

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут інформатики та радіoeлектроніки
Факультет радіoeлектроніки та телекомунікацій
(повне найменування інституту, назва факультету)

Кафедра захисту інформації
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти (освітній ступінь))

на тему «Вдосконалення захисту каналів передачі інформації з
використанням протоколу WebSocket»

Виконав: студент 6 курсу, групи РТ-813м
спеціальності (напряму підготовки)

125 Кібербезпека

(код і назва напрямку підготовки, спеціальності)

Логвиненко Ярослав Максимович

(прізвище та ініціали)

Керівник Воскобойник В.О., к.т.н., доцент
кафедри захисту інформації

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

м. Запоріжжя
2018 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет
 (повне найменування вищого навчального закладу)

Інститут, факультет _____ ІРЕ, ФРЕТ _____
 Кафедра _____ захисту інформації _____
 Ступінь вищої освіти (освітній ступінь) _____ магістр _____
 Спеціальність _____ 125 Кібербезпека _____
 (код і назва)
 Напрямок підготовки _____ Безпека інформаційних і комунікаційних систем _____
 (код і назва)

ЗАТВЕРДЖУЮ
 Завідувач кафедри захисту інформації,
 проф., д.т.н., Карпуков Л.М.
 “ _____ ” _____ 2018 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Логвиненку Ярославу Максимовичу
 (прізвище, ім'я, по батькові)

1. Тема проекту (роботи) «Вдосконалення захисту каналів передачі інформації з використанням протоколу WebSocket»

керівник проекту (роботи) Воскобойник В.О., к.т.н., доцент кафедри захисту інформації

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “ 7 ” листопада 2018 року № 328

2. Строк подання студентом проекту (роботи) _____ 3 грудня 2018 року _____

3. Вихідні дані до проекту (роботи) Література в галузі захисту інформації, пакети прикладних програм для розробки веб-додатків, протокол WebSocket як механізм захисту каналів передачі інформації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Дослідження проблем безпеки інформації веб-додатків; забезпечення захисту каналів передачі інформації з використанням протоколу WebSocket; вдосконалення захисту каналів передачі інформації.

5. Перелік графічного матеріалу (зточним зазначенням обов'язкових креслень)
Схема реалізації SQL атаки; архітектура DDoS атаки; модель взаємодії клієнта та сервера за допомогою протоколів HTTPS та WebSocket.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основний	Воскобойник В.О., доцент кафедри захисту інформації		
Охорона праці	Коробко О.В., старший викладач кафедри ОПНС		
Економічна частина	Лівощко Т.В., доцент кафедри обліку і оподаткування		
Нормо-контроль	Нікуліщев Г.І., старший викладач кафедри захисту інформації		

7. Дата видачі завдання _____ 3 жовтня 2018 _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Ознайомлення з темою дослідження та постановка задачі	03.10 – 04.10	
2	Ознайомлення з літературою та вибір джерел інформації	05.10 – 07.10	
3	Дослідження структури та вразливостей системи передачі інформації	8.10 – 14.10	
4	Аналіз дійсних методів передачі інформації	15.10 – 21.10	
5	Вибір альтернативного методу передачі інформації	22.10 – 28.10	
6	Розробка ефективних методів захисту	29.10 – 04.11	
7	Розробка рекомендації щодо підвищення рівня захисту каналів передачі інформації	05.11 – 11.11	
8	Впровадження запропонованих методів у службу миттєвих повідомлень	12.11 – 18.11	
9	Охорона праці та безпека у надзвичайних ситуаціях	19.11 – 21.11	
10	Діагностика економічного ризику використання нової системи захисту	22.11 – 25.11	
11	Оформлення пояснювальної записки	26.11 – 30.11	

Студент

(підпис)

(прізвище та ініціали)

Керівник проекту (роботи)

(підпис)

(прізвище та ініціали)

РЕФЕРАТ

ПЗ: 88 страниц, 20 рисунков, 9 таблиц, 18 формул.

Область исследования - уровень защищённости каналов передачи информации.

Объект исследования - уязвимости и методы защиты каналов передачи информации, протокол WebSocket.

Целью работы является совершенствование защиты каналов передачи информации с использованием протокола WebSocket.

