РАЗРАБОТКИ КОМПЛЕКСА СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТ-МАГАЗИНА

Студент _____ Агапчев Иван Сергеевич

Руководитель _____ Мали В.А.

Нормоконтролёр _____ Егорова Н.А.

Рецензент инженер 2 кат. АО “НПП Рубин” _____ Яшин Е.В.

Работа допущена к защите (протокол заседания кафедры от 16.06.23 № 10)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой хорошо (протокол заседания ГЭК от 27.06.23 № 2)

Секретарь ГЭК _____ А.П. Иванов

Пенза 2023

Содержание

Введение 5

1 Разработка и описание жизненного цикла создания безопасного интернет-магазина 7

1.1 Жизненный цикл разработки защищенных приложений, представленный Microsoft 7

1.2 Жизненный цикл разработки безопасного интернет-магазина ... 9

1.2.1 Составление модели жизненного цикла разработки безопасного интернет-магазина 9

1.2.2 Составление требований к информационной безопасности интернет-магазина 10

1.2.3 Безопасная разработка 12

1.2.3.1 Разработка модели угроз информационной безопасности при реализации разработки интернет-магазина 12

1.2.3.2 Проведение статического и динамического тестирования 13

1.2.3.3 Проведение функционального тестирования 16

1.2.3.4 Проведение фаззинг-тестирования 17

1.2.4 Безопасное развертывание 18

1.2.4.1 Внедрение дополнительных систем для большей безопасности приложения 18

1.2.4.2 Наличие SSL-сертификата 19

1.2.4.3 Проверка на наличие наиболее популярных уязвимостей 21

1.2.4.4 Проведение тестирования на проникновение ... 21

1.2.4.5 Выполнение требований для сертификации PCI DSS 22

1.2.5 Безопасное использование 24

2 Разработка комплекса средств для информационной безопасности интернет-магазина 26

2.1 Разработка модели жизненного цикла безопасного интернет-магазина 26
2.2 Проверка системы с помощью модели угроз STRIDE и разработанной модели угроз персональных данных 26
2.2.1 Составление модели угроз STRIDE 26
2.2.2 Составление модели угроз персональных данных 27
2.3 Использование статического анализатора кода SonarQube 28
2.3.1 Установка необходимых компонентов 28
2.3.2 Настройка подключения к SQL серверу 28
2.3.3 Настройка SonarQube 28
2.3.4 Запуск Sonar Scanner 30
2.4 Проведение функционального тестирования ручным и автоматическим способом 30
2.4.1 Проведение тестирования ручным способом 30
2.4.2 Использование Selenium WebDriver для автоматического функционального тестирования интернет-магазина 33
2.4.2.1 Установка необходимых компонентов 33
2.4.2.2 Создание теста с помощью Selenium WebDriver 34
2.5 Использование Burp Suite Intruder для фаззинг-тестирования интернет-магазина 35
2.5.1 Установка и настройка компонентов Burp Suite 35
2.5.2 Запуск фаззинг-тестирования 36
2.6 Использование OWASP ZAP для проведения тестирования на проникновение 36
2.7 Внедрение системы разграничения доступа 38
2.8 Внедрение парольной политики 40
2.9 Внедрение системы хеширования паролей с добавлением оригинальных дополнительный данных для каждого регистрируемого пользователя 41
2.10 Установка SSL сертификата 42

2.11 Использование сервиса Cloudflare 42
2.11.1 Подключение сайта к сервису Cloudflare 42
2.11.2 Настройка WAF Cloudflare 44
2.11.3 Установка HTTPS протокола на Cloudflare 45
2.12 Проведение регулярного резервного копирования сайта 45
3 Разработка модели угроз информационной безопасности интернет-магазина 47
3.1 Общие положения 47
3.2 Описание систем и сетей и их характеристика как объектов защиты 49
3.3 Возможные негативные последствия от реализации (возникновения) угроз безопасности информации 51
3.4 Возможные объекты воздействия угроз безопасности информации 52
3.5 Источники угроз безопасности информации 55
3.6 Способы реализации (возникновения) угроз безопасности информации 62
3.7 Возможные уязвимости 63
3.8 Актуальные угрозы безопасности информации 63
3.9 Меры защиты от выявленных угроз 64
4 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие . 89
Заключение 91
Список используемых источников 92

Введение

Каждый день в интернете появляется множество новых интернет-магазинов, предоставляющих различные товары и услуги. В современном мире существует несколько вариантов создания интернет-магазина, но все они могут быть подвержены атакам злоумышленников. Согласно исследованию Positive Technologies [1] нарушители могли проводить атаки на пользователей веб-приложений в 98% случаях.

Часто неопытные разработчики допускают множество ошибок в процессе разработки или настройке сайта, начиная от выбора сомнительного хостинга и заканчивая установкой вредоносного программного обеспечения на свой персональный компьютер. Этим и пользуются злоумышленники. К последствиям взлома можно отнести утечку персональных данных пользователей, размещение вредоносного программного обеспечения на взломанном сайте, подмены информации на сайте или же полное удаление всего сайта. Не редко малоизвестные сайты не могут продолжать поддерживать работоспособность своего сайта из-за отсутствия навыков и опыта при взломе.

Одной из главных причин взлома являются уязвимости, которые были допущены самими разработчиками в процессе разработки веб-приложения. Чтобы уменьшить шанс взлома сайта, необходимо постоянно углубляться в тематику безопасности разрабатываемого приложения и придерживаться основным правилам администрирования веб-приложения, чтобы уменьшить возможности злоумышленников и лучше обезопасить свой сайт.

Целью настоящей дипломной работы является разработка методики разработки комплекса средств для обеспечения информационной безопасности интернет-магазина.

Одним из самых первых действий при создании безопасного интернет-магазина является выбор, каким именно способом будет разработан интернет-магазин, так как от этого будут зависеть дальнейшие способы его управления и

модификации. В настоящее время существуют три основных способа реализации интернет-магазина, включающие:

– создание с помощью конструкторов сайтов;
– создание при помощи CMS;
– создание при помощи различных специализируемых фреймворков.

В данной методике будут рассматриваться только два последних варианта, так как при использовании конструкторов отсутствует возможность как-то влиять на код или безопасность создаваемого сайта. Представленные методы защиты подойдут к обоим способам реализации интернет-магазина, несмотря на их особенности в разработке.

Данная методика подойдет владельцам интернет-магазинов для грамотного составления требований к безопасности сайта, а также подойдет самим разработчикам для осуществления структурированной и поэтапной разработки безопасного веб-приложения.

В качестве операционной системы будет использована Windows 10 (microsoft.com). Хостинг будет использоваться от компании TimeWeb (timeweb.com).

1 Разработка и описание жизненного цикла создания безопасного интернет-магазина

1.1 Жизненный цикл разработки защищенных приложений, представленный Microsoft

На сегодняшний день одной из главных задач для успешной разработки любого программного обеспечения (в том числе и сайта) является составление жизненного цикла разработки. В данной методике за основу будет взят жизненный цикл разработки безопасного программного обеспечения Microsoft (Microsoft SDL) [2] и жизненный цикл, рассматриваемый в ГОСТ Р 56939 – 2016 [3].

Компания Microsoft представила свою модели жизненного цикла разработки безопасных приложений еще в далеком 2004 году. Несмотря на дату выпуска данная модель разработки продолжает успешно функционировать в наше время. Жизненный цикл представлен на рисунке 1.

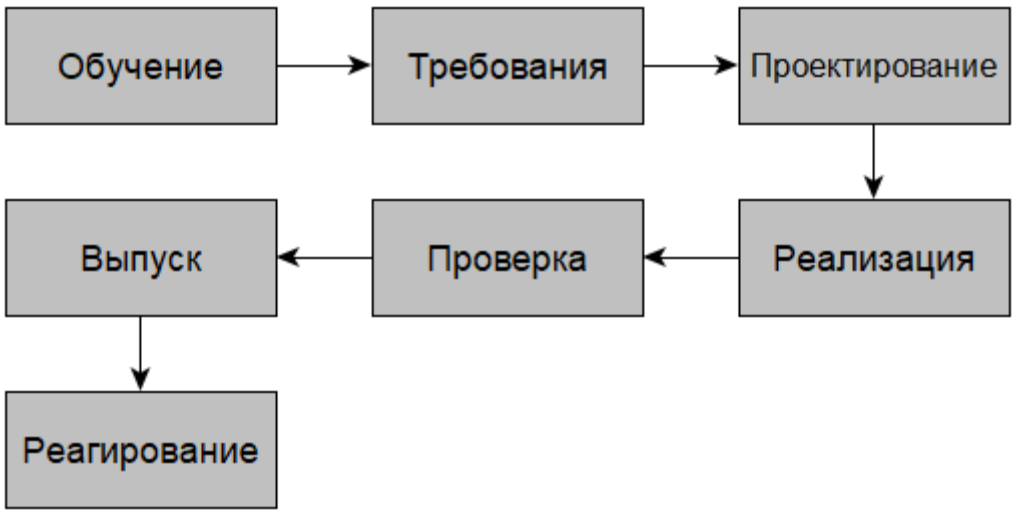

Рисунок 1 – Жизненный цикл разработки представленный Microsoft SDL

Представленный выше жизненный цикл включает следующие этапы:

– обучение. Данный этап заключаться в обучении сотрудников по всем вопросам безопасности;

– требования. На данном этапе определяются все требования к безопасности и конфиденциальности разрабатываемой системы. Данный этап

является одним из самых важных при разработке безопасного программного обеспечения;

– проектирование. После определения всех требований безопасности начинается стадия проектирования, которая более детально рассматривает вопросы безопасности и конфиденциальности разрабатываемой системы. На данном этапе также необходимо разработать модель рисков и угроз информационной безопасности. Если решение данных вопросов выполняется в самом начале жизненного цикла проекта, то они обходятся гораздо дешевле как по времени, так и по финансам;

– реализация. Данный этап начинается с написания кода в соответствии с требованиями, представленными на предыдущих этапах. Помимо простого написания кода проводят статический и динамический анализ кода;

– проверка. После реализации всех требований и планов по разработке начинается этап полной проверки приложения на наличие ошибок и уязвимостей;

– выпуск. В момент завершения всех тестов и проверок безопасности конечный продукт не сразу выпускается для всех клиентов. Сборки выпускаются постепенно в более крупные группы людей, включающие группу разработчиков, группу бета-тестеров и группу всех основных клиентов по всему миру;

– реагирование. После выпуска продукт постоянно анализируется и отслеживается в целях выявления потенциальных угроз и уязвимостей информационной безопасности.

Представленная модель жизненного цикла является базовой и подходит как для крупных компаний, так и для людей, разрабатывающих программное обеспечение в одиночку. Однако данная модель описывает все этапы достаточно базово и без какой-либо конкретики по выполнению действий на каждом этапе.

На основе представленной модели жизненного цикла и ГОСТ Р 56939 – 2016 [3] был составлен жизненный цикл для разработки безопасного интернет-магазина.

1.2 Жизненный цикл разработки безопасного интернет-магазина

1.2.1 Составление модели жизненного цикла разработки безопасного интернет-магазина

Представленная модель жизненного цикла включает в себя 4 основных этапа, которые будут использоваться в процессе разработки. Однако стоит отметить, что жизненный цикл – это непрерывный процесс, который может дополняться и изменятся на любом из представленных этапов. Жизненный цикл разработки безопасного интернет-магазина представлен на рисунке 2.

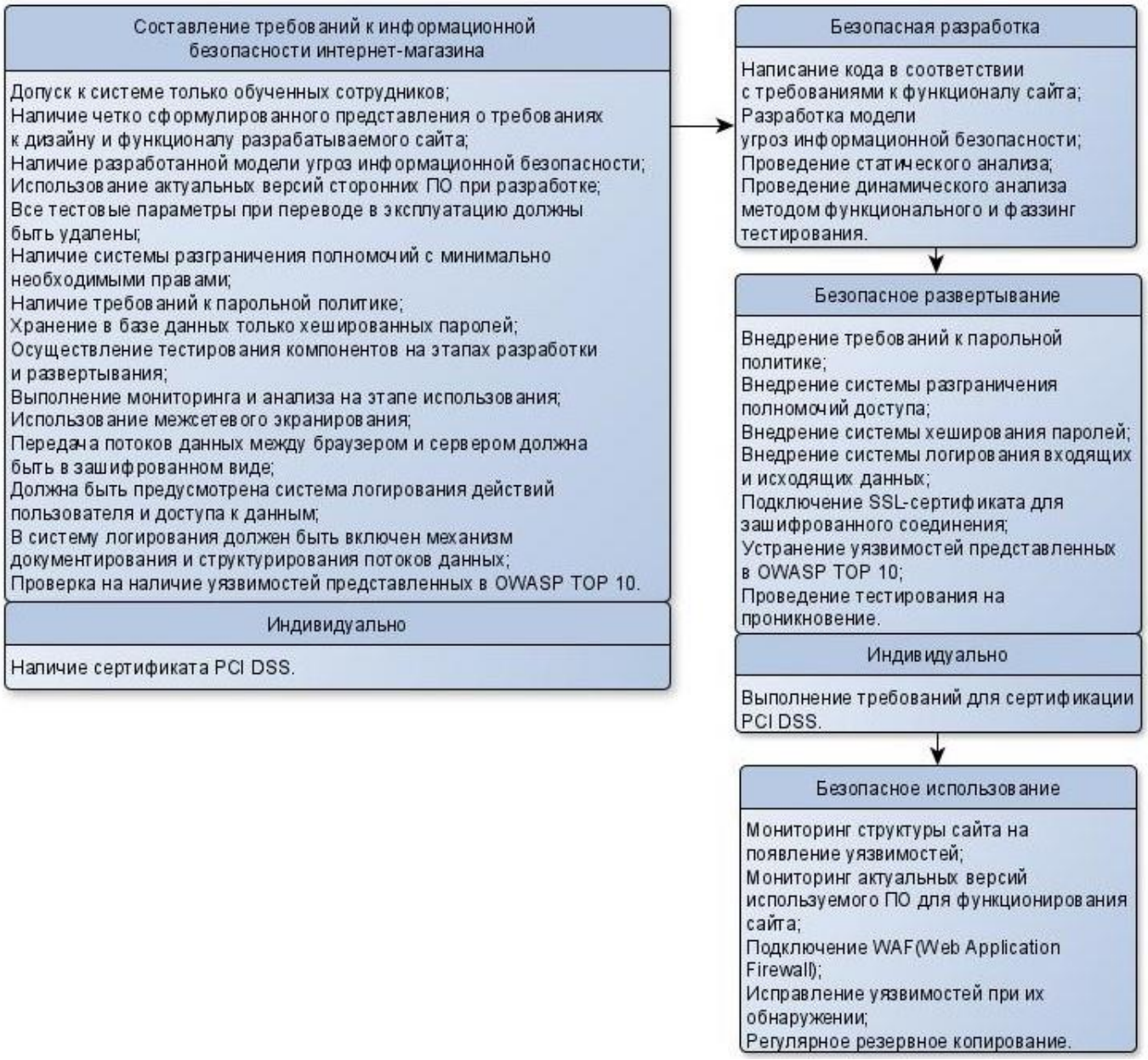

Рисунок 2 – Жизненный цикл разработки безопасного интернет-магазина

1.2.2 Составление требований к информационной безопасности интернет-магазина

Данный этап является самой первой и одной из самых важных стадий в процессе разработки безопасного интернет-магазина, так как на нем создаются и утверждаются требования, которые разработчик должен выполнять на всех этапах разработки. На данном этапе стоит отметить такие пункты как:

– допуск к системе только обученных сотрудников. Обучение администраторов затрагивает все основные вопросы безопасности системы интернет-магазина, им также предоставляется вся необходимая документация и правила, требуемые при работе в системе;

– наличие четко сформулированного представления о требованиях к дизайну и функционалу разрабатываемого сайта. В данном пункте разрабатываются бизнес-требования к продукту, учитываются запросы и потребности пользователей, определяются ограничения проекта. В конечном итоге должны быть определены ответы на вопросы “Какие задачи должен выполнять разрабатываемый сайт?” и ”Какой продукт в итоге требуется создать?”;

– наличие разработанной модели угроз информационной безопасности интернет-магазина. При создании модели угроз в процессе проектирования осуществляется выявление, классификация и оценка потенциальных рисков. Данная модель должна поддерживаться и регулярно обновляться по мере внесения изменений в проект на протяжении всего жизненного цикла разработки;

– использование актуальных версий сторонних ПО при разработке. В процессе разработки стоит учесть версии используемых сторонних приложений и библиотек, так как в них тоже могут выявляться уязвимости;

– все тестовые параметры при переводе в эксплуатацию должны быть удалены. Часто в процессе интеграции применяются конфиденциальные данные, что может повлечь за собой возможность их утечки. Рекомендуется запускать

тестовые данные в рамках эксперимента, после чего их следует изменить или удалить перед переносом в рабочую среду;

– наличие системы разграничения полномочий с минимально необходимыми правами. Для правильной работы системы необходимо внедрить механизм контроля доступа, который может быть основан на ролевой или смешанной модели доступа;

– наличие требований к парольной политике. Одними из самых популярных и опасных уязвимостей являются уязвимости, связанные с легкостью получения пароля пользователя злоумышленником. Именно поэтому необходимо разработать и реализовать требования к парольной политике;

– хранение в базе данных только хешированных паролей. В базе данных должны храниться только хеши паролей, которые будут проверяться каждый раз при попытке авторизации на сайте;

– осуществление тестирования компонентов на этапах разработки и развертывания. В процессе разработки и развертывания необходимо проводить регулярные тесты на наличие ошибок и уязвимостей. Тесты могут проводиться как в ручном, так и в автоматическом режиме;

– выполнение мониторинга и анализа на этапе использования. Данное требование реализуется с помощью инструмента, который контролирует активность приложения и базы данных интернет-магазина, с последующим логированием полученных данных в случае выявления подозрительных действий;

– использование межсетевого экранирования. Данное требование обуславливается необходимостью контроля поступающего трафика к веб-приложению в режиме реального времени с целью блокирования потенциальных атак на сайт;

– передача потоков данных между браузером и сервером должна быть в зашифрованном виде. Различные данные пользователей должны передаваться по SSL/TLS протоколу;

– должна быть предусмотрена система логирования действий пользователя и его доступа к данным. В данной системе должны присутствовать все основные данные, необходимые для успешного мониторинга или же сбора статистики. Однако стоит учесть, что в логах не должно присутствовать критичных данных;

– в систему логирования должен быть включен механизм документирования и структурирования потоков данных. Данный механизм значительно упростит контроль и поддержку разработанного приложения;

– проверка на наличие уязвимостей, представленных в OWASP TOP TEN [4]. Перед итоговой публикацией стоит повторно проверить всю систему на наличие наиболее популярных уязвимостей;

– наличие сертификата PCI DSS. Данный сертификат необходим для подтверждения соответствия организации стандартам безопасности данных, использующихся в процессе обработки платежных карт. Однако данный сертификат необходим только если компания собирает, обрабатывает и хранит данные банковских карт в своей системе.