Результат и их новизна. Развитие и усовершенствование информационных технологий и систем связи является недостижимой целью без создания новых программных и аппаратных средств и веб-приложений, предназначенных для персонального или корпоративного использования. Наряду с этим фактом также возникает проблема защиты прав создателей и владельцев продуктов информационных технологий. Недостаточное или полное отсутствие защиты часто является главной причиной оттока из сферы производства программного обеспечения способных к разработке специалистов, а также снижению качества новых информационных ресурсов и качеству обслуживания действующих программных средств и веб-приложений.

Значимость работы и выводы. Проведена работа по исследованию уязвимостей и атак, направленных на каналы передачи информации. Предложены методы и рекомендации по повышению уровня безопасности в исследуемой области, направленные на совершенствование защиты действующих каналов передачи. А также разработана и внедрена реализация системы защиты на примере службы мгновенных сообщений.

КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ, БЕЗОПАСНОСТЬ, АТАКА, УГРОЗА, УЯЗВИМОСТЬ, BRUTE FORCE, WEBSOCKET, XSS.

СПИСОК СОКРАЩЕНИЙ

DoS - Denial of Service

DDos - Distributed Denial of Service

HTTP - Hyper Text Transport Protocol

WEB - World Wide Web

ИТ - информационные технологии

НСД - несанкционированный доступ

ПК - персональный компьютер

ПО - программное обеспечение

СОДЕРЖАНИЕ

Введение	8
1 Исследование проблем безопасности веб-приложений и каналов передачи информации	10
1.1 Политика информационной безопасности веб-приложения	10
1.2 Угрозы информационной безопасности веб-приложения	13
1.3 Классификация уязвимостей и атак на веб-приложения	17
1.4 Направления защиты веб-приложения	24
2 Обеспечение защиты каналов передачи информации с помощью протокола «WebSocket»	33
2.1 Протокол WebSocket, как механизм защиты каналов передачи информации	33
2.2 Недостатки протокола WebSocket и пути их устранения	38
3 Совершенствование защиты каналов передачи информации	42
3.1 Механизм защиты от успешной реализации XSS уязвимости	42
3.2 Защита паролей с использованием методов шифрования	46
3.3 Защита JavaScript кода с помощью обфускации	48
4 Экономическая часть	53
4.1 Актуальность темы с позиции маркетинга	53
4.2 Расчет сметы затрат на практическую реализацию проекта	55
4.3 Расчет заработной платы	56
4.4 Расчет отчислений на единый социальный взнос	56
4.5 Расчет расходов на оборудование	57
4.6 Расчет расходов на услуги сторонних организаций	58
4.7 Расчет расходов на общехозяйственные затраты	59
4.8 Расчет на амортизацию объектов основных средств и нематериальных активов	59
4.9 Бальная оценка экономической эффективности проекта	61
5 Охрана труда и безопасность в чрезвычайных ситуациях	65

5.1 Анализ потенциальных опасностей	65
5.2 Мероприятия по обеспечению безопасности.....	67
5.3 Мероприятия производственной санитарии и гигиены труда	72
5.4 Мероприятия по пожарной безопасности.....	79
5.5 Меры безопасности в чрезвычайных ситуациях.....	81
Выводы	84
Список использованной литературы.....	87

ВВЕДЕНИЕ

Актуальность темы исследования. Защита информации и проблема обеспечения целостности и конфиденциальности приобретает актуальность для очень многих людей, в том числе, чья деятельность находится вне области, где эти вопросы решают государственные органы.

В наши дни основным информационным ресурсом является глобальная сеть интернет, соответственно возрастает число веб-приложений в международной виртуальной сети и количество каналов передачи информации, а также их разнообразие.

Защита каналов передачи информации должна предоставлять сохранность пересылаемых данных от широкого круга различных угроз, таких, как утечка информации, несанкционированные воздействия, копирование и незаконное использование.

Программные продукты являются результатом труда специалистов высокой квалификации. Процесс проектирования и создания новых программных продуктов сопровождается значительными финансовыми и трудовыми затратами, основан на использовании наукоемких технологий и инструментов, требует применения соответствующего уровня дорогостоящей техники. Это влечет за собой необходимость принятия мер по защите интересов разработчика, его программного продукта, не только внутри фирмы, но и за ее пределами от несанкционированного копирования и использования.

В целях защиты каналов передачи информации разработаны и предложены методы защиты, среди которых представлен собственный фильтр для проверки вводимых данных пользователями, механизм проверки активности пользователя и его пользования веб-приложением, а также способы защиты пароля и программного кода.

Целью работы является совершенствование защиты каналов передачи информации с использованием протокола WebSocket.

Объектом исследования являются уязвимости и методы обеспечения безопасности каналов передачи информации, протокол WebSocket.

Предметом исследования является уровень защищённости каналов передачи информации.

Задачи:

- ознакомление с темой исследования и постановка задачи;
- выбор литературы;
- изучение структуры и уязвимостей системы передачи информации;
- анализ существующих методов передачи и выбор альтернативного способа;
- разработка наиболее эффективных средств защиты данных при их приёме и передаче.

В качестве результата работы будет представлен наиболее эффективный альтернативный вариант передачи информации, а также предложены методы и рекомендации по повышению уровня безопасности в исследуемой области, направленные на совершенствование защиты действующих каналов передачи информации, что позволит в дальнейшем совершенствовать и расширять методику передачи данных.

Также разработана и внедрена реализация системы защиты на примере службы мгновенных сообщений.

1 ИССЛЕДОВАНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ И КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

1.1 Политика информационной безопасности веб-приложения

Веб-приложения с каждым днем вызывают все больше интереса со стороны хакеров в качестве ресурсов и способа заработка. Полученная в результате взлома информация, может послужить инструментом доступа к атакуемому ресурсу с дальнейшим использованием в личных целях.

Большая заинтересованность злоумышленника и высокая стоимость информации заставляют атакующего находить уязвимости в приложении и способы их реализации.

Заблуждения владельцев о высокой степени защищенности своих веб-ресурсов и отсутствии уязвимостей часто уменьшают долю внимания, приходящуюся на планирование и проведение работ по информационной безопасности.

Согласно отчету о хакерских атаках на веб-приложения и сайты за 2017 год, компания Google сообщила, что количество взломанных ресурсов увеличилось на 30% по сравнению с 2016 годом.

Информационная безопасность веб-ресурса - это мероприятия проводимые с целью обеспечения конфиденциальности, целостности и доступности информации, которая попадает, обрабатывается, хранится и создается в пределах приложения.

При организации информационной безопасности необходимо учитывать другие свойства, такие как, подлинность, целесообразность, своевременность, отчетность, безотказность и достоверность информации.

Информационная безопасность веб-ресурса реализуется при помощи использования различных уровней ответственности в структуре приложения, приведенных на графике уровней ответственности (рис. 1.1).

Нулевая ответственность распределяется на конечных потребителей веб-приложения, которыми часто являются неавторизованные пользователи,

имеющие только право на просмотр публичной информации и пользовательского информационного наполнения сайта на коллаборативной основе и не отвечают за информационную безопасность.