После составления всех необходимых требований можно переходить на этап безопасной разработки, включающий в себя составление, разработку и тестирование основных функциональных составляющих безопасного интернет-магазина.

1.2.3 Безопасная разработка

1.2.3.1 Разработка модели угроз информационной безопасности при реализации разработки интернет-магазина

Наиболее часто встречающиеся угрозы в процессе разработки описываются в ГОСТ Р 58412 – 2019 [5]. Данный документ можно брать как основу для составления модели угроз, так как он содержит 19 высокоуровневых угроз, возникающих на каждом этапе жизненного цикла разработки безопасного приложения.

Кроме представленного документа можно использовать и другие источники для моделирования угроз в рамках разработки, например использовать модель угроз STRIDE [6], являющейся компонентом используемой Microsoft SDL [2]. Данная модель включает в себя не только основные составляющие безопасности информации (конфиденциальность, доступность, целостность), но и добавляет такие классификации как подлинность, неотказуемость и достоверность (повышение привилегий). Модель угроз STRIDE позволяет расширить традиционный подход к оценке безопасности информации и взглянуть на информационную систему с позиции злоумышленника.

Однако следует отметить, что представленные модели угроз используются для идентификации угроз безопасности при реализации разработки веб-приложения и не рассматривают конкретные риски и угрозы, связанные с персональными данными посетителей интернет-магазина. Поэтому модель угроз информационной безопасности персональных данных стоит разработать отдельно.

1.2.3.2 Проведение статического и динамического тестирования

Во всем цикле разработки необходимо проводить статическое и динамическое тестирование.

Основными различиями данных тестов является то, что статическое тестирование производится без запуска итоговой программы. Данный вид тестирования проверяет сам код на наличие некорректного синтаксиса, присутствие в коде незадействованных переменных или переменных с неизвестными значениями, а также осуществляет проверку на мёртвый код или бесконечные циклы. Что касается динамического тестирования, то оно проводится уже с запущенным приложением и осуществляет проверку правильности выполнения программы. Другими словами, динамическое тестирование позволяет находить ошибки, возникающие при работе пользователя с приложением, а также позволяет разработчикам тестировать

приложение и выявлять недостатки, которые не были обнаружены обычными тестами. Наиболее популярными методами динамического тестирования является тестирование методом черного, серого и белого ящика.

Тестирование черного ящика означает тестирование приложения без проверки внутренней структуры кода.

Тестирование белого ящика подразумевает тестирование структуры макета и кода приложения. При реализации данного метода код будет заметен тестеру.

Тестирование серого ящика подразумевает гибрид тестирования методом черного и белого ящика, так как тестировщику будут известны некоторые особенности реализации тестируемой системы.

Как статическое, так и динамическое тестирование может осуществляться как в ручном, так и в автоматическом режиме с использованием специальных программ. При ручном тестировании разработчику необходимо осуществлять проверку от правильности написания кода до правильного и бесперебойного выполнения программы, опираясь только на свой опыт, силы и знания. При использовании автоматического режима тестирования будут использоваться специализированные программы, позволяющие проводить тестирование всех компонентов разрабатываемой системы. Однако при выборе статического анализатора стоит учесть, какие языки программирования поддерживает выбранное средство. Перечень наиболее популярных средств для проведения статического анализа кода веб-приложения представлен в таблице 1.

Таблица 1 – Наиболее популярные средства для статического анализа кода

Название	Характеристики			
	Особенности	Цена	Поддерживаемые языки программирования	Дата последнего обновления
Embold	В бесплатной версии за одну проверку можно проверить максимум 20 000	Присутствует как бесплатная, так и платная версия.	Java, C,C++, TypeScript,JavaScript, HTML, CSS, SASS, Python PHP, C#, Objective-C, Go,	Последнее обновление: 6 марта 2023 года.

Продолжение таблицы 1

Название	Характеристики			
	Особенности	Цена	Поддерживаемые языки программирования	Дата последнего обновления
	строк кода.		Kotlin, Solidity, SQL.	
SonarQube	Поддержка многих языков веб-программирования; Простота проверки кода; Формирование детальных отчетов по анализу.	Присутствует как бесплатная, так и платная версия.	Поддерживает более 30 различных языков программирования.	Последнее обновление: апрель 2023 года.
Solar appscreener		Лицензии на проекты оцениваются в зависимости от размера и тестируемого проекта.	Поддерживает 30 различных языков программирования.	Последнее обновление: 5 мая 2021 года.
Услуги провидения статического анализа сторонними компаниями	Постоянная обратная связь с заказчиком; Наиболее подробное описание каждого обнаружения со снимками экрана и советами по исправлению.	Стоимость зависит от количества и сложности выполняемой работы.	Все возможные языки программирования.	-

В рамках настоящей методики, для статического тестирования кода веб-приложения будет использоваться программа SonarQube (sonarsource.com/products/sonarqube/).

Как было сказано ранее, при динамическом тестировании веб-приложения происходит отправка запросов, эмулируется действие пользователя, происходит нажатие на кнопки в пользовательском интерфейсе, а также осуществляется передача на сервер искусственных данных, таких как скобки, кавычки и символы в различных кодировках. Главная цель заключается в том, чтобы изучить, как приложение работает, и как оно обрабатывает внешние данные. Перечень наиболее популярных средств для проведения динамического анализа веб-приложения представлен в таблице 2.

Таблица 2 – Наиболее популярные средства для динамического анализа

Название	Описание
Selenium IDE	Программное средство позволяющее в автоматическом режиме осуществлять нажатия на элементы пользовательского интерфейса в соответствии с заданными ранее тестами. Утилита является полностью бесплатной и устанавливается в качестве расширения в браузере. Основными недостатками является необходимость писать собственные тесты под каждую задачу, позволяет реализовать только легкие тесты, поддерживается только в браузере Firefox и Google Chrome.
Selenium WebDriver	Это фреймворк для автоматизации тестирования веб-приложений. Он позволяет тестировать веб-страницы, имитируя поведение пользователя и проверяя результаты. Selenium WebDriver работает с любым браузером, взаимодействуя с его элементами (например, нажимая на кнопки, заполняя поля ввода и т.д.). Он может быть использован на различных языках программирования, таких как Java, Python, Ruby и другие.
Burp Suite	Один из самых популярных динамических анализаторов. Имеет множество настроек для проведения различных тестов веб-приложения. Имеет как бесплатную(ограниченную) версию, так и платную.
Arachni	Высокопроизводительный сканер. Отличительной особенностью является наличие собственного веб-интерфейса для удобства проверки веб-приложения
OWASP ZAP	Полностью бесплатная утилита позволяющая выявлять уязвимости веб-приложений. Имеет большую базу данных для проведения тестирования на проникновение в систему

Из представленной таблицы можно понять, что большинство средств для динамического анализа имеют свои особенности, поэтому в рамках разрабатываемой методики будут использоваться несколько анализаторов, наиболее подходящих к каждому способу тестирования.

1.2.3.3 Проведение функционального тестирования

Функциональное тестирование проводится методом чёрного ящика, так как на данном этапе необходимо без доступа к коду провести проверку выполнения функциональных требований в соответствии со спецификацией для разработки. Несмотря на то, что конкретный магазин может иметь некоторые особенности, пользовательский сценарий типичен для любого интернет-магазина: вход на сайт, просмотр каталога, выбор товара, оформление заказа и оплата. Также зачастую в него добавляется регистрация и авторизация.

Чтобы процесс покупки в интернет-магазине был положительным, страницы должны ясно и понятно отображать необходимую информацию и не выходить за пределы привычного для покупателя сценария. Яркий дизайн и быстрая скорость страницы не помогут, если покупатель не сможет найти нужный товар или не поймет, как оформить заказ.

Часто функциональное тестирование проводится ручным способом путем создания чек-листа, в котором прописываются основные категории проверки и результаты, которые предположительно должны получиться. Однако для автоматизации проведения функционального тестирования веб-приложения можно использовать специальные программы, например Selenium WebDriver (selenium.dev). Selenium специализируется на кибербезопасности и представляет инструменты для составления и прохождения тестов с целью обнаружения ошибок и уязвимостей. Данный инструмент позволяет осуществлять функциональное тестирование и составлять собственные тесты, проверяющие работоспособность сайта, с последующим логированием полученных ошибок.

1.2.3.4 Проведение фаззинг-тестирования

Одним из тестов, входящих в динамическое тестирование, является фаззинг-тестирование. Данное тестирование необходимо для поиска аномального поведения веб-приложения. Реализуется данное тестирование путем передачи на вход приложению различных специально сгенерированных данных. Для проведения фаззинг-тестирования часто используются сторонние программы, например такие как Burp Suite (portswigger.net/burp). Данный инструмент позволяет составлять карты веб-приложения, осуществлять поиск файлов и папок, модификацию запросов, а также проводить фаззинг-тестирование. Пример интерфейса программы представлен на рисунке 3.

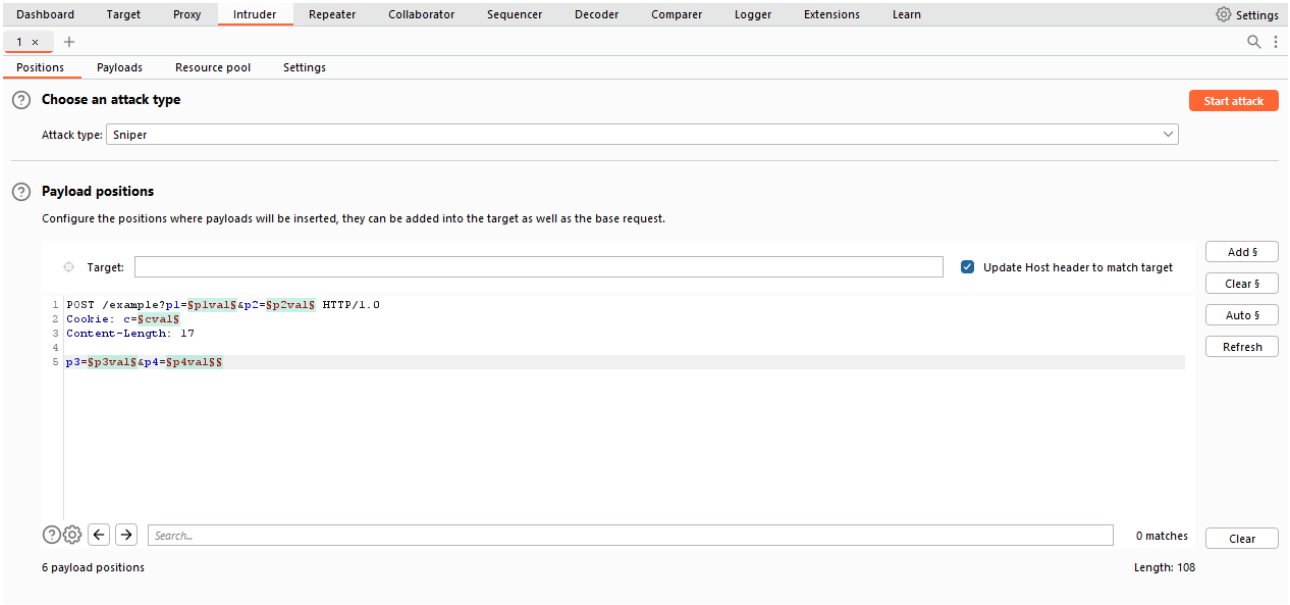

Рисунок 3 – Интерфейс Burp Suite Intruder

1.2.4 Безопасное развертывание

1.2.4.1 Внедрение дополнительных систем для большей безопасности приложения

После завершения этапа безопасной разработки начинается этап безопасного развертывания, включающий в себя создание, внедрение и использование дополнительных способов осуществления безопасности разрабатываемого продукта.

К наиболее необходимым к внедрению системам можно отнести:

– внедрение парольной политики;

– внедрение системы хеширования паролей;

– внедрение системы разграничения доступа;

– внедрение системы логирования входящих и исходящих данных;

– внедрение системы “Проверка на робота”.

Все представленные выше пункты можно реализовать собственными силами, если сайт магазина разрабатывается на основе фреймворка, или же с помощью устанавливаемых плагинов на используемую CMS (система управления контентом).

Под CMS понимается специальное ПО, которое позволяет создавать и управлять контентом на сайте. Это может быть как платный коммерческий продукт, так и бесплатный со свободным доступом к исходным кодам. В России наиболее популярными CMS являются OpenCart, 1С-Битрикс, Joomla! и WordPress. Однако согласно данным W3Tech [7], несомненным лидером является CMS система WordPress, на которой работают более 40% всех сайтов в интернете. Статистика представлена на рисунке 4.

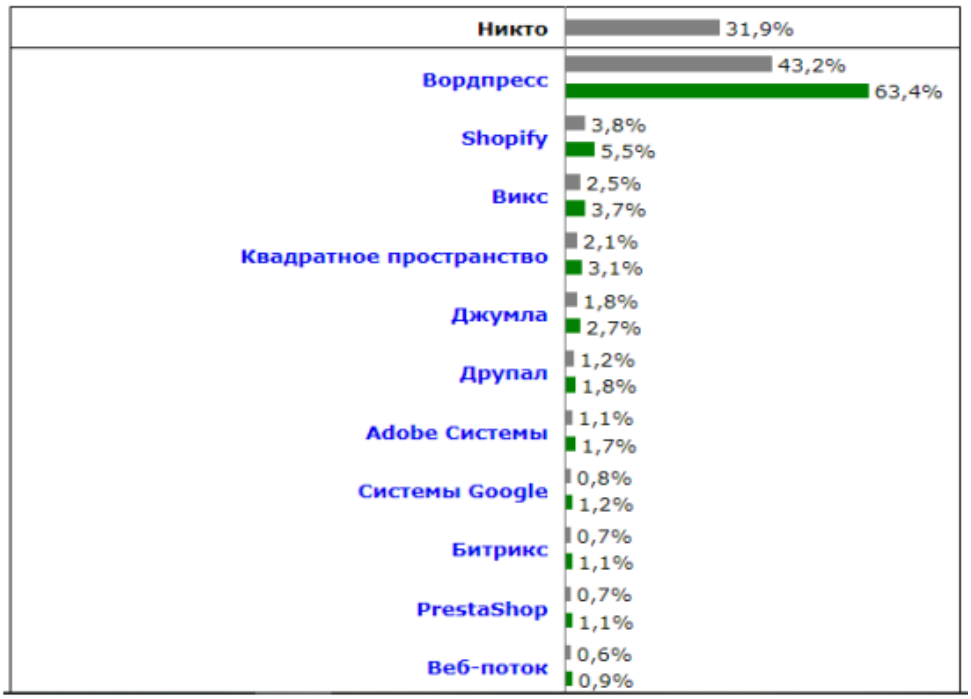

Рисунок 4 – Статистика используемых CMS по версии W3Tech

1.2.4.2 Наличие SSL-сертификата

SSL (secure sockets layer — уровень защищённых сокетов), является протоколом для безопасной связи с использованием криптографии. В последующих версиях он был заменен на TLS (безопасность транспортного уровня), но термин "SSL" все еще наиболее распространен для обозначения этого протокола.

Цель данного протокола заключается в обеспечении безопасной передачи данных. При этом для аутентификации используются асимметричные алгоритмы шифрования (пара открытый - закрытый ключ), а для обеспечения

конфиденциальности - симметричные алгоритмы (секретный ключ). К возможным типам сертификатов проверки можно отнести:

– сертификат, предоставляемый после расширенной проверки владельца веб-сервиса (EV SSL);

– сертификат, предоставляемый после подтверждения организации (OV SSL);

– сертификат, предоставляемый после подтверждения домена (DV SSL).

Когда пользователь открывает веб-сайт, его браузер запрашивает SSL-сертификат с открытым ключом у сервера. Браузер проверяет этот сертификат на совпадение с названием сайта и наличие корневого сертификата от надежного центра сертификации. Если проверка пройдена успешно, то браузер генерирует предварительный секрет (сочетание алгоритма шифрования и ключа) на основе открытого ключа и начинает общение с сервером, который расшифровывает секрет своим закрытым ключом. Если сервер готов продолжать общение с браузером, то обе стороны создают общий секрет на основе определенного вида шифрования и используют его для безопасной коммуникации на время текущей сессии. По завершении сессии ключ уничтожается, и при следующем посещении сайта процесс повторяется. Процесс прохождения аутентификации через SSL/TLS протокол представлен на рисунке 5.