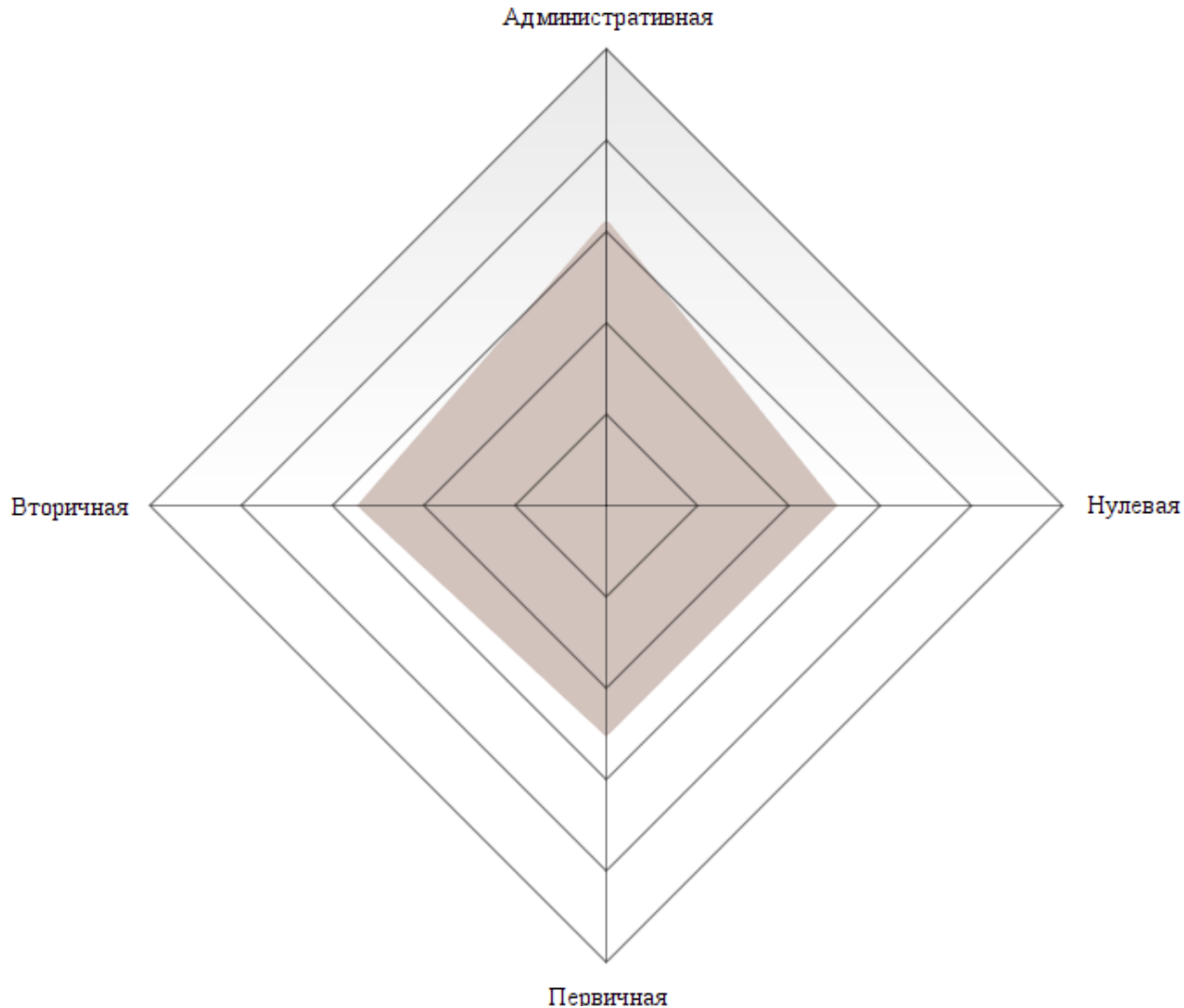


Рисунок 1.1 - График важности соблюдения всех уровней ответственности в структуре приложения

Первичная ответственность распределяется среди авторизованных пользователей веб-ресурса, которые не только просматривают, но и участвуют в создании официального информационного наполнения, т.е. размещают информацию из официальных источников в пределах веб-сайта или отдельных

его разделов, что в свою очередь касается достоверности и актуальности информации, а также качественного ее представления.

Вторичная ответственность распределяется среди авторизованных пользователей веб-ресурса, которые осуществляют анализ, консолидацию и продвижение информационного наполнения и касаются уместности и своевременности информации.

Административная ответственность распределяется среди круга лиц, обеспечивающих техническую поддержку веб-ресурса и управляющего коллектива, которые обеспечивают работоспособность системы и целостность хранения данных.

Согласно предоставленному графику на рисунке 1.1, можно сделать вывод, что важно поддерживать все 4 уровня ответственности, так как нет приоритетного уровня.

Административно ответственные лица должны проводить такие мероприятия по безопасности относительно надёжного функционирования веб-ресурса и эффективного использования программно-аппаратного обеспечения:

- систематическое резервное копирование баз данных и файлов;
- ведение централизованного банка программного обеспечения и лицензий, что используются при эксплуатации сайта;
- сбор документации, необходимой для использования ресурса в целом и отдельных его компонентов;
- учёт проблем при эксплуатации ресурса, отдельных его компонентов и мероприятий по администрированию;
- проверки и усиления надежности механизмов защиты паролей, изменения существующих незащищенных протоколов аутентификации на защищённые.

Важной частью создания политики информационной безопасности является учет источников информации, как внутренних, так и внешних,

которые будут использоваться для формирования информационного наполнения веб-ресурса.

Для достижения защищённости ресурса от вирусов и хакеров, нужно уделять достаточно большое внимание политике информационной безопасности и уровню доступа, предоставляемого к публичной информации, размещенной на веб-ресурсе, согласно Закону Украины «О доступе к публичной информации».

Последняя редакция Закона определяет порядок обеспечения права каждого на доступ к информации, находящейся во владении субъектов властных полномочий, других распорядителей публичной информации, определенных настоящим Законом, и информации, представляющей общественный интерес.

Помимо изложенных выше мер предосторожностей, также следует соблюдать уровни ответственности, поддерживать программное обеспечение и оборудование в актуальном состоянии, правильно настраивать хостинг и следить за доступами к сайту. Если хотя бы один из этих элементов будет слабым звеном, веб-ресурс останется уязвимым.

1.2 Угрозы информационной безопасности веб-приложения

Современный мир функционирует благодаря работе сотням миллионов различных сайтов, веб-ресурсов и веб-приложений, поддерживающих работу информационных систем, обеспечивающих выполнение огромного количества работы, начиная от мелких торговых операций и заканчивая поддержкой электронного правительства.

Такие системы содержат не только персональные данные, но и финансовую информацию, которая требует защиты при хранении, обработке и передаче.

Внедрение различных платежных систем и торговых операций, которые заключаются удаленно, не только расширили круг потенциальных

злоумышленников, желающих заполучить доступ к этим объектам, но и дали огромный толчок развитию различного рода кибератак.

Как уже упоминалось ранее, за последние годы стремительно увеличивается количество атак, которые нацелены на веб-ресурсы.

Преступность в этой сфере стала более организованной и перешла от простейших замыслов студентов-хакеров, утверждающихся за счет таких сомнительных деяний к вполне осмысленным и тщательно подготовленным действиям по массовому сбору паролей и воровству финансовой информации.

Именно благодаря этому факту, безопасность информационных систем уже традиционно связывают с защитой от внешних угроз: вирусов, хакерских атак, спама.

Компания «ESET» является одной из лидирующих в сфере информационной безопасности, которая представляет основные направления распространения угроз. Согласно отчетам, на март 2018 года, по полученным данным с помощью системы быстрого оповещения ESET Live Grid, уверенными лидерами в Украине оставались вредоносные ПО для перенаправления жертв на зараженные сайты, ПО для скрытой добычи крипто-валюты, а также рекламное программное обеспечение. Согласно обзору событий, тенденция распространения компьютерных угроз продолжает нарастать.

Первое место в украинском рейтинге угроз в марте 2018 года (рис. 1.2) удалось удержать вредоносной программе HTML/Script Inject. Уровень распространения значительно снизился по сравнению с январем и февралем этого года. Вредоносное ПО перенаправляло пользователей на веб-сайты со встроенным вредоносным кодом в HTML страницы. Пользователи ничего не подозревали вплоть до момента перехода на ложный ресурс, но тогда уже было поздно.

Второе место заняло ПО - JavaScript Coin Miner для скрытой добычи крипто валюты. Вредоносный скрипт злоумышленники размещали как на фальшивых ресурсах, так и на зараженных легитимных сайтах. Пик

активности угрозы был зафиксирован в январе 2018 года. В течении первых трех месяцев уровень распространения JavaScript Coin-Miner уменьшился почти на 4% в Украине и на 13% в мире. Также небольшое уменьшение активности в течение марта продемонстрировали угрозы с подобным функционалом, такие как Win32 Coin Miner и Win64 Coin Miner.

Лидирующие позиции среди вредоносных программ замыкает угроза JavaScript Adware Agent S, которая после заражения устройства жертвы показывала рекламные баннеры и всплывающие рекламные сообщения во всех установленных на пользовательском ПК браузерах.

Четвертое место в рейтинге досталось угрозе в виде популярного интернет загрузчика Win32 Media Get с уровнем распространения 6.22%. Вредоносное ПО после установки в системе пользователя получало доступ к настройке расширений браузера, добавлению файлов для запуска во время загрузки системы и проникновению в другие процессы компьютера. Киберпреступники использовали данную угрозу для загрузки вредоносных приложений, рекламного ПО и также были зафиксированы случаи хищения личной информации с компьютера жертвы.

Последние позиции в рейтинге разделили с незначительным разрывом вредоносная программа HTML/Refresh, которая перенаправляла жертву на зараженные сайты, и программное обеспечение рекламного характера - PowerShell/Adware Adposhel.

В связи с постоянным совершенствованием вредоносных программ специалисты компании ESET рекомендуют пользователям быть предельно осторожными при работе в сети Интернет. Не пренебрегать использованием комплексных решений для эффективной защиты личных данных и конфиденциальной информации. Также воздержаться от посещения подозрительных и незнакомых сайтов будет крайне эффективным решением.