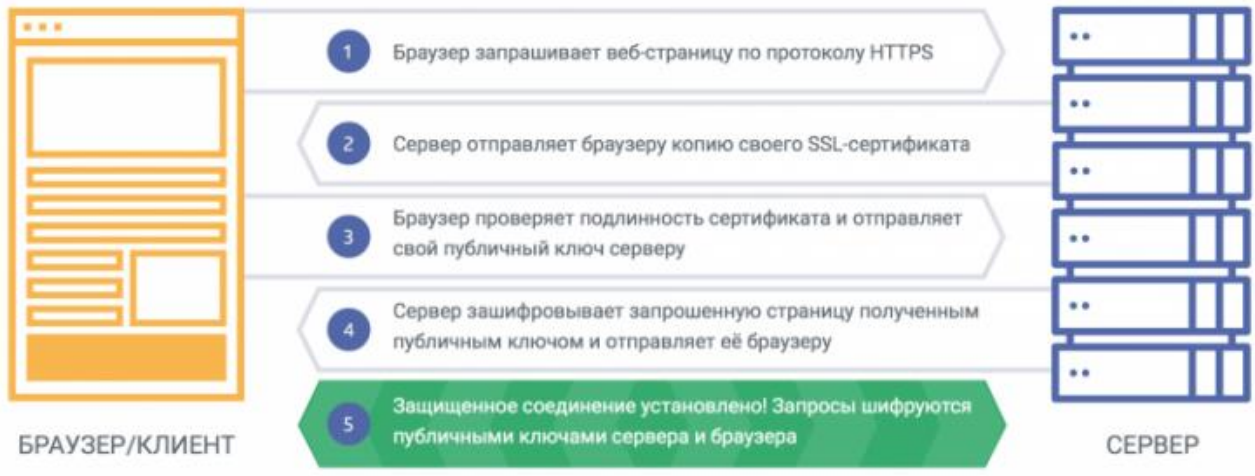

Рисунок 5 – Процесс прохождения аутентификации через SSL/TLS

1.2.4.3 Проверка на наличие наиболее популярных уязвимостей

На сегодняшний день существует множество источников, описывающих наиболее популярные уязвимости приложений. Однако наиболее востребованным считается “OWASP Top Ten – 2021” [4], включающий в себя список из десяти наиболее популярных категорий уязвимостей для любых приложений. Категории “OWASP Top Ten – 2021” включают в себя:

- A01 – Недостатки контроля доступа;
- A02 – Криптографические сбои;
- A03 – Инъекции;
- A04 – Небезопасное проектирование;
- A05 – Некорректная настройка параметров безопасности;
- A06 – Уязвимые и устаревшие компоненты;
- A07 – Недостатки идентификации и аутентификации;
- A08 – Недостатки проверки целостности ПО и данных;
- A09 – Недостатки журналирования и мониторинга;
- A10 – Подделка запросов со стороны сервера (SSRF).

Данный ресурс представляет не только основные категории, но и перечень недостатков безопасности для каждой из категорий с описанием способов их устранения.

1.2.4.4 Проведение тестирования на проникновение

Тестирование на проникновение чаще всего проводится методом черного ящика на готовом продукте. Данный метод тестирования также называется пентестингом и реализуется для обнаружения и эксплуатации возможных уязвимостей и недостатков, способных привести к нарушению конфиденциальности, целостности и доступности информации, спровоцировать некорректную работу системы или привести к отказу системы в обслуживании. Тестируя данным методом, тестировщик выступает в роли потенциального нарушителя и пытается обнаружить различные уязвимости в системе как в ручном, так и в автоматическом режиме.

В современной методологии тестирования различают три основных подхода:

– классический тест на проникновение. Особенностью данного подхода является поиск не всех уязвимостей в системе, а только тех, которые необходимы для достижения выбранных целей;

– сканирование на наличие уязвимостей. Данный подход заключается в полном сканировании системы на наличие известных уязвимостей. Сканирование можно проводить не только вручную путем исследования и сбора информации из доступных частей системы, но и с помощью сканеров уязвимостей. Сканеры проверяют наличие уязвимостей по своей базе данных. Одним из популярных сканеров является OWASP ZAP (zaproxy.org), имеющий множество функций и регулярно обновляющуюся базу уязвимостей;

– анализ конфигураций. Данный подход заключается в проверке всех настроек и компонентов, используемых в системе. Анализ конфигураций является самым безопасным способом проверки защищенности, так как не вносит изменения в структуру системы и не пытается вызвать потенциальные ошибки.

Стоит отметить, что для достижения полноценного тестирования не стоит пользоваться только одним из рассмотренных способов, так как при одиночном использовании они являются менее эффективными. Например, автоматический сканер уязвимостей может пропустить комбинации уязвимостей, которые в совокупности могут создать угрозу безопасности, а ошибки, обнаруженные при анализе конфигурации, не всегда могут приводить к реальной возможности проникновения.

1.2.4.5 Выполнение требований для сертификации PCI DSS

Сертификат PCI DSS (стандарт безопасности данных индустрии платежных карт) разработан крупнейшими платежными системами и позволяет подтвердить, что компания соответствует стандартам безопасности данных, использующихся в процессе обработки платежных карт. Данный сертификат

содержит более 250 различных требований к безопасности, которые необходимы для достижения определенной степени защиты. Для большей компактности данные требования можно разделить на 6 главных категорий защиты. Данные категории включают:

– защита данных карты. Хранение, передача и обработка данных карты должны быть защищены таким образом, чтобы минимизировать риск несанкционированного доступа;

– защита сети. В системе должны присутствовать внедрённые функции межсетевых экранов, а также иные способы защиты сети;

– управление уязвимостями. Регулярный мониторинг и тестирование безопасности должны быть проведены для идентификации и устранения уязвимостей в системе;

– управление контролем доступа. Доступ к данным, связанным с картами, должен быть строго управляемым и ограниченным только необходимым лицам;

– проведение мониторинга и журналирования. Внутренние системы должны непрерывно мониториться и логироваться, чтобы обеспечить быстрое обнаружение и реагирование на возможные инциденты;

– управление политиками информационной безопасности. В системе должны устанавливаться политики и процедуры для обеспечения безопасной работы с данными карт и защиты от угроз безопасности.

После реализации всех требований и написания всей необходимой документации, а также ознакомлением с документацией всех сотрудников, которые вовлечены в работу с данными карт, привлекается независимый аудитор, обладающий статусом QSA (квалификационный оценщик безопасности). Данный аудитор проверит знания сотрудников и систему на соответствие всех требований безопасности PCI DSS и на основе составленного отчета будет решать вопрос о выдаче соответствующего сертификата.

Если интернет-магазин не собирает данные карт и использует для оплаты сторонний онлайн-сервис, то наличие у интернет-магазина сертификата PCI DSS

не требуется. Однако стоит учесть, что используемый онлайн-сервис для оплаты должен соответствовать всем стандартам безопасности и ежегодно проходить сертификацию PCI DSS.

1.2.5 Безопасное использование

После завершения всех этапов разработки и проведения всех тестов, веб-приложение готово к публикации. Однако осуществление безопасности приложения на этом не останавливается, так как требуется постоянный мониторинг состояния систем на выявление новых уязвимостей или атак злоумышленников. Для данных задач могут использоваться сторонние приложения и расширения, например инструменты WAF, которые позволяют осуществлять проверку трафика в реальном времени.

Под Web Application Firewall (WAF) подразумевается защитный межсетевой экран позволяющий блокировать атаки на веб-приложения: SQL-инъекции, межсайтовый скриптинг, удаленное выполнение кода и обход авторизации. Данные межсетевые экраны обеспечивают защиту путем постоянного мониторинга входящего и исходящего трафика, а также содержимого всех веб-страниц сайта на наличие подозрительных изменений.

На сегодняшний день существует три основных типа межсетевых экранов:

– сетевой тип подключения. Развертывание происходит путем приобретения специализированных вычислительных устройств и подключения их к своей системе;

– программный тип подключения. Развертывание происходит путем подключения WAF в качестве дополнения для какого-либо ПО с последующей работой на одном сервере с ним;

– облачный тип развертывания. Развертывание происходит путем временной аренды услуг WAF какой-либо специализирующейся на этом компании.

Наиболее востребованным вариантом является облачное развертывание межсетевого экрана, так как в нем отсутствует необходимость в больших

затратах по времени и финансам. В качестве примера одного из популярных облачных межсетевых экранов можно привести Cloudflare WAF (cloudflare.com). Данное решение позволяет осуществлять по подписке постоянный мониторинг входящего и исходящего трафика, а также защищает веб-приложения от распространенных уязвимостей, таких как атаки с использованием SQL-инъекций, межсайтовый скриптинг, межсайтовые подделки, без изменений в существующей инфраструктуре. Пример работы межсетевого экрана представлен на рисунке 6.

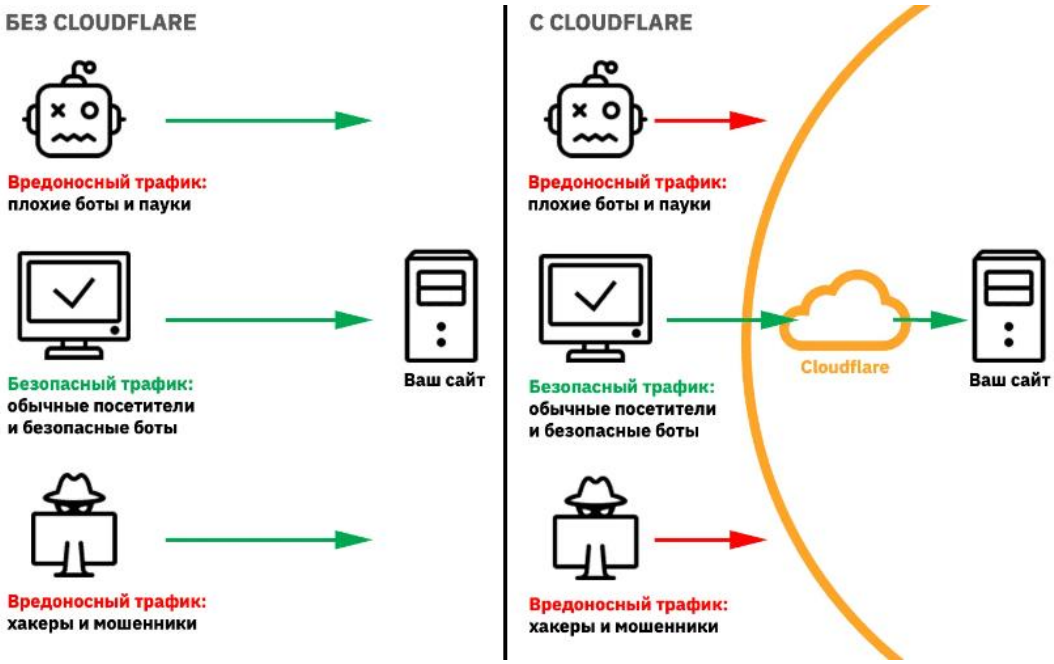

Рисунок 6 – Процесс работы межсетевого экрана (WAF)

Исходя из представленного жизненного цикла можно сделать вывод, что разработка, поддержание и развитие безопасного интернет-магазина является непрерывным и трудоемким занятием с постоянным изменением и добавлением новых элементов в его структуру.

2 Разработка комплекса средств для информационной безопасности интернет-магазина

2.1 Разработка модели жизненного цикла безопасного интернет-магазина

В рамках данной главы был составлен перечень средств для информационной безопасности как на этапах разработки, так и на этапе функционирования интернет-магазина. Представленные средства рассчитаны на нейтрализацию и устранение имеющихся угроз и уязвимостей в системе, а также на повышение степени защищенности уже работающей системы. Данный перечень является динамическим и может изменяться в соответствии с требованиями к системе.

Одной из основных мер защиты от угроз информационной безопасности является грамотная разработка модели жизненного цикла разработки безопасного интернет-магазина, включающей в себя этап составления требований к безопасности, этап безопасной разработки (написание кода, разработку модели угроз, проведение базовых тестирований), этап безопасного развертывания и безопасного использования готового продукта. Более подробное описание всех этапов представлено в первой главе настоящей методики.

2.2 Проверка системы с помощью модели угроз STRIDE и разработанной модели угроз персональных данных

2.2.1 Составление модели угроз STRIDE

После составления модели жизненного цикла интернет-магазина можно приступать к разработке модели угроз безопасности информации. Как уже отмечалось в первой главе настоящей методики, разработать модель угроз можно с помощью модели STRIDE [6]. Данная модель угроз позволяет взглянуть на систему глазами нарушителя и обхватить все основные аспекты проблем безопасности информационной системы путем ответа на вопросы:

– как нарушитель может выдать себя за другого пользователя? (Spoofing –

притворство);

– присутствует ли возможность изменения данных в системе и как это можно реализовать? (Tempering – изменение данных);

– как можно доказать, что пользователь выполнил определенное действие? (Repudiation – отказ от ответственности);

– является ли обрабатываемая информация конфиденциальной, какими способами она передается в системе и какие негативные последствия могут наступить в случае ее разглашения? (Information disclosure – разглашение сведений);

– какие последствия может вызвать прекращение работы системы и как быстро ее можно восстановить? (Denial of service – отказ в обслуживании);

– присутствует ли в системе функции разграничения прав доступа и как пользователь может повысить уровень доступа к системе? (Elevation of privilege – повышение привилегий).

2.2.2 Составление модели угроз персональных данных

Основное отличие модели угроз информационной безопасности персональных данных от модели угроз STRIDE заключается в том, что модель угроз разработанная на основе вопросов STRIDE, является более общей и не учитывает мелких деталей возможных угроз, в то время как модель угроз персональных данных создается более детализированной и позволяет учитывать даже небольшие проблемы в хранении, обработке и передаче персональных данных клиентов интернет-магазина.

Пример разработанной модели угроз безопасности персональных данных в информационной системе интернет-магазина представлен в третьей главе данной методики.

Основываясь на вопросах безопасности STRIDE и разработанной модели угроз персональных данных, можно приступать к написанию основного кода или в случае с CMS установкой или созданием необходимых плагинов и шаблонов.

2.3 Использование статического анализатора кода SonarQube

2.3.1 Установка необходимых компонентов

Следующим этапом защиты является использование статического анализатора кода для разрабатываемого веб-приложения. Как было указано в первой главе, в рамках настоящей методики будет использоваться статический анализатор кода SonarQube (sonarsource.com/products/sonarqube/).

Для использования анализатора в операционной системе Windows необходимо поэтапно произвести установку следующих компонентов.

1. Установить Java плагин минимум 11 версии.

2. Скачать дистрибутив SonarQube с официального сайта компании и разархивировать его.

3. Скачать дистрибутив Sonar-Scanner (docs.sonarqube.org/latest/analyzing-source-code/scanners/sonarscanner/) с официального сайта компании и разархивировать его.

2.3.2 Настройка подключения к SQL серверу

Для записи результатов анализа SonarQube необходимо развернуть любой SQL сервер (кроме MySQL) и создать в нем базу данных. Далее для подключения к базе данных необходимо.

1. В корневой папке `SonarQube/conf/sonar.properties` в строках `sonar.jdbc.username` и `sonar.jdbc.password` указать имя пользоваться для подключения к базе данных и его пароль, в строке `sonar.jdbc.url` необходимо указать IP-адрес и имя, подключаемой базы данных.

2. В строках `sonar.web.javaOpts`, `sonar.ce.javaOpts`, `sonar.search.javaOpts` необходимо установить максимальное и минимальное значение выделяемой оперативной памяти для возможности запуска основных функций SonarQube.

2.3.3 Настройка SonarQube

Для настройки сервиса SonarQube необходимо выполнить следующее.

1. В корневой папке `SonarQube/conf/wrapper.conf` найти строку `wrapper.java.command` и указать прямой путь к файлу java, например `C:/jdk-11/bin/java`, или оставить значение по умолчанию и открыть свойства компьютера, дополнительные параметры системы, переменные среды, найти переменную среды “PATH” и добавить в нее каталог bin, в котором лежит файл java.

2. Запустить SonarQube. Для этого необходимо в командной строке прописать путь к файлу `StartSonar.bat` и запустить данный сервис. Успешный запуск можно проверить наличием “SonarQube is up” в командной строке или проверить путем подключения к административной панели SonarQube по URL адресу `http://localhost/9000/maintetance`. Пример успешной проверки представлен на рисунке 7.

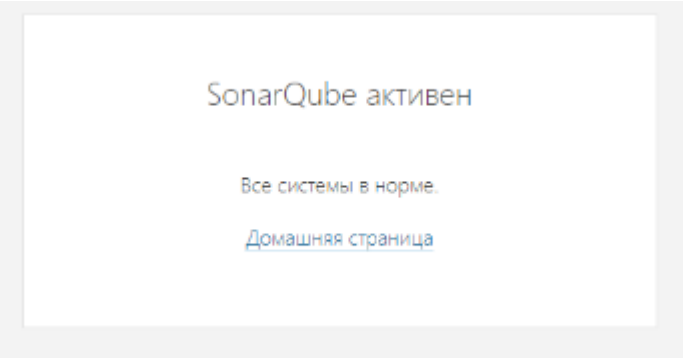

Рисунок 7 – Успешный запуск SonarQube

3. Зайти в админ панель с помощью логина и пароля `admin`.

4. После входа необходимо перейти на вкладку “Projects” и нажать на блок “Create new project”. На открывшейся странице необходимо придумать имя для проекта.

5. Далее в созданном проекте необходимо нажать на блок “Locally” и на открывшиеся странице придумать ключ проекта, выбрать группу языков для проверки и операционную систему, на которой осуществляется проверка. В итоге будет сформирован код для запуска анализатора.

6. Открыть свойства компьютера, дополнительные параметры системы, переменные среды, найти переменную среды “PATH” и добавить в нее каталог

bin из папки sonar-scanner.

2.3.4 Запуск Sonar Scanner

Для старта анализатора необходимо выполнить следующее.

1. Перейти в корневую папку тестируемого проекта и создать любой файл с разрешением `.bat`. В файле необходимо вставить код, который был ранее сгенерирован в административной панели, дополнив его необходимыми параметрами. К наиболее используемым параметрам можно отнести:

– `sonar.login=` (обязательное условие для запуска анализатора, в нем указывается токен, который был сгенерирован в административной панели SonarQube при создании проекта);

– `sonar.host.url=` (адрес сервера SonarQube, например `http://localhost:9000/`);

– `sonar.projectKey=` (ключ проекта);

– `sonar.sources=` (путь к каталогу для проверки только указанных каталогов , например `website/src`);

– `sonar.sourceEncoding=` (кодировка, например UTF-8);

– `sonar.inclusions=` (маска для проверки определенных файлов, например **/*.php).

2. Запустить созданный `.bat` файл через командную строку и дождаться завершения его работы.

Для просмотра результатов сканирования выбранных файлов с подробным описанием ошибок и замечаний, найденных в ходе анализа, необходимо зайти в административную панель SonarQube и перейти в созданный ранее на сайте проект.

2.4 Проведение функционального тестирования ручным и автоматическим способом

2.4.1 Проведение тестирования ручным способом

После разработки и реализации основных функций интернет-магазина необходимо проводить регулярное функциональное тестирование в

соответствии с заданными требованиям при разработке.

Для интернет-магазина необходимо выделить следующие группы требований к тестированию:

1) тестирование регистрации и авторизации. В данную группу входят следующие тесты:
   - регистрация (создание) нового аккаунта;
   - вход в систему;
   - восстановление пароля;
2) тестирование функционала для поиска товаров на сайте:
   - поиск товаров по названию товара;
   - поиск товара по категории;
   - фильтрация товаров по цене, производителю и популярности;
3) тестирование каталогов товаров:
   - отображение информации о наличии товара на складе;
   - просмотр карточки товара;
4) тестирование функциональности корзины:
   - добавление товаров в корзину;
   - изменение количества товаров, добавленных в корзину;
   - удаление товаров из корзины;
   - успешный переход на страницу оформления заказа;
5) тестирование функционала оформления заказа:
   - проверка возможности заказать товар без регистрации;
   - проверка возможности заказать товар на зарегистрированном аккаунте;
   - выбор способа доставки;
   - выбор способа оплаты;
   - проверка правильности заполнения данных;
6) тестирование лояльности клиента:
   - проверка системы скидок;

– начисление бонусов постоянным клиентам;

– проверка правильности начисления бонусов;

7) тестирование отслеживания заказа:

– отправление уведомления о состоянии заказа;

– отслеживание статуса заказа в личном кабинете;

8) тестирование функционала отзывов:

– оставление и редактирование отзывов о товарах;

– проверка правильности отображения отзывов на странице товара;

9) тестирование системы обратной связи:

– проверка функциональности формы обратной связи;

– ответ на сообщение клиента;

– проверка возможности ознакомиться с политикой конфиденциальности, пользовательским соглашением и правилами сайта;

10) тестирование функционала администратора:

– управление заказами;

– управление ценами на сайте и товарной номенклатурой;

– возможность выполнения действий по оперативному решению проблем;

11) тестирование корректности работы веб-приложения на разных устройствах и браузерах.

Представленный список является динамическим и может изменяться в соответствии с требованиями или реализованными функциями сайта. Процесс ручного тестирования заключается в проверке всех или отдельно выбранных тестов путем выполнения определенных шагов и ввода данных в приложение, сравнения результатов работы с ожидаемыми, а также последующей регистрации найденных дефектов.

2.4.2 Использование Selenium WebDriver для автоматического функционального тестирования интернет-магазина

2.4.2.1 Установка необходимых компонентов

Данный метод тестирования отличается от предыдущего тем, что реализует написание всех тестов с помощью языков программирования. Используя Selenium WebDriver, можно добиться полной автоматизации при проведении тестирования и получить более качественные результаты.

В рамках примера будет создан тест на языке программирования Java для авторизации на сайте интернет-магазина в браузере Google Chrome. В качестве программных средств будет использоваться среда разработки от компании Intellij idea (jetbrains.com/ru-ru/idea/) и сборщик Maven. Для успешного функционирования необходимо следующее.

1. Установить Node.js с официального сайта компании.

2. Установить Java плагин минимум 11 версии.

3. Установить бесплатную версию Intellij idea с официального сайта.

4. Открыть среду разработки и создать новый проект (перейти по пути File, далее New, далее Project) и выбрать в качестве сборщика Maven.

5. В открывшемся окне ввести придуманное имя проекта и нажать “Finish”.

6. Установить chromedriver актуальной версии и перенести его в корневую папку проекта.

7. После установки всех пакетов для успешной работы Maven необходимо перейти по пути src, test, java и создать новый класс в данной папке, например TestWeb.

8. Перейти на официальный сайт репозитория Maven (mvnrepository.com) и установить Selenium Java и Selenium Chrome Driver.

9. Для установки необходимо на вкладках репозитория выбрать актуальную версию и скопировать представленный на сайте код для Maven.

10. После копирования необходимо перейти в “pom.xml” и прописать `<dependencies> </dependencies>`, между которым следует установить

скопированный код.

11. Сохранить и перезагрузить созданный проект.

12. Перейти в TestWeb и внутри класса прописать `public static void main (String[] args){}`.

2.4.2.2 Создание теста с помощью Selenium WebDriver

Для создания теста требуется выполнить следующее.

1. В классе `main` необходимо создать новый тест-кейс и вызвать метод `get()`, который загрузит страницу авторизации.

2. Указать правильные данные для авторизации. Для этого необходимо использовать методы "`findElement`" и "`sendKeys`". Эти методы позволяют найти элемент на странице по его идентификатору, имени или XPath-выражению и ввести в него необходимые данные.

3. После ввода данных необходимо нажать на кнопку "`submit`" для отправки формы авторизации. Эту операцию можно выполнить, выбрав элемент на странице и вызвав метод "`submit`".

4. Чтобы убедиться, что авторизация прошла успешно, следует проверить, что после нажатия на кнопку "`submit`" пользователь перенаправляется на страницу его аккаунта. Для этого можно использовать метод "`getCurrentUrl`", который возвращает текущий URL страницы.

5. После успешного выполнения теста необходимо закрыть браузер, чтобы освободить ресурсы. Для этого необходимо использовать метод "`quit`".

6. Для запуска теста необходимо нажать правую кнопку мыши и выбрать “Run “TestWeb.main()””.

Итоговый код для теста выглядит следующим образом:

```
public static void main (String[] args){

WebDriver driver = new ChromeDriver();

driver.get("https://сайт/login");

WebElement username =
```

```
driver.findElement(By.name("username"));

    WebElement password =
driver.findElement(By.name("password"));

    WebElement submitButton =
driver.findElement(By.id("submit"));

    username.sendKeys("admin");

    password.sendKeys("password");

    submitButton.submit();

    String expectedUrl = "https://сайт/account";

    String actualUrl = driver.getCurrentUrl();

    assert.assertEquals(expectedUrl, actualUrl);
    driver.quit();
    }
```

2.5 Использование Burp Suite Intruder для фаззинг-тестирования интернет-магазина

2.5.1 Установка и настройка компонентов Burp Suite

При проведении фаззинг-тестирования интернет-магазина реализуется процесс тестирования, при котором генерируются случайные или систематические входные данные (сообщения или запросы) и отправляются на сервер, чтобы найти уязвимости в коде, которые могут использоваться злоумышленниками для получения несанкционированного доступа.

Для успешного функционирования программы необходимо следующее.

1. Установить Java плагин минимум 11 версии.

2. Установить бесплатную версию Burp Suite с официального сайта.

3. Запустить программу и открыть внутренний браузер от Burp Suite (перейти в графу Proxy, далее Intercept и нажать на Open browser).

4. Переключить кнопку “Intercept is off” в положение “Intercept is on”.

5. В открывшемся браузере следует открыть тестируемый сайт и попытаться перейти в нем на какие-нибудь страницы.

6. В программе Burp Suite в графе Proxy и разделе Intercept будет показываться перехваченный запрос, который можно изменять на свое усмотрение. После изменения запроса следует нажать “Forward” для отправки запроса на сервер.

2.5.2 Запуск фаззинг-тестирования

Для проведения фаззинг-тестирования, например, для проверки на наличие SQL-уязвимости необходимо выполнить следующее.

1. Перехватить запрос на сайте, в котором происходит взаимодействие с полем, которое передает информацию в базу данных на сервере, например с полем ввода логина и пароля.

2. Передать запрос на Intruder. Для этого требуется нажать правую кнопку мыши на передаваемом запросе и выбрать “Send to Intruder”.

3. В Intruder следует выделить вводимую информацию путем ее включения в специальные кавычки. После проведения данных действий выделенная информация будет заменяться в процессе фаззинг-тестирования.

4. Перейти в графу “Payloads” и загрузить полезную нагрузку (специальные символы или команды) в блоке “Playload settings”, далее нажать “Start Attack”.

5. После тестирования необходимо подготовить документацию, содержащую результаты анализа уязвимостей, которые были обнаружены в процессе тестирования.

2.6 Использование OWASP ZAP для проведения тестирования на проникновение

Данное программное средство позволяет просканировать и выявить различного рода уязвимости и ошибки в веб-приложении.

Для его использования необходимо.

1. Установить Java плагин минимум 11 версии.

2. Установить OWASP ZAP (zaproxy.org) с официального сайта.

3. Запустить программу. Интерфейс программы представлен на рисунке 8.

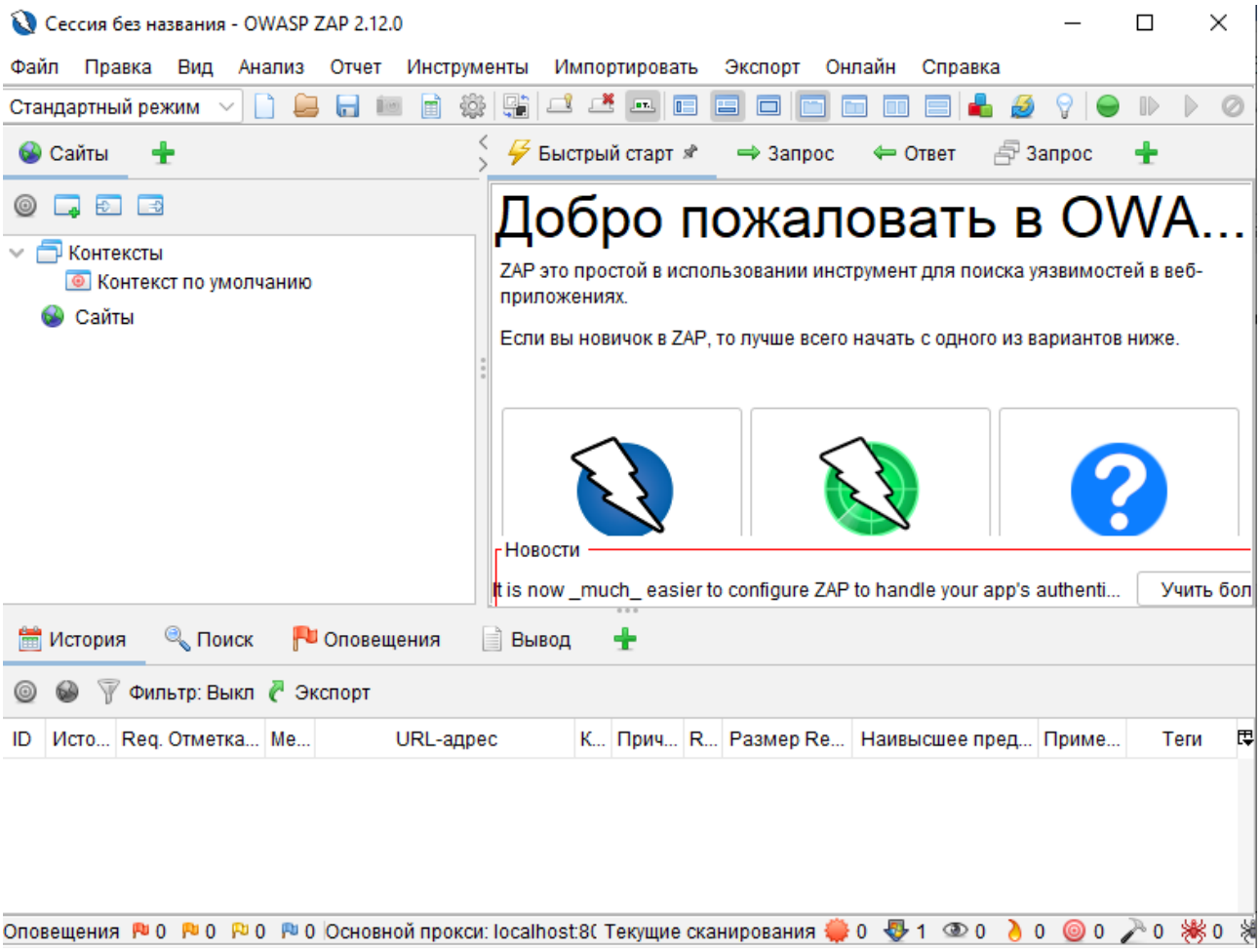

Рисунок 8 – Интерфейс программы OWASP ZAP

4. Выбрать один из режимов сканирования:

– стандартный режим;

– безопасный режим. Данный режим выполняет только те действия, которые не навредят системе;

– защищенный режим. Данный режим позволяет имитировать потенциально опасные уязвимости;

– режим атаки. Самый агрессивный режим, который помимо сканирования выполняет атаки на сайт.

5. Нажать на блок “Автоматическое сканирование”;

6. Ввести URL-адрес сканируемого веб-приложения;

7. Включить функцию “Использовать традиционного паука”. Функция

OWASP ZAP паук позволяет автоматически обнаруживать новые URL-адреса на проверяемом сайте.

8. Нажать “Атака”. После старта сканирования паук начинает искать URL, имеющие отношение к сканирующему сайту. После завершения поиска адресов начинается “Активное сканирование” обнаруженных сайтов в целях выявить потенциальные уязвимости, используя известные атаки.

После завершения тестирования следует ознакомиться с его результатами в разделе “Оповещения”. Содержимое данного раздела представлено на рисунке 9.

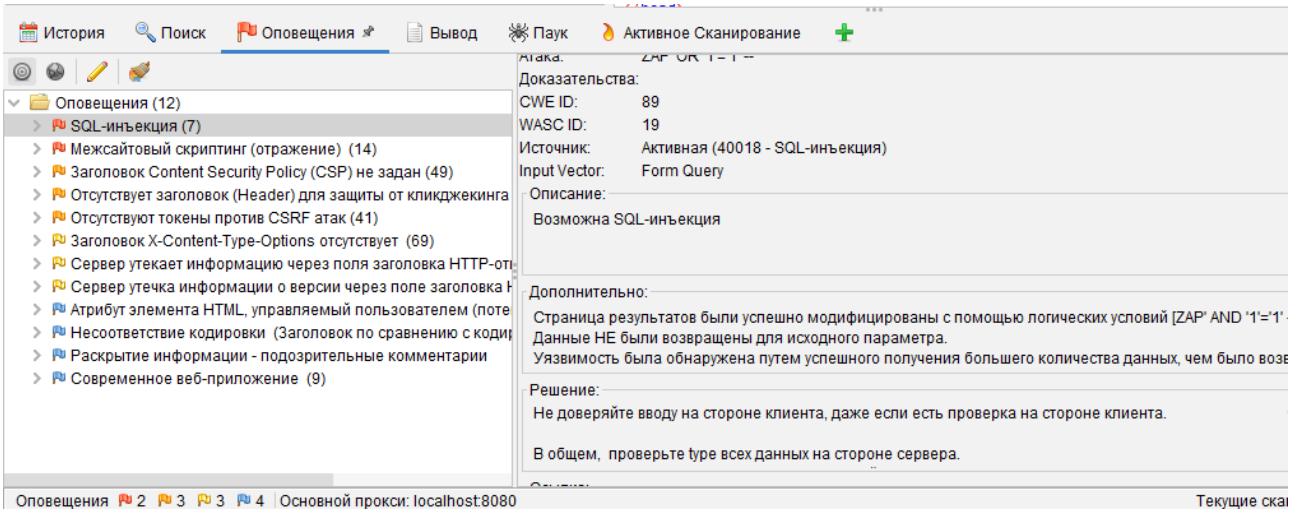

Рисунок 9 – Содержимое раздела “Оповещения”

2.7 Внедрение системы разграничения доступа

Для всех, кто участвует в жизнедеятельности системы интернет-магазина, необходимо создать и назначить права ролевого разграничения доступа к определенным функциям или контенту на сайте. Данные действия необходимы для предоставления гарантий что:

– работник или посетитель интернет-магазина не будет влиять на все элементы управления и компоненты системы, так как ему будет предоставляться только тот доступ, который необходим для выполнения его основных функций;

– при несанкционированном доступе к аккаунту пользователя, злоумышленник будет ограничен в своих возможностях. Мера ограничений будет определена в соответствии с правами доступа пользователя через которого

было выполнено подключение.