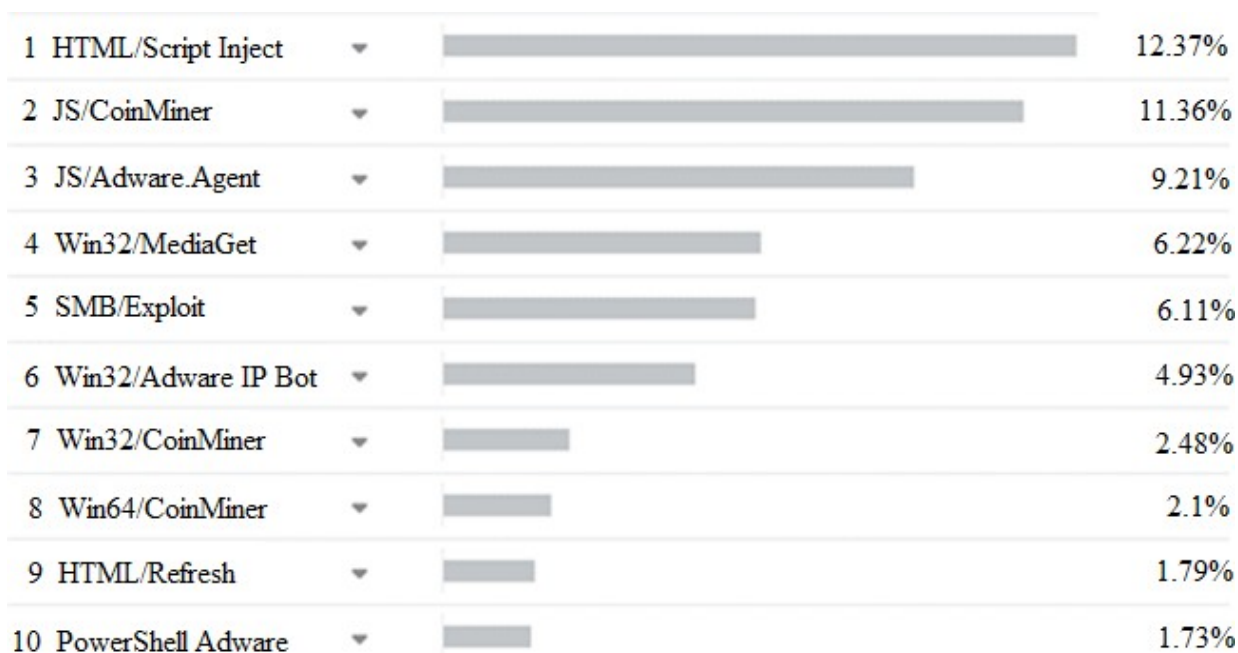


Рисунок 1.2 – Рейтинг вредоносных программ и скриптов в Украине: март, 2018

Однако в последнее время для ИТ-специалистов и заказчиков более актуальна тема внутренней безопасности, а именно методов и свойств, направленных на предотвращение утечки конфиденциальной информации предприятий по причине умышленных и неумышленных неправомерных действий собственных сотрудников. Как показывает опрос, этот вопрос является не менее важным в сравнении с первым вопросом.

Исследование проблемы внутренних ИТ-угроз показало, что украинские компании больше всего обеспокоены утечкой конфиденциальной информации: 48% опрошенных поставили данную угрозу на первое место. Второе место заняла возможность искажения информации - 32%. Остальные угрозы, показанные на рисунке 1.3, отстают с большим разрывом: сбои в работе ИС по причине халатности персонала - 13%, потеря информации - 4% и кража оборудования - 3%.

Как вывод следует тот факт, что чем крупнее организация, тем актуальнее для нее борьба с предотвращением утечки конфиденциальной информации.