Для сайта интернет-магазина необходимо создать следующие роли:

– “Администратор”. Данная роль подразумевает доступ ко всем системам и элементам управления сайта. Администратором может быть как владелец интернет-магазина, так и специально назначенный на эту должность работник;

– “Менеджер по продажам”. Данному работнику выдается доступ к частям системы, в которой осуществляется обработка заказов, отслеживание процесса доставки товаров, а также предоставляется доступ к контактным данным покупателя для подтверждения заказа;

– “Контент-менеджер”. Данный работник отвечает за создание и редактирование текстовых и графических элементов на сайте. Поэтому для данной роли необходимо выдавать соответствующий доступ, позволяющий реализовывать данные функции;

– “Технический администратор”. Работники, входящие в данную группу ролей, будут получать доступ к управлению серверной части интернет-магазина, а также проводить мониторинг безопасности и оптимизацию работы сайта;

– “Оператор техподдержки”. Данная роль выдается сотрудникам, которые решают проблемы клиентов по вопросам использования сайта, а также в случаях обнаружения пользователями технических проблем в работе сайта, фиксируют данные проблемы и передают данную информацию техническим администраторам;

– “Зарегистрированный пользователь”. Данная роль позволяет пользователю осуществлять просмотр страниц интернет-магазина, взаимодействовать со своим личным кабинетом на сайте и осуществляет возможность заказа товаров путем указания своих персональных данных;

– “Незарегистрированный (анонимный) пользователь”. Данная роль позволяет пользователю осуществлять просмотр страниц интернет-магазина. Однако запрещает возможность заказа без прохождения регистрации и указания своих персональных данных.

2.8 Внедрение парольной политики

Для создания и доступа в личный кабинет пользователя необходимо реализовать систему регистрации, авторизации и аутентификации. Однако на этапе регистрации пользователь может установить слишком слабый и уязвимый пароль, который можно достаточно быстро подобрать методом автоматического перебора паролей. Для предотвращения данных угроз необходимо разработать и внедрить правила к создаваемому паролю (парольную политику) при регистрации нового пользователя на сайте интернет-магазина. К данным правилам следует отнести:

– установку минимальной длины пароля. Рекомендованная длина пароля при регистрации на сайте интернет-магазина должна быть не менее 8 символов;

– составление требований к регистру создаваемого пароля. В ходе создания пароля необходимо использовать как заглавные, так и прописные буквы;

– составление требований к содержанию создаваемого пароля. В ходе создания пароля необходимо использовать как минимум один неалфавитный символ, такой как цифры или специальные символы, например <*&(^%$>!);

– запрет на использование пароля, если он полностью повторяет логин, используемый при регистрации;

– запрет на использование паролей из списка запрещенных паролей. Необходимо составить список запрещенных паролей, который включает в себя наиболее популярные и простые пароли, а также пароли, которые были скомпрометированы в результате предыдущих взломов. В случае, если пароль пользователя не выполняет данное правило, система должна сообщить ему об этом и кратко объяснить причину того, почему пароль невозможно использовать;

– установку ограничений для неудачных попыток входа. Чтобы ограничить возможность угадывания пароля, необходимо установить временную блокировку возможности авторизации после превышения заранее

определенного лимита неудачных попыток входа;

– реализацию возможности подключения двухфакторной аутентификации. После успешной регистрации на сайте интернет-магазина стоит проинформировать пользователя, о необходимости дополнительной безопасности, путем подключения двухфакторной аутентификации способами, которые предоставляются сайтом. К наиболее популярному способу двухфакторной аутентификации можно отнести ввод одноразового ключа, который присылается на e-mail адрес или номер телефона пользователя, а также может быть сгенерирован в специальном приложении.

2.9 Внедрение системы хеширования паролей с добавлением оригинальных дополнительный данных для каждого регистрируемого пользователя

После регистрации на сайте интернет-магазина все пароли записываются в базу данных на сервере в открытом и незашифрованном виде. Если злоумышленник сможет получить доступ к сведениям из базы данных, то он получит логины и пароли всех пользователей, зарегистрированных в системе. Для того, чтобы устранить данную угрозу, необходимо принимать на сервер пароли в читаемом виде, далее проводить хеширование и сохранять в базе данных только сами хеши паролей. Существует несколько способов хеширования паролей, однако одним из самых надежных является хешифрование с добавлением от сервера оригинальных данных (“salt”) в пароль зарегистрированного пользователя, с последующим шифрованием методами криптографических протоколов. После регистрации в базу данных будет записывается логин, хеш пароля и “salt” информация, которая добавлялась в момент хеширования. Если злоумышленник сможет получить данные сведения из базы данных, то ему придётся подставлять каждую “salt” информацию к каждому паролю в своем словаре паролей, а также хешировать каждый сформированный пароль, чтобы сравнить его с полученными хешами из базы данных сайта.

В процессе авторизации пользователя проверяется вводимый логин и пароль. Если веденый логин существует в базе данных, то браузеру пользователя отправляется “salt” информация для авторизуемой учетной записи. Далее браузер вычисляет хеш комбинацию веденого пользователем пароля и “salt”, после передает полученный хеш на сервер. Сервер сверяет полученную информацию с той, что лежит в базе данных и в случае сходства осуществляет авторизацию пользователя.

2.10 Установка SSL сертификата

Для обеспечения безопасности от угроз перехвата информации необходимо реализовать способы шифрования при передаче данных между клиентом и сервером с помощью SSL технологий шифрования. Для реализации данного способа можно подключить бесплатный сертификат от “Let’s Encrypt”(letsencrypt.org). На сегодняшний день большинство хостингов позволяют включить его непосредственно в личном кабинете хостинга или в его административной панели. Например, для подключения данного сертификата на хостинге TimeWeb необходимо:

– перейти на сайте хостинга в “Домены” и найти настройки SSL-сертификатов. В открывшемся окне перейти в “Магазин сертификатов” и выбрать “SSL Let’s Encrypt”;

– необходимо выбрать домен, для которого будет создаваться сертификат, при необходимости отключить дополнительные платные услуги представляемые в момент настройки и нажать кнопку “Заказать”.

После установки сертификата на хостинг передача информации между браузером пользователя и сервером считается зашифрованной и будет проходить по HTTPS протоколу.

2.11 Использование сервиса Cloudflare

2.11.1 Подключение сайта к сервису Cloudflare

Главной мерой защиты для уже функционирующего сайта является подключение сервиса Cloudflare (cloudflare.com). Данный сервис позволяет

фильтровать и мониторить поступающий на сервер трафик в реальном времени путем обнаружения и блокирования подозрительных и вредоносных запросов.

Для возможности анализа входящего трафика необходимо осуществить подключение веб-сайта к сервису Cloudflare. Для этого необходимо выполнить следующее.

1. Зарегистрировать аккаунт на официальном сайте сервиса.
2. Добавить свой веб-сайт в дашборде Cloudflare, указав его URL.
3. Выбрать тарифный план подключения и дождаться завершения анализа DNS записей подключаемого сайта.
4. Перейти в личный кабинет сайта, где арендовался домен, и в настойках домена просмотреть какие DNS-записи там присутствуют. Если в административной панели отсутствует возможность проверки, то необходимо перейти в административную панель на сайте хостинга и повторить процесс проверки.
5. После завершения анализа подключённых к сайту DNS-записей, необходимо проверить правильность интегрированных записей. В случае обнаружения ошибки необходимо добавить записи вручную путем нажатия на “Add record”. Если ошибки отсутствуют, необходимо нажать на “Continue”.
6. Произвести замену старых DNS серверов на новые. Для этого необходимо перейти в личный кабинет сайта, где арендовался домен, и в настойках домена найти Name-сервера (Nameserver) или DNS-сервера (DNS server) и добавить те, которые предлагает Cloudflare.
7. На сайте Cloudflare нажать “Done, check nameservers” для завершения процесса подключения.

После подключения должно пройти какое-то количество времени перед тем, как интернет-магазин начнет работать совместно с сервисом Cloudflare. Схема функционирования сайта представлена на рисунке 10.

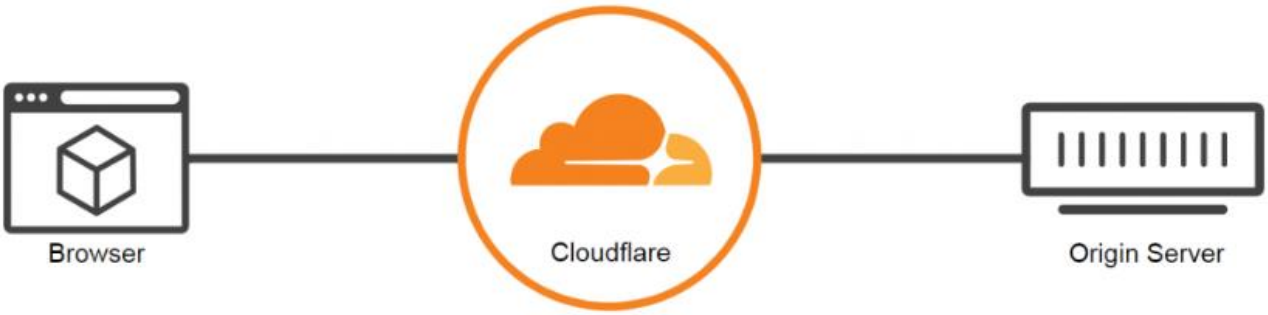

Рисунок 10 – Схема функционирования сайта после подключения

После успешного подключения все данные и запросы, передаваемые на сервер, будут предварительно анализироваться на Cloudflare и в случае подозрительный действий будут блокироваться.

2.11.2 Настройка WAF Cloudflare

Кроме основных настроек безопасности следует подключить и дополнительные инструменты, такие как WAF (Web Application Firewall). Данный инструмент позволяет установить дополнительные правила, при согласовании которых осуществляется вход на сайт. Например, чтобы сделать доступ к админ-панели только с определенных IP-адресов, необходимо выполнить следующее.

1. Зайти в раздел “Firewall” в панели управления Cloudflare, создать новое правило, выбрать “URI” и ввести путь к админ панели (например /wp-admin или /admin.php).

2. Далее следует нажать “And” и выбрать “IP Access Rules”, в поле “Operator” необходимо выбрать “does not equal” и указать разрешенный IP-адрес.

После установки данного правила возможность перехода по указанным ссылкам станет возможна только для установленных IP-адресов.

Кроме ограничений на подключение определенных IP-адресов в WAF Cloudflare присутствуют множество других правил, например возможность ограничивать подключение из других стран или осуществлять проверку на робота (вывод на экран капчи), если сервис посчитает подключение сомнительным.

2.11.3 Установка HTTPS протокола на Cloudflare

На сервисе Cloudflare присутствует возможность включить один из вариантов шифрования данных сразу после подключения сайта к сервису. Например, вариант шифрования “Flexible”, при котором защищенное соединение происходит только между браузером пользователя и Cloudflare, далее информация на веб-сервер идет по открытому протоколу HTTP. Однако, если на хостинге имеется действующий SSL сертификат (например “SSL Let’s Encrypt”), то следует выбрать метод шифрования с его помощью. Для реализации данного способа требуется следующее.

1. На главной панели сервиса Cloudflare перейти в раздел “SSL/TLS”, вкладка “Overviev” и включить режим “Full”.

2. Перейти в “Edge Certificates” и включить параметры “Automatic HTTPS Rewrites” для перезаписи кода с HTTP на HTTPS и “Always Use HTTPS” для перенаправления всех запросов на HTTPS, после этого сохранить настройки.

После проведения данных настроек сервис Cloudflare станет обрабатывать весь входящий трафик через HTTPS протокол. Схема функционирования сайта в защищенном исполнении представлена на рисунке 11.

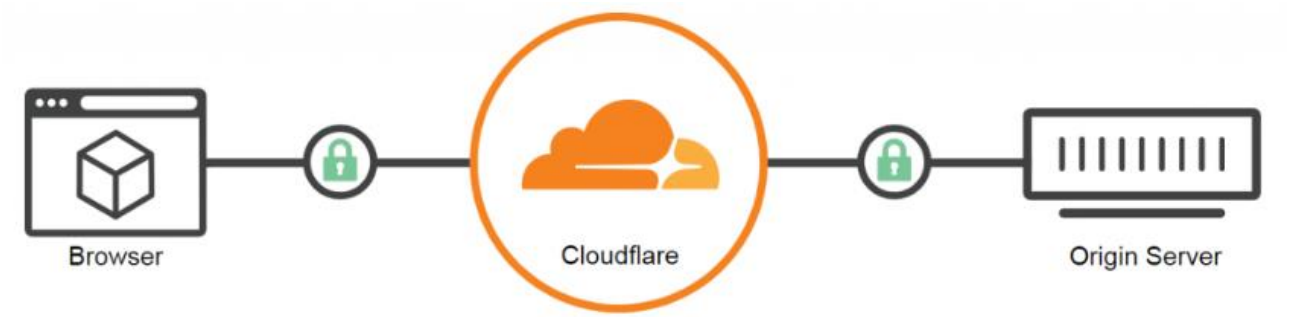

Рисунок 11 – Схема функционирования сайта после установки HTTPS протокола передачи данных

2.12 Проведение регулярного резервного копирования сайта

Резервное копирование сайта на хостинге — это необходимое мероприятие, которое поможет обезопасить сайт и защитить его данные, контент и медиафайлы. К основным плюсам резервного копирования можно отнести:

– защиту от сбоев и потери данных. Резервное копирование сайта

позволяет обезопасить сайт от внезапных сбоев, потери данных, технических проблем или непредвиденных ситуаций, таких как атаки злоумышленников или ошибки пользователей. Если вдруг произойдет сбой системы, то будет проще восстановить сайт благодаря наличию резервной копии;

– защита при внесении изменений и обновлений на сайт. Если в ходе работы сайта появляется необходимость в его обновлении, то перед внесением изменений стоит произвести резервное копирование. Если что-то пойдет не так при обновлении сайта, его можно легко восстановить из резервной копии.

Используя представленные в данной методике способы защиты при разработке и функционировании интернет-магазина можно в значительной степени увеличить безопасность и надежность не только конкретных параметров, но и всей системы в целом. Однако стоит еще раз отметить, что поддержка разработанного сайта является неотъемлемым и непрерывным занятием с постоянными модификациями и улучшениями систем безопасности.

3 Разработка модели угроз информационной безопасности интернет-магазина

3.1 Общие положения

Данная глава включает в себя разработку типовой модели угроз информационной безопасности персональных данных в информационной системе «Интернет-магазин клиенты» на основе документа “Методика оценки угроз безопасности информации”, утвержденного Федеральной службой по техническому и экспортному контролю 5 февраля 2021 года [8]. Общая модель угроз ФСТЭК позволяет более подробно описать причины, условия и последствия возникновения угроз. Цель разрабатываемой модели заключается в выявлении более конкретного набора угроз, которые могут привести к нарушению информационной безопасности персональных данных посетителей интернет-магазина. Разрабатываемая модель является более узконаправленной чем модель, разрабатываемая на стадии жизненного цикла разработки безопасного интернет-магазина, так как она более детально рассматривает моменты связанные с персональными данными. На основе выше указанной методики оценки угроз безопасности информации реализуются следующие требования к содержанию модели:

– определить все последствия, которые могут возникнуть в случае реализации угроз;

– определить все возможные объекты для атак;

– оценить возможности вероятных злоумышленников;

– определить возможные способы реализации угроз;

– определить актуальные угрозы;

Представленная ниже модель угроз может дополняться и изменяться в зависимости от требований к сайту, способов его разработки и используемых при этом программных и технических средств.

Модель угроз безопасности информации в информационной системе персональных данных (далее ИСПДн) «Интернет-магазин клиенты» разработана

в целях реализации требований Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" [9], постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [10].

Модель угроз безопасности информации применяется в ИСПДн «Интернет-магазин клиенты» для решения следующих задач:

– определения требуемого уровня защищенности персональных данных;

– разработки системы защиты персональных данных;

– выбора технических и организационных мер по обеспечению безопасности персональных данных;

– проведения мероприятий по предотвращению несанкционированного доступа к персональным данным.

Для оценки угроз безопасности информации используются следующие документы:

– методический документ «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) [8];

– федеральный закон N 152-ФЗ “О персональных данных” от 27 июля 2006 г [9];

– постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [10].

Ответственным за обеспечение защиты информации, а также систем и сетей в интернет-магазине является администратор информационной безопасности интернет-магазина.

Модель угроз информационной безопасности должна поддерживаться в актуальном состоянии в процессе функционирования систем и сетей.

Изменение модели угроз безопасности информации осуществляется в

случаях:

– изменения требований нормативных правовых актов Российской Федерации, методических документов Федеральной службы по техническому и экспертному контролю России, регламентирующих вопросы оценки угроз безопасности информации;

– изменений архитектуры и условий функционирования систем и сетей, режима обработки информации, правового режима информации, влияющих на угрозы безопасности информации;

– выявления, в том числе по результатам контроля уровня защищенности систем и сетей и содержащейся в них информации (анализа уязвимостей, тестирований на проникновение, аудита), новых угроз безопасности информации или новых сценариев реализации существующих угроз;

– включения в банк данных угроз безопасности информации ФСТЭК России сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации;

– появления сведений и фактов о новых возможностях потенциальных нарушителей.

Модель угроз содержит результаты оценки антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей и техногенных источников угроз. При этом в настоящей Модели угроз не рассматриваются угрозы, связанные с техническими каналами утечки информации (угрозы утечки акустической, видовой информации и информации по каналам ПЭМИН), так как характер и объем обрабатываемой в рассматриваемой системе информации недостаточен для мотивации нарушителей к реализации таких угроз.

3.2 Описание систем и сетей и их характеристика как объектов защиты

Модель угроз безопасности разработана для ИСПДн «Интернет-магазин

клиенты» посетителей интернет-магазина.

На основе требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 [10], для рассматриваемой системы необходимо установить и реализовать 3-ий уровень защищенности.

ИСПДн «Интернет-магазин клиенты» создана и (или) функционирует в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) «О персональных данных» [9]. Данная ИСПДн создана для обеспечения возможности покупки и доставки приобретенных через интернет-магазин товаров и услуг.

В ИСПДн посетителей интернет-магазина обрабатываются следующие персональные данные: фамилия, имя, отчество, номер телефона, адрес электронной почты, данные платежных карт.

Для функционирования системы используются следующие технические средства: АРМ администраторов, АРМ директора, выделенный виртуальный сервер. Внутренними пользователями ИСПДн являются администраторы интернет-магазина. Данным пользователям требуется авторизация в системе интернет-магазина и в случае наличия необходимых прав будет осуществлен доступ к ПДн посетителей. Внешними пользователями ИСПДн являются все посетители интернет-магазина. Данным пользователям также может потребоваться авторизация на сайте интернет-магазина для получения доступа к оформлению покупки.

Представленная ИСПДн использует сеть международного обмена данными “Интернет”. Вся ИСПДн работает на арендованном виртуальном сервере. Для функционирования системы используются следующие программные средства:

– операционная система «Windows 10», установленная на АРМ администраторов и директора интернет-магазина;

– операционная система «AlmaLinux», установленная на виртуальном сервере;

– программа «APACHE HTTP SERVER», установленная на виртуальном сервере;

– программа «Nginx», установленная на виртуальном сервере;

– система управления базами данных (СУБД) «MySQL», установленная на виртуальном сервере;

– Kaspersky Endpoint Security установленный на АРМ администраторов и директора интернет-магазина;

– система управления контентом (CMS) WorldPress;

– программа для работы с документами «МойОфис Профессиональный»;

– браузер «Yandex» для администрирования интернет-магазина.

3.3 Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

К рискам, которые могут наступить в результате нарушения или прекращения основных процессов, относятся: ущерб физическому лицу, риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью.

К негативным последствиям, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба), относятся: нарушение конфиденциальности (утечка) персональных данных, разглашение персональных данных граждан, нарушение неприкосновенности частной жизни, нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах, необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций, нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, потеря конкурентного преимущества, потеря клиентов и утрата доверия.

На основе представленных выше данных была сформирована таблица соответствия негативных последствий к видам возможных рисков. Результаты соответствия представлены в таблице 3.

Таблица 3 – Соответствие негативных последствий к видам риска

Идентификатор	Негативные последствия	Виды риска (ущерба)
НП.1	Разглашение персональных данных граждан	У1. Ущерб физическому лицу
НП.2	Нарушение неприкосновенности частной жизни	
НП.3	Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах	
НП.4	Нарушение конфиденциальности (утечка) персональных данных	
НП.5	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций	У2. Риски юридическому лицу, индивидуальному предпринимателю.
НП.6	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	
НП.7	Потеря клиентов	
НП.8	Утрата доверия	
НП.9	Потеря конкурентного преимущества	

3.4 Возможные объекты воздействия угроз безопасности информации

К объектам воздействия участвующим в обработке и хранении защищаемой информации относятся: Веб-сайт, Информационная система, учетные данные пользователя, АРМ администраторов, АРМ директора, АРМ администратора ИБ, выделенный виртуальный сервер, СУБД «MySQL», прикладное программное обеспечение, линия связи между пользователями или АРМ администраторов и выделенным сервером (сетевой трафик).

В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям. Рассматриваемые виды воздействия представлены в таблице 4.

Таблица 4 – Виды воздействия

Идентификатор	Виды воздействия
ВВ.1	Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
ВВ.2	Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ВВ.3	Отказ в обслуживании компонентов (нарушение доступности)
ВВ.4	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
ВВ.5	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации

Итоговый перечень объектов воздействия со списком возможных видов воздействия на них, реализация которых может привести к негативным последствиям, представлен в таблице 5.

Таблица 5 – Объекты воздействия и виды воздействия

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан (НП.1)	Информационная система	ВВ.1;ВВ.2;ВВ.3;ВВ.4;ВВ.5
	Прикладное программное обеспечение	ВВ.2; ВВ.3; ВВ.4
	АРМ администраторов, АРМ директора	ВВ.1;ВВ.2;ВВ.3; ВВ.5
	Сетевой трафик	ВВ.1;ВВ.2;ВВ.4
	СУБД «MySQL»	ВВ.1;ВВ.2;ВВ.4; ВВ.5
	Учетные данные пользователя	ВВ.1;ВВ.2;ВВ.4
Нарушение неприкосновенности частной жизни (НП.2)	Информационная система	ВВ.1;ВВ.2;ВВ.3;ВВ.4;ВВ.5
	СУБД «MySQL»	ВВ.1;ВВ.2;ВВ.4; ВВ.5
	Учетные данные пользователя	ВВ.1;ВВ.2;ВВ.4
	АРМ администраторов, АРМ директора	ВВ.1;ВВ.2;ВВ.3; ВВ.5
	Сетевой трафик	ВВ.1;ВВ.2;ВВ.4
Нарушение иных прав и свобод гражданина, заключенных в Конституции Российской Федерации и федеральных законах (НП.3)	Информационная система	ВВ.1;ВВ.2;ВВ.3;ВВ.4;ВВ.5
	СУБД «MySQL»	ВВ.1;ВВ.2;ВВ.4; ВВ.5
	АРМ администраторов, АРМ директора	ВВ.1;ВВ.2;ВВ.3; ВВ.5
	Сетевой трафик	ВВ.1;ВВ.2;ВВ.4

Продолжение таблицы 5

Негативные последствия	Объекты воздействия	Виды воздействия
Нарушение конфиденциальности (утечка) персональных данных (НП.4)	Информационная система	ВВ.1;ВВ.2;ВВ.3;ВВ.4;ВВ.5
	Прикладное программное обеспечение	ВВ.1;ВВ.2;ВВ.3;ВВ.4;ВВ.5
	АРМ администраторов, АРМ директора	ВВ.1;ВВ.2;ВВ.3; ВВ.5
	Сетевой трафик	ВВ.1;ВВ.2;ВВ.5
	СУБД «MySQL»	ВВ.1;ВВ.2; ВВ.3
	Учетные данные пользователя	ВВ.1;ВВ.2;ВВ.4;
Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций (НП.5)	Информационная система	ВВ.1;ВВ.2; ВВ.4
	Прикладное программное обеспечение	
	АРМ администраторов, АРМ директора	
	Сетевой трафик	
Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса (НП.6)	АРМ администратора ИБ	ВВ.2;ВВ.3; ВВ.5
	Выделенный виртуальный сервер	
	Информационная система	
	Прикладное программное обеспечение	
	Веб-сайт	
Потеря клиентов (НП.7)	Выделенный виртуальный сервер	ВВ.3;ВВ.4; ВВ.5
	Информационная система	
	Прикладное программное обеспечение	
	Веб-сайт	
Утрата доверия (НП.8)	Выделенный виртуальный сервер	ВВ.3;ВВ.4; ВВ.5
	Информационная система	
	Прикладное программное обеспечение	
	Веб-сайт	
Потеря конкурентного преимущества (НП.9)	Выделенный виртуальный сервер	ВВ.3;ВВ.4; ВВ.5
	Информационная система	
	Прикладное программное обеспечение	
	Веб-сайт	

3.5 Источники угроз безопасности информации

В ходе оценки угроз безопасности информации были определены возможные антропогенные источники угроз безопасности информации, к которым относятся лица, осуществляющие реализацию угроз безопасности информации путем несанкционированного доступа и воздействия на информационные ресурсы и компоненты ИСПДн «Интернет-магазин клиенты», - актуальные нарушители.

Формирование перечня рассматриваемых видов нарушителей и их возможных целей по реализации угроз безопасности информации и предложений об их отнесении к числу возможных нарушителей представлены в таблице 6.

Таблица 6 – Перечень рассматриваемых нарушителей

№ п/п	Вид нарушителя	Возможные цели реализации угроз информационной безопасности	Предположения об отнесении к числу возможных нарушителей
1.	Специальные службы иностранных государств	Нанесения ущерба государству в области обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики; Дискредитация деятельности отдельных органов государственной власти, организаций; Получение конкурентных преимуществ на уровне государства; Срыв заключения международных договоров; Создание внутриполитического кризиса	Цели не предполагают потенциальное наличие нарушителя
2.	Террористические, экстремистские группировки	Совершение террористических актов, угроза жизни граждан; Нанесение ущерба отдельным сферам деятельности или секторам экономики государства; Дестабилизация общества; Дестабилизация деятельности органов государственной власти, организаций	Цели не предполагают потенциальное наличие нарушителя

Продолжение таблицы 6

№ п/п	Вид нарушителя	Возможные цели реализации угроз информационной безопасности	Предположения об отнесении к числу возможных нарушителей
3.	Преступные группы (криминальные структуры)	Получение финансовой или материальной выгоды; Желание самореализации (подтверждение статуса)	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
4.	Отдельные физические лица(хакеры)	Получение финансовой или материальной выгоды; Желание самореализации (подтверждение статуса)	
5.	Конкурирующие организации	Получение финансовой или материальной выгоды; Получение конкурентных преимуществ	
6.	Разработчики программных, программно-аппаратных средств	Получение финансовой или материальной выгоды; Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки; Непреднамеренные, неосторожные или неквалифицированные действия	
7.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или материальной выгоды; Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки; Непреднамеренные, неосторожные или неквалифицированные действия	
8.	Поставщики вычислительных услуг, услуг связи	Получение финансовой или материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия	
9.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия	
10.	Лица, обеспечивающие функционирование систем и сетей	Получение финансовой или материальной выгоды; Непреднамеренные, неосторожные или неквалифицированные действия	

Продолжение таблицы 6

№ п/п	Вид нарушителя	Возможные цели реализации угроз информационной безопасности	Предположения об отнесении к числу возможных нарушителей
11.	Авторизованные пользователи систем и сетей	Получение финансовой или материальной выгоды; Желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
12.	Системные администраторы и администраторы безопасности	Получение финансовой или материальной выгоды; Желание самореализации (подтверждение статуса); Непреднамеренные, неосторожные или неквалифицированные действия; Месть за ранее совершенные действия	
13.	Бывшие (уволенные) работники	Получение финансовой или материальной выгоды; Месть за ранее совершенные действия	

Актуальность нарушителя определялась по следующему принципу: нарушитель признается актуальным, если возможные цели реализации нарушителем угроз безопасности информации могут привести к определенным для ИСПДн «Интернет-магазин клиенты» негативным последствиям и соответствующим рискам. Категории и уровни возможностей нарушителя определяются на основе данных, представленных в методическом документе “Методика оценки угроз безопасности информации" ФСТЭК [8]. Итоговые характеристики возможных нарушителей представлены в таблице 7.

Таблица 7 – Характеристики возможных нарушителей

№ п/п	Вид нарушителя	Возможные цели реализации угроз информационной безопасности	Вид риска		Категория	Уровень нарушителя	Актуальность
			Нанесение ущерба физическому лицу	Нанесение ущерба юридическому люди, индивидуальному предпринимателю			
1.	Преступные группы (криминальные структуры)	Получение финансовой или материальной выгоды	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внешний	Н3. Нарушитель, обладающий средними возможностями	Да
		Желание самореализации (подтверждение статуса)	НП.1; НП.2; НП.3; НП.4	НП.7; НП.8; НП.9			
2.	Отдельные физические лица(хакеры)	Получение финансовой или материальной выгоды	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внешний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
		Желание самореализации (подтверждение статуса)	НП.1; НП.2; НП.3; НП.4	НП.7; НП.8; НП.9			
3.	Конкурирующие организации	Получение финансовой или материальной выгоды	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внешний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
		Получение конкурентных преимуществ	-	НП.7; НП.8; НП.9			
4.	Лица, обеспечивающие поставку и разработку программных, программно-	Получение финансовой или материальной выгоды;	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
		Внедрение дополнительных функциональных	НП.4	НП.6; НП.9			

Продолжение таблицы 7

№ п/п	Вид нарушителя	Возможные цели реализации угроз информационной безопасности	Вид риска		Категория	Уровень нарушителя	Актуальность
			Нанесение ущерба физическому лицу	Нанесение ущерба юридическому люди, индивидуальному предпринимателю			
	аппаратных средств, обеспечивающих систем	возможностей в программные или программно-аппаратные средства на этапе разработки;					
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.2; НП.4	НП.6; НП.9			
5.	Поставщики вычислительных услуг, услуг связи	Получение финансовой или материальной выгоды;	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внешний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.2; НП.4	НП.6; НП.9			
6.	Лица, привлекаемые для установки,	Получение финансовой или материальной выгоды;	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да

Продолжение таблицы 7

№ п/п	Вид нарушителя	Возможные цели реализации угроз информационной безопасности	Вид риска		Категория	Уровень нарушителя	Актуальность
			Нанесение ущерба физическому лицу	Нанесение ущерба юридическому люди, индивидуальному предпринимателю			
	настройки, испытаний, пусконаладочных и иных видов работ	Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.2; НП.4	НП.6; НП.9			
7.	Лица, обеспечивающие функционирование систем и сетей	Получение финансовой или материальной выгоды;	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
		Непреднамеренные, неосторожные или неквалифицированные действия	НП.1; НП.2; НП.4	НП.6; НП.9			
8.	Авторизованные пользователи систем и сетей (клиенты)	Непреднамеренные, неосторожные или неквалифицированные действия;	НП.1; НП.2; НП.4	НП.6; НП.9	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.4	НП.6; НП.9			

Продолжение таблицы 7

№ п/п	Вид нарушителя	Возможные цели реализации угроз информационной безопасности	Вид риска		Категория	Уровень нарушителя	Актуальность
			Нанесение ущерба физическому лицу	Нанесение ущерба юридическому люди, индивидуальному предпринимателю			
9.	Системные администраторы и администраторы безопасности	Получение финансовой или материальной выгоды;	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внутренний	Н2. Нарушитель, обладающий базовыми повышенными возможностями	Да
		Желание самореализации (подтверждение статуса);	НП.1; НП.2; НП.3; НП.4	НП.7; НП.8; НП.9			
		Непреднамеренные, неосторожные или неквалифицированные действия;	НП.1; НП.2; НП.4	НП.6; НП.9			
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.4	НП.6; НП.9			
10.	Бывшие (уволенные) работники	Получение финансовой или материальной выгоды;	НП.1; НП.2; НП.3; НП.4	НП.5; НП.8	Внешний	Н1. Нарушитель, обладающий базовыми возможностями	Да
		Месть за ранее совершенные действия	НП.1; НП.2; НП.3; НП.4	НП.6; НП.9			

3.6 Способы реализации (возникновения) угроз безопасности информации

В ходе оценки угроз безопасности информации были определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальным нарушителям могут быть реализованы угрозы безопасности информации в ИСПДн «Интернет-магазин клиенты», - актуальные способы реализации угроз безопасности информации. Процесс определения актуальных способов реализации включает в себя составление перечня потенциально возможных способов или групп способов реализации угроз безопасности информации и определения возможных интерфейсов объектов воздействия. Перечень потенциально возможных способов реализации угроз представлен в таблице 8.

Таблица 8 – Перечень потенциально возможных способов реализации угроз

Идентификатор	Способ реализации
СР.1	Использование уязвимостей (уязвимостей кода, а также многофакторных и организационных уязвимостей)
СР.2	Использование недостатков конфигурации системы
СР.3	Использование недостатков архитектуры системы
СР.4	Внедрение вредоносного программного обеспечения
СР.5	Прослушивание (захват) сетевого трафика
СР.6	Сканирование сетевой инфраструктуры
СР.7	Использование недостатков безопасности при поставках программных средств и услуг по их установке и настройки
СР.8	Изучение о информации о системе
СР.9	Использование атаки типа “человек по середине”
СР.10	Считывание вводимой и выводимой информации
СР.11	Реализация социальной инженерии
СР.12	Использование атаки типа “отказ в обслуживании”
СР.13	Подбор или восстановление информации для входа в систему(аутентификации)
СР.14	Использование недостатков механизмов разграничения доступа
СР.15	Модификация операционной системы (изменение системных файлов ОС)

Продолжение таблицы 8

Идентификатор	Способ реализации
СР.16	Автоматический сбор человеко-читаемых данных
СР.17	Искажение или повреждение передаваемых и получаемых данных
СР.18	Атака на Веб-приложение

К возможным интерфейсам объектов воздействия были отнесены: веб-интерфейс системы администрирования сайта, пользовательский веб-интерфейс доступа к базе данных информационной системы, веб-интерфейс пользователя веб-сайта, канал передачи данных между АРМ сотрудника и сервером, веб-интерфейс удаленного доступа для управления веб-сервером. Результаты процесса определения актуальных способов реализации (возникновения) угроз безопасности информации представлены в таблице 9.

3.7 Возможные уязвимости

На основе данных, представленных на сайте “Банк данных угроз безопасности информации ФСТЭК России” [11], были сформированы группы наиболее вероятных уязвимостей интернет-магазина, через которые могут быть реализованы угрозы безопасности персональных данных, а также были представлены способы их устранения. Сформированные группы представлены в таблице 10.