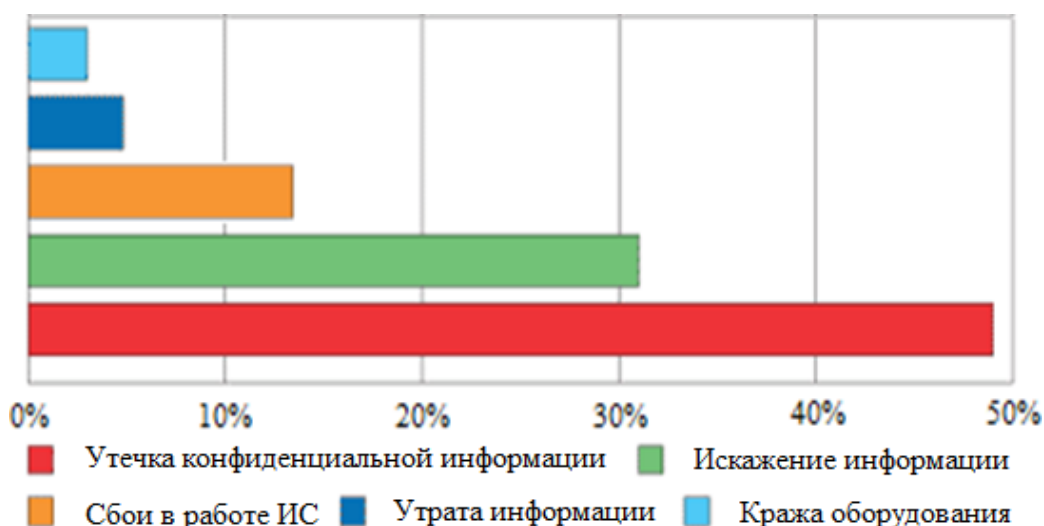


Рисунок 1.3 - Диаграмма наиболее значимых угроз

Из-за дублирования важных данных на резервных накопителях для экстренного восстановления в случае искажения или утраты оригинальных данных, повышаются шансы успешной атаки в два раза. В связи с большими объемами информации на крупных предприятиях, контроль над обращением информации - процесс трудоемкий, а значит и существенно возрастает цена утечки. Утрата конфиденциальности влечет за собой в первую очередь потерю статуса компании, что неминуемо приводит к материальному ущербу, а в особых случаях - и риск раскрытия государственной тайны.

1.3 Классификация уязвимостей и атак на веб-приложения

По мере продвижения компании в направлении распределенной обработки информации и упрощения доступа к ней, угроза нарушения безопасности соответственно приобретает более масштабный характер.

Такие обстоятельства определяют высокий уровень озабоченности данной проблемой не только представителей крупного бизнеса, но и правительственных организаций, задействованных в борьбе с целевыми атаками на веб-ресурсы.

Целевые атаки - это атаки, специально нацеленные на один сайт, веб-ресурс или их группу, объединенную общим признаком, таким как общий владелец, единая сфера развития. Опасность данного типа атак заключается именно в «заказном» характере. Исполнителями таких атак становятся злоумышленники, обладающие высокой квалификацией в области безопасности веб-приложений. Целью таких атак зачастую является получение конфиденциальной информации, которая может быть использована конкурентами или преступниками для получения прибыли. Целевые атаки проводятся в тени, тщательно планируются и чаще всего наносят удар в самые слабозащищенные места веб-ресурса. На рисунке 1.4 представлена круговая диаграмма наиболее популярных атак на веб-приложения.

Нецелевые атаки проводятся фактически «на удачу», а ее жертвами становятся случайные сайты независимо от популярности, размера бизнеса, географии или отрасли. Нецелевая атака на сайт не преследует конкретной цели получения несанкционированного доступа к веб-ресурсу, при которой злоумышленник не ставит целью взломать конкретный сайт, а атакует сразу большое количество ресурсов, отобранных по какому-то критерию.

Нецелевые атаки довольно «шумные» и в большинстве случаев не достигают поставленных целей, но, тем не менее, могут доставить множество проблем владельцу веб-ресурса.

При попытке взлома веб-ресурса атакующий преследует успешное достижение поставленных целей:

- закрепить на сайте, загрузив хакерский скрипт;
- оставить backdoor;
- добавить дополнительную учетную запись администратора;
- внедрить вредоносный код или получить необходимую информацию из базы данных.

Для обеспечения высокого уровня безопасности, необходимо учитывать, что угрозы в первую очередь, это уязвимости веб-приложений и их

компонентов, а также связаны с используемыми механизмами проверки идентификации.



Рисунок 1.4 – Рейтинг атак на веб-приложения

Атаки, направленные на автоматизированный процесс поочередного перебора подобрать имя пользователя, пароль, номер кредитной карточки