3.8 Актуальные угрозы безопасности информации

На данном этапе были определены возможные угрозы безопасности информации для ИСПДн. Угроза безопасности возможна, если есть объект воздействия (информационные ресурсы, компоненты систем и сетей), нарушители или другие источники угроз, которые будут осуществлять воздействие на объект, а также способы реализации угрозы, которые могут привести к негативным последствиям. В качестве исходного перечня угроз безопасности информации использовался “Банк данных угроз безопасности информации ФСТЭК России” [11].

Кроме выявления потенциальных угроз была осуществлена проверка на их

актуальность в информационной системе путем определения наличия сценария для их реализации. При наличии хотя бы одного сценария угроз безопасности информации, такая угроза признается актуальной и включается в список актуальных угроз безопасности информации. Перечень возможных сценариев реализации угрозы представлен в приложениях методического документа «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021) [8]. Результаты оценки возможных угроз безопасности информации представлены в таблице 11.

3.9 Меры защиты от выявленных угроз

Для выявленных угрозы безопасности информации в ИСПДн «Интернет-магазин клиенты» были сформированы меры защиты, препятствующие их возникновению. Меры защиты представлены в таблице 12.

Таблица 9 – Определение актуальных способов реализации угроз безопасности персональных данных и соответствующие им виды нарушителей и их возможности

Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации(идентификаторы)
Преступные группы (криминальные структуры)	Внешний	Веб-сайт	Веб-интерфейс системы администрирования сайта	СР.1; СР.2; СР.3; СР.6; СР.8; СР.12; СР.13; СР.14; СР.18
		Информационная система		СР.1; СР.2; СР.3; СР.4; СР.8; СР.10; СР.12; СР.15; СР.17; СР.18
		АРМ директора, администраторов		СР.1; СР.2; СР.3; СР.4; СР.11; СР.13; СР.14; СР.15; СР.16; СР.18
		Учетные данные пользователя	Веб-интерфейс пользователя веб-сайта	СР.1; СР.2; СР.3; СР.4; СР.11; СР.13; СР.16; СР.18
		Выделенный виртуальный сервер	Веб-интерфейс удаленного доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.4; СР.7; СР.8; СР.12; СР.14; СР.15; СР.17
		Сетевой трафик	Канал передачи данных между АРМ сотрудника и сервером	СР.1; СР.2; СР.3; СР.5; СР.6; СР.9; СР.10; СР.17; СР.18
Отдельные физические лица(хакеры)	Внешний	Веб-сайт	Веб-интерфейс системы администрирования сайта	СР.1; СР.2; СР.3; СР.6; СР.8; СР.12; СР.13; СР.14; СР.18
		Информационная система		СР.1; СР.2; СР.3; СР.4; СР.8; СР.10; СР.12; СР.18
		АРМ директора, администраторов		СР.1; СР.2; СР.3; СР.4; СР.11; СР.13; СР.14; СР.16; СР.18
		Учетные данные пользователя	Веб-интерфейс пользователя веб-сайта	СР.1; СР.2; СР.3; СР.4; СР.11; СР.13; СР.16; СР.18
		Выделенный	Веб-интерфейс удаленного	СР.1; СР.2; СР.3; СР.4; СР.7;

Продолжение таблицы 9

Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации(идентификаторы)
		виртуальный сервер	доступа для управления веб-сервером	СР.8; СР.12; СР.14
		Сетевой трафик	Канал передачи данных между АРМ сотрудника и сервером	СР.1; СР.2; СР.3; СР.5; СР.6; СР.9; СР.10; СР.18
Конкурирующие организации	Внешний	Веб-сайт	Веб-интерфейс системы администрирования сайта	СР.1; СР.2; СР.3; СР.5; СР.6; СР.8; СР.13; СР.14; СР.16; СР.18
		Информационная система		СР.1; СР.2; СР.3; СР.8; СР.12; СР.14; СР.18
Лица, обеспечивающие поставку и разработку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	АРМ директора, администраторов	Веб-интерфейс системы администрирования сайта	СР.1; СР.2; СР.3; СР.4; СР.7; СР.14
		Выделенный виртуальный сервер	Веб-интерфейс удаленного доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.4; СР.7; СР.14; СР.15
		Прикладное программное обеспечение	Веб-интерфейс удаленного доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.4; СР.7; СР.10; СР.12; СР.14;
Поставщики вычислительных услуг, услуг связи	Внутренний	Веб-сайт	Веб-интерфейс системы администрирования сайта	СР.1; СР.2; СР.3; СР.6; СР.8; СР.12; СР.14; СР.18;
		Информационная система		СР.1; СР.2; СР.3; СР.6; СР.8; СР.12; СР.14; СР.18;
		Сетевой трафик	Канал передачи данных между АРМ сотрудника и сервером	СР.1; СР.2; СР.3; СР.5; СР.6; СР.8; СР.10; СР.17;
Лица, привлекаемые для установки, настройки, испытаний,	Внутренний	Информационная система	Веб-интерфейс системы администрирования сайта	СР.1; СР.2; СР.3; СР.6; СР.7; СР.8; СР.10; СР.12; СР.14; СР.15; СР.17;
		АРМ директора, администраторов		

Продолжение таблицы 9

Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации(идентификаторы)
пусконаладочных и иных видов работ		Выделенный виртуальный сервер	Веб-интерфейс удаленного доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.6; СР.8; СР.12; СР.14; СР.15; СР.16; СР.17
		Сетевой трафик	Канал передачи данных между АРМ сотрудника и сервером	СР.1; СР.2; СР.3; СР.5; СР.9; СР.10; СР.16; СР.17
		СУБД «MySQL»	Пользовательский веб-интерфейс доступа к базе данных информационной системы	СР.1; СР.2; СР.3; СР.6; СР.10; СР.12; СР.14; СР.17
		Прикладное программное обеспечение	Веб-интерфейс удаленного доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.4; СР.7; СР.10; СР.12; СР.14;
Лица, обеспечивающие функционирование систем и сетей	Внутренний	Информационная система	Веб-интерфейс системы администрирования сайта	СР.1; СР.2; СР.3; СР.6; СР.7; СР.8; СР.12; СР.14; СР.15; СР.17
		Выделенный виртуальный сервер	Веб-интерфейс удаленного доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.4; СР.6; СР.10; СР.12; СР.14; СР.15; СР.17
		Прикладное программное обеспечение	доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.4; СР.7; СР.10; СР.12; СР.14; СР.17
		СУБД «MySQL»	Пользовательский веб-интерфейс доступа к базе данных информационной системы	СР.1; СР.2; СР.3; СР.6; СР.9; СР.10; СР.12; СР.14; СР.17
Авторизованные пользователи систем и сетей (клиенты)	Внешний	Веб-сайт	Веб-интерфейс системы администрирования сайта; Веб-интерфейс пользователя веб-сайта	СР.1; СР.2; СР.3; СР.8; СР.12; СР.13; СР.18

Продолжение таблицы 9

Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации(идентификаторы)
Системные администраторы и администраторы безопасности	Внутренний	Информационная система	Веб-интерфейс системы администрирования сайта	СР.1; СР.2; СР.3; СР.4; СР.6; СР.8; СР.10; СР.12; СР.14
		Выделенный виртуальный сервер	Веб-интерфейс удаленного доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.4; СР.6; СР.10; СР.12; СР.14; СР.15; СР.17
		Прикладное программное обеспечение	Веб-интерфейс удаленного доступа для управления веб-сервером	СР.1; СР.2; СР.3; СР.4; СР.7; СР.10; СР.12; СР.14; СР.17
		СУБД «MySQL»	Пользовательский веб-интерфейс доступа к базе данных информационной системы	СР.1; СР.2; СР.3; СР.6; СР.9; СР.10; СР.12; СР.14; СР.17
		Сетевой трафик	Канал передачи данных между АРМ сотрудника и сервером	СР.1; СР.2; СР.3; СР.5; СР.9; СР.10; СР.16; СР.17
Бывшие (уволенные) работники	Внешний	Веб-сайт	Веб-интерфейс системы администрирования сайта;	СР.1; СР.2; СР.3; СР.8; СР.12; СР.13; СР.18
		АРМ директора, администраторов	Веб-интерфейс пользователя веб-сайта	СР.1; СР.2; СР.3; СР.4; СР.11; СР.13
		Учетные данные пользователя	Веб-интерфейс пользователя веб-сайта	СР.1; СР.2; СР.3; СР.4; СР.11; СР.13

Таблица 10 – Группы уязвимостей интернет-магазина

Идентификатор	Название группы уязвимостей	Способы устранения
BDU:W01	Уязвимости связанные с недостатками проверки вводимых данных	Использование фреймворков с автоматическими проверками и преобразованием пользовательских данных; Использование проверки входных данных по “белым спискам”; Использование WAF
BDU:W02	Уязвимости связанные с недостатками управления доступом и зашиты данных	Классификация данных, обрабатываемых, хранимых или передаваемых приложением и последующая реализация разграничения доступа согласной классификации; Хранение паролей с использованием надежных функций хеширования; Запрет доступа к ресурсам в стандартной конфигурации для всех ресурсов, за исключением общедоступных; Контроль доступа к моделям данных путем назначения владельцев записей; Отключение вывода списка каталогов веб-сервера, а также обеспечение отсутствия метаданных файлов и файлов резервных копий в корневых веб-каталогах; Регистрация событий запрета доступа; Ограничение частоты доступа к веб-интерфейсу для минимизации возможностей по использованию инструментов автоматизации атак
BDU:W03	Уязвимости связанные с недостатками работы со структурами данных	Запуск кода с минимальными привилегиями; Использование WAF

Продолжение таблицы 10

Идентификатор	Название группы уязвимостей	Способы устранения
BDU:W04	Уязвимости связанные с недостатками проверки подлинности	Реализация многофакторной аутентификации для предотвращения автоматизированных атак; Запрет на использование предустановленных учетных данных; Проверка надежности создаваемых паролей; Ограничения количества попыток входа в систему с увеличением интервала между попытками
BDU:W05	Уязвимости связанные с недостатками управления ресурсами	Использование проверки типов и допустимых значений входных данных; Использование фреймворков с автоматическими проверками и преобразованием пользовательских данных; Использование проверки входных данных по “белым спискам”; Использование WAF

Таблица 11 – Результаты оценки возможных угроз безопасности информации

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации (идентификаторы)	Возможные сценарии реализации угрозы
УБИ.: 006	Угроза внедрения кода или данных	Внешний нарушитель, обладающий базовыми возможностями; Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение	НП.4; НП.6; НП.9	СР.1;СР.2; СР.3;СР.4; СР.7	Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами
УБИ.: 008	Угроза восстановления и/или повторного использования аутентификационной информации		Учетные данные пользователя	НП.2; НП.4	СР.1;СР.2; СР.5;СР.9; СР.13	Т1.12. Сбор личной идентификационной информации, в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
УБИ.: 012	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель, обладающий базовыми возможностями	Прикладное программное обеспечение	НП.4; НП.6; НП.9	СР.1;СР.2; СР.3;СР.4; СР.7;СР.15; СР.17	Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе.
УБИ.: 015	Угроза доступа к защищаемым файлам с использованием обходного пути	Внешний нарушитель, обладающий базовыми возможностями; Внутренний нарушитель, обладающий базовыми повышенными возможностями	Выделенный виртуальный сервер; Веб-сайт	НП.4	СР.1;СР.2; СР.4;СР.6; СР.7;СР.8; СР.14	Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации (идентификаторы)	Возможные сценарии реализации угрозы
УБИ.: 017	Угроза доступа/перехвата/изменения HTTP cookies	Внешний нарушитель, обладающий базовыми возможностями	Веб-сайт	НП.1; НП.4; НП.7; НП.8	СР.1;СР.5; СР.6;СР.17; СР.18	Т6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими
УБИ.: 019	Угроза заражения DNS-кеша		Сетевой трафик; АРМ директора, администраторов	НП.1; НП.2; НП.4	СР.1;СР.4; СР.9;СР.10; СР.17;СР.18	Т1.7 . Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking
УБИ.: 028	Угроза использования альтернативных путей доступа к ресурсам	Внешний нарушитель, обладающий базовыми возможностями; Внутренний нарушитель, обладающий базовыми возможностями	Веб-сайт; Прикладное программное обеспечение	НП.2; НП.4	СР.1;СР.2; СР.3;СР.4; СР.6;СР.7; СР.8;СР.14; СР.15	Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств.

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации(идентификаторы)	Возможные сценарии реализации угрозы
УБИ.:031	Угроза использования механизмов авторизации для повышения привилегий	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Выделенный виртуальный сервер	НП.2; НП.4	СР.11;СР.13; СР.14	Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
УБИ.:041	Угроза межсайтового скриптинга	Внешний нарушитель, обладающий базовыми возможностями	Веб-сайт	НП.1; НП.2; НП.3; НП.4; НП.5	СР.1;СР.4; СР.5;СР.6; СР.10;СР.18	Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)
УБИ.:043	Угроза нарушения доступности облачного сервера	Внешний нарушитель, обладающий базовыми возможностями; Внутренний нарушитель, обладающий базовыми возможностями	Веб-сайт; Выделенный виртуальный сервер	НП.7; НП.8; НП.9	СР.1;СР.4; СР.7; СР.12	Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети
УБИ.:054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Внешний нарушитель, обладающий базовыми возможностями	Выделенный виртуальный сервер; Информационная система	НП.1; НП.2; НП.3; НП.4	СР.1;СР.2 СР.3;СР.9; СР.12;СР.17	Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации (идентификаторы)	Возможные сценарии реализации угрозы
УБИ.: 055	Угроза незащищённого администрирования облачных услуг	Внешний нарушитель, обладающий базовыми возможностями; Внутренний нарушитель, обладающий базовыми возможностями	АРМ директора, администраторов	НП.1; НП.2; НП.3; НП.4; НП.5	СР.1;СР.9 СР.13;СР.14	Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
УБИ.: 074	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями; Внутренний нарушитель, обладающий базовыми возможностями	СУБД «MySQL»; АРМ директора, администраторов	НП.1; НП.2; НП.3; НП.4; НП.5	СР.1;СР.4; СР.5;СР.6; СР.9;СР.11; СР.13;СР.16	Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
УБИ.: 088	Угроза несанкционированного копирования защищаемой информации			НП.1; НП.2; НП.3; НП.4; НП.5	СР.1;СР.2; СР.4;СР.5; СР.9;СР.10; СР.14	
УБИ.: 090	Угроза несанкционированного создания учётной записи пользователя	Внутренний нарушитель, обладающий базовыми возможностями	Выделенный виртуальный сервер	НП.1; НП.2; НП.3; НП.4	СР.1;СР.2; СР.14;СР.15	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации(идентификаторы)	Возможные сценарии реализации угрозы
УБИ.: 099	Угроза обнаружения хостов	Внешний нарушитель, обладающий базовыми возможностями	Сетевой трафик	НП.2; НП.4	СР.1;СР.3; СР.6;СР.10	Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений.
УБИ.: 100	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель, обладающий базовыми возможностями	Веб-сайт	НП.2; НП.4	СР.1;СР.2; СР.3;СР.13	Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
УБИ.: 116	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель, обладающий базовыми возможностями	Сетевой трафик	НП.1; НП.2; НП.3; НП.4; НП.5	СР.1; СР.5; СР.9; СР.10; СР.16	Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях –

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации (идентификаторы)	Возможные сценарии реализации угрозы
						идентификационной информации пользователей
УБИ.: 122	Угроза повышения привилегий	Внутренний нарушитель, обладающий базовыми повышенными возможностями	АРМ директора, администраторов	НП.1; НП.2; НП.3; НП.4; НП.5	СР.1; СР.11; СР.14; СР.15	Т8.1. Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа
УБИ.: 127	Угроза подмены действия пользователя путём обмана	Внешний нарушитель, обладающий базовыми возможностями	АРМ директора, администраторов	НП.1; НП.2; НП.3; НП.4; НП.5	СР.11	Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
УБИ.: 128	Угроза подмены доверенного пользователя	Внешний нарушитель, обладающий базовыми возможностями	АРМ директора, администраторов	НП.2; НП.4;	СР.1;СР.2; СР.3;СР.4; СР.9; СР.13	Т2.9. Несанкционированное подключение внешних устройств.
УБИ.: 135	Угроза потери и утечки данных, обрабатываемых в облаке	Внешний нарушитель, обладающий базовыми возможностями	АРМ директора, администраторов; СУБД «MySQL»	НП.1; НП.2; НП.3; НП.4; НП.5	СР.1;СР.4; СР.5;СР.9; СР.11;СР.13; СР.16; СР.17	Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации (идентификаторы)	Возможные сценарии реализации угрозы
УБИ.: 140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель, обладающий базовыми возможностями; Внутренний нарушитель, обладающий базовыми возможностями	Веб-сайт; Выделенный виртуальный сервер	НП.6; НП.7; НП.8; НП.9	СР.1;СР.4; СР.7;СР.12; СР.14;СР.15	Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети
УБИ.: 145	Угроза пропуска проверки целостности программного обеспечения	Внутренний нарушитель, обладающий базовыми возможностями	Прикладное программное обеспечение	НП.2; НП.4; НП.6	СР.2;СР.3; СР.7	Т3.8. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.
УБИ.: 152	Угроза удаления аутентификационной информации	Внешний нарушитель, обладающий базовыми возможностями; Внутренний нарушитель, обладающий базовыми возможностями	АРМ директора, администраторов	НП.2; НП.3; НП.4	СР.1;СР.11; СР.13;СР.14	Т2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)
УБИ.: 159	Угроза «форсированного веб-браузинга»	Внешний нарушитель, обладающий базовыми возможностями	Веб-сайт	НП.2; НП.4	СР.1;СР.6; СР.14;СР.18	Т2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет)

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации(идентификаторы)	Возможные сценарии реализации угрозы
УБИ.: 165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний нарушитель, обладающий базовыми возможностями	Прикладное программное обеспечение	НП.4; НП.6	СР.3;СР.4; СР.7	Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.
УБИ.: 167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Внешний нарушитель, обладающий базовыми возможностями	АРМ директора, администраторов	НП.4; НП.6	СР.2;СР.4	Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение
УБИ.: 168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Внешний нарушитель, обладающий базовыми возможностями	Учетные данные пользователя	НП.1; НП.2; НП.3; НП.4; НП.5	СР.1;СР.11; СР.13; СР.16	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных
УБИ.: 174	Угроза «фарминга»	Внешний нарушитель, обладающий базовыми возможностями	АРМ директора, администраторов; Сетевой трафик	НП.2; НП.4	СР.1;СР.2; СР.4;СР.18	Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.
УБИ.: 175	Угроза «фишинга»	Внешний нарушитель, обладающий базовыми возможностями	АРМ директора, администраторов; Сетевой трафик	НП.2; НП.4	СР.11	Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
УБИ.: 188	Угроза подмены программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение	НП.4; НП.6; НП.9	СР.2;СР.3; СР.7;СР.14	Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе.

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации(идентификаторы)	Возможные сценарии реализации угрозы
УБИ.: 191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение	НП.4; НП.6; НП.9	СР.1;СР.4; СР.7; СР.15	Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей
УБИ.: 192	Угроза использования уязвимых версий программного обеспечения	Внутренний нарушитель, обладающий базовыми возможностями	Прикладное программное обеспечение	НП.4; НП.6; НП.9	СР.1;СР.4; СР.7	Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке.
УБИ.: 197	Угроза хищения аутентификационной информации из временных файлов cookie	Внешний нарушитель, обладающий базовыми повышенными возможностями	Учетные данные пользователя; АРМ директора, администраторов	НП.1; НП.2; НП.3; НП.4; НП.5	СР.1;СР.5; СР.6;СР.18	Т6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими
УБИ.: 215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Внешний нарушитель, обладающий базовыми повышенными возможностями	Веб-сайт	НП.2; НП.4	СР.1;СР.3; СР.5; СР.8	Т2.12. Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования

Продолжение таблицы 11

Идентификатор	Наименование угрозы	Характеристика нарушителя	Объект воздействия	Негативные последствия	Способы реализации (идентификаторы)	Возможные сценарии реализации угрозы
						сотрудников сторонних организаций, используемого для доступа.
УБИ.: 217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Внутренний нарушитель, обладающий базовыми повышенными возможностями	Прикладное программное обеспечение	НП.4; НП.6; НП.9	СР.1;СР.4; СР.7	Т3.8. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.

Таблица 12 – Меры защиты от актуальных угроз безопасности информации

Идентификатор	Наименование угрозы	Мера защиты
УБИ.:006	Угроза внедрения кода или данных	Использование антивирусных средств для автоматического контроля в реальном времени поведения программ и передаваемых данных в системе; Предоставление внутренним пользователям минимально необходимые привилегии для выполнения их основных функций в системе
УБИ.:008	Угроза восстановления и/или повторного использования аутентификационной информации	Реализация двухфакторной аутентификации для дополнительного уровня защиты
УБИ.:012	Угроза деструктивного изменения конфигурации/среды окружения программ	Настройка ролевого разграничения доступа; Предоставление внутренним пользователям минимально необходимые привилегии для выполнения их основных функций в системе
УБИ.:015	Угроза доступа к защищаемым файлам с использованием обходного пути	Использование антивирусных средств для автоматического контроля в реальном времени поведения программ и передаваемых данных в системе; Настройка компонентов программного обеспечения таким образом, чтобы пользователь не смог получить доступ к объектам доступа, на доступ к которым у него нет прав; Предоставить возможность ввода информации в информационную систему в соответствии с представленными привилегиями
УБИ.:017	Угроза доступа/перехвата/изменения HTTP cookies	Мониторинг и контроль доступа к cookies на предмет выявления несанкционированного удаленного доступа;

Продолжение таблицы 12

Идентификатор	Наименование угрозы	Мера защиты
		Использование защищенных протоколов передачи данных, таких как HTTPS
УБИ.:019	Угроза заражения DNS-кеша	Использование антивирусных средств для автоматического контроля в реальном времени поведения программ и передаваемых данных в системе; Периодически очищать кеш
УБИ.:028	Угроза использования альтернативных путей доступа к ресурсам	Настройка компонентов программного обеспечения таким образом, чтобы пользователь не смог получить доступ к объектам доступа, на доступ к которым у него нет прав; Предоставить возможность ввода информации в информационную систему в соответствии с представленными привилегиями
УБИ.:031	Угроза использования механизмов авторизации для повышения привилегий	Предоставление внутренним пользователям минимально необходимые привилегии для выполнения их основных функций в системе; Оповещать администратора информационной безопасности системы, об изменении сведений о пользователе, его полномочий и привилегий в системе
УБИ.:041	Угроза межсайтового скриптинга	Фильтрация и валидация данных, получаемых от пользователя, для предотвращения внедрения скриптов и других вредоносных кодов
УБИ.:043	Угроза нарушения доступности облачного сервера	Использовать более мощные сервисы для облачных серверов, включающие защиту от типовых способов введения системы в состояние отказа в обслуживании

Продолжение таблицы 12

Идентификатор	Наименование угрозы	Мера защиты
УБИ.:054	Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	Выбор сервиса, в котором реализованы и прописаны все должностные и иные правила и инструкции, которые обязан выполнять работник данного сервиса
УБИ.:055	Угроза незащищённого администрирования облачных услуг	Реализация двухфакторной аутентификации для дополнительного уровня защиты; Предоставление внутренним пользователям минимально необходимые привилегии для выполнения их основных функций в системе
УБИ.:074	Угроза несанкционированного доступа к аутентификационной информации	Использование антивирусных средств для мониторинга состояний АРМ администраторов; Составление и утверждение правил, в которых прописывается условия хранения, передачи и использования паролей для входа в систему; Использование защищенных протоколов передачи данных, таких как HTTPS; Осуществление мониторинга и анализа подключений к системе или базе данных
УБИ.:088	Угроза несанкционированного копирования защищаемой информации	Предоставление внутренним пользователям минимально необходимые привилегии для выполнения их основных функций в системе; Оповещать администратора информационной безопасности системы, об попытке копирования защищаемой информации
УБИ.:090	Угроза несанкционированного создания учётной записи пользователя	Предоставление возможности создавать новые учетные записи только администратору информационной безопасности;

Продолжение таблицы 12

Идентификатор	Наименование угрозы	Мера защиты
		Оповещать администратора информационной безопасности системы, об изменении в списке пользователей, зарегистрированных в системе
УБИ.:099	Угроза обнаружения хостов	Использование WAF; Скрытие серверной информации, такой как версия веб-сервера
УБИ.:100	Угроза обхода некорректно настроенных механизмов аутентификации	Составление и реализация парольной политики для входа в систему; Реализовать систему контроля и мониторинга входных данных; Реализация двухфакторной аутентификации для дополнительного уровня защиты
УБИ.:116	Угроза перехвата данных, передаваемых по вычислительной сети	Использование защищенных протоколов передачи данных, таких как HTTPS
УБИ.:122	Угроза повышения привилегий	Предоставление внутренним пользователям минимально необходимые привилегии для выполнения их основных функций в системе; Разрешить настройку ролевого разграничения доступа только администратору безопасности; Мониторинг состояния ролевого разграничения доступа и оповещение администратора безопасности в случае его изменения
УБИ.:127	Угроза подмены действия пользователя путём обмана	Составление правил работы администраторов с указанием перечня сведений, которые нельзя разглашать
УБИ.:128	Угроза подмены доверенного пользователя	Реализация двухфакторной аутентификации для дополнительного уровня защиты; Реализация и мониторинг аудита входа администраторов

Продолжение таблицы 12

Идентификатор	Наименование угрозы	Мера защиты
		в систему для выявления нестандартных и подозрительных авторизаций
УБИ.:135	Угроза потери и утечки данных, обрабатываемых в облаке	Использовать надежные сервисы для облачных серверов с достаточной степенью надежности защиты информации; Формирование правил к парольной политике; Реализация двухфакторной аутентификации для дополнительного уровня защиты
УБИ.:140	Угроза приведения системы в состояние «отказ в обслуживании»	Использовать более мощные сервисы для облачных серверов, включающие защиту от типовых способов введения системы в состояние отказа в обслуживании; Использование WAF
УБИ.:145	Угроза пропуска проверки целостности программного обеспечения	Использование антивирусных средств для мониторинга состояний системы и проверки устанавливаемых компонентов и программ; Производить установку компонентов только под контролем администратора безопасности; Оповещать администратора безопасности при попытке установки без его согласия; Производить установку только с официальных источников
УБИ.:152	Угроза удаления аутентификационной информации	Разрешить функцию сброса или удаления аутентификационной информации только администратору безопасности
УБИ.:159	Угроза «форсированного веб-браузинга»	Осуществление проверки корректности вводимых данных в адресной строке браузера; Если есть необходимость закрыть для просмотра

Продолжение таблицы 12

Идентификатор	Наименование угрозы	Мера защиты
		определённую папку, то необходимо в нее включить файл .htaccess и прописать в нем необходимые команды
УБИ.:165	Угроза включения в проект не достоверно испытанных компонентов	Использование антивирусных средств для мониторинга состояний системы и проверки устанавливаемых компонентов и программ; Производить установку компонентов только под контролем администратора безопасности; Оповещать администратора безопасности при попытке установки без его согласия; Включать в проект только стабильные и испытанные компоненты
УБИ.:167	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Использование антивирусных средств для мониторинга состояний АРМ администраторов
УБИ.:168	Угроза «кражи» учётной записи доступа к сетевым сервисам	Если в системе предусмотрена регистрация администраторов, то необходимо проверять существование указываемого e-mail адреса при регистрации; Формирование правил к парольной политике; Реализация двухфакторной аутентификации для дополнительного уровня защиты
УБИ.:174	Угроза «фарминга»	Использование защищенных протоколов передачи данных, таких как HTTPS; Составление требований к бдительности администраторов
УБИ.:175	Угроза «фишинга»	Использование защищенных протоколов передачи данных, таких как HTTPS; Составление требований к бдительности администраторов

Продолжение таблицы 12

Идентификатор	Наименование угрозы	Мера защиты
УБИ.:188	Угроза подмены программного обеспечения	Использование антивирусных средств для мониторинга состояний системы и проверки устанавливаемых компонентов и программ; Производить установку только под контролем администратора безопасности; Оповещать администратора безопасности при попытке установки без его согласия; Производить установку только с официальных и проверенных источников
УБИ.:191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Использование антивирусных средств для мониторинга состояний системы и проверки устанавливаемых компонентов и программ; Установка программ и компонентов только из разрешенных и официальных источников
УБИ.:192	Угроза использования уязвимых версий программного обеспечения	Мониторинг наличия обновлений и использование только актуальных версий программного обеспечения; При ручном обновлении производить установку только с официальных источников
УБИ.:197	Угроза хищения аутентификационной информации из временных файлов cookie	Мониторинг и контроль доступа к cookies файлам на предмет выявления несанкционированного удаленного доступа; Использование антивирусных средств для мониторинга состояний АРМ администраторов; Периодическое очищение cookies файлов; Использование защищенных протоколов передачи данных, таких как HTTPS

Продолжение таблицы 12

Идентификатор	Наименование угрозы	Мера защиты
УБИ.:215	Угроза несанкционированного доступа к системе при помощи сторонних сервисов	Запрет на использование сторонних сервисов авторизации для администраторов системы; Реализация двухфакторной аутентификации для дополнительного уровня защиты
УБИ.:217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	При автоматическом и регулярном обновлении осуществлять мониторинг списка, разрешенный источников и оповещать администратора безопасности при изменении данного списка; При ручном обновлении производить установку только с официальных источников

4 Вредные психофизиологические факторы, влияющие на сердечно-сосудистую систему специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Специалисты по защите информации, как и многие работники, часто подвергаются воздействию вредных психофизиологических факторов, которые могут негативно повлиять на их сердечно-сосудистую систему. К наиболее распространяемым факторам можно отнести:

– сидячий образ жизни. Работа в IT-отрасли часто связана с многочасовым пребыванием за компьютером и отсутствием достаточной физической активности. Это может приводить к неправильной работе сердечно-сосудистой системы и различным заболеваниям;

– стресс. Работа специалиста по защите информации связана с большими нагрузками и ответственностью, что может вызывать стресс и утомление. Длительный стресс может приводить к освобождению гормонов, которые усиливают сокращение сердца и приводят к повышенному кровяному давлению;

– низкое качество воздуха. Работа в замкнутом помещении и наличие компьютеров и другой электроники могут добавлять в воздух различные вредные вещества, что может негативно повлиять на сердечно-сосудистую систему;

– неправильное питание. Неправильное, несбалансированное питание, содержащее жирную и соленую пищу, может приводить к образованию холестерина и различным сердечно-сосудистым заболеваниям.

В целом, специалисты по защите информации, как и другие работники, должны следить за своим здоровьем и стараться минимизировать воздействие этих вредных факторов на их сердечно-сосудистую систему. Например, для снижения факторов риска заболеваний сердечно-сосудистой системы необходимо проводить регулярные занятия физической культурой, которые могут включать в себя:

– аэробные тренировки, такие как бег, ходьба, велосипедная езда или плавание. Такие упражнения улучшают сердечно-сосудистую систему и снижают уровень холестерина;

– силовые тренировки, такие как подтягивания, отжимания, приседания. Эти упражнения помогают укреплять мышцы и кости, а также снижают уровень жировой ткани;

– растяжка и упражнения на гибкость, такие как йога или пилатес. Они помогают сохранять гибкость суставов и мышц, что снижает риск травм;

Кроме представленных способов, необходимо следить за правильным питанием и отказаться от вредных привычек, таких как курение и употребление алкоголя. Такой подход поможет снизить риск заболеваний сердца и сосудов.

Заключение

В результате выполнения выпускной квалификационной работы была разработана методика разработки комплекса средств для обеспечения информационной безопасности интернет-магазина.

В процессе работы был составлен и описан жизненный цикл разработки безопасного интернет-магазина. Были описаны базовые требования на каждом из этапов жизненного цикла.

На втором этапе были описаны организационные и программные методы и средства защиты при разработке безопасного интернет-магазина. Составлен примерный перечень действий для каждого из представленных методов защиты.

На третьем этапе была составлена модели угроз информационной безопасности интернет-магазина включающая в себя:

- все последствия, которые могут возникнуть в случае реализации угроз;
- возможные объекты для атак;
- вероятных злоумышленников и их возможности;
- возможные способы реализации угроз;
- возможные угрозы и способы их предотвращения.

Разработаны организационные и технические мероприятия для снижения воздействия психофизиологических факторов, влияющих на сердечно-сосудистую систему специалиста по защите информации.

Результатом выпускной квалификационной работы является разработанный комплекс средств для обеспечения информационной безопасности интернет-магазина, включающий в себя модель жизненного цикла разработки интернет-магазина, используемые программные и организационные методы и средства, составленную модель угроз информационной безопасности персональных данных посетителей интернет-магазина.

Таким образом, задание на выпускную квалификационную работу выполнено в полном объеме.

Список используемых источников

1 Исследование компании Positive Technologies. [Электронный ресурс] – URL: https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020-2021/ (дата обращения: 09.03.2023).

2 Жизненный цикл разработки защищенных приложений Microsoft. [Электронный ресурс] – URL: https://learn.microsoft.com/ru-ru/compliance/assurance/assurance-microsoft-security-development-lifecycle (дата обращения: 12.03.2023).

3 ГОСТ Р 56939–2016. [Электронный ресурс] – URL: https://docs.cntd.ru/document/1200135525 (дата обращения: 15.03.2023).

4 OWASP TOP TEN. [Электронный ресурс] – URL: https://owasp.org/www-project-top-ten/ (дата обращения: 25.03.2023).

5 ГОСТ Р 58412–2019. [Электронный ресурс] – URL: https://docs.cntd.ru/document/1200164529 (дата обращения: 31.03.2023).

6 Модель угроз STRIDE. [Электронный ресурс] – URL: https://learn.microsoft.com/ru-ru/azure/security/develop/threat-modeling-tool-threats#stride-model (дата обращения: 06.04.2023).

7 Статистика использования систем управления контентом. [Электронный ресурс] – URL: https://w3techs.com/technologies/overview/content_management (дата обращения: 10.04.2023).

8 Методика оценки угроз безопасности информации. [Электронный ресурс] – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 20.04.2023).

9 Федеральный закон N 152-ФЗ “О персональных данных” от 27 июля 2006. [Электронный ресурс] – URL: https://learn.microsoft.com/ru-ru/azure/security/develop/threat-modeling-tool-threats#stride-model (дата обращения: 23.04.2023).

10 Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных. [Электронный ресурс] – URL: https://pd.rkn.gov.ru/docs/Postanovlenie_Pravitel6stva_RF_1119.pdf (дата обращения: 23.04.2023).

11 Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс] – URL: https://bdu.fstec.ru:8443/threat (дата обращения: 28.04.2023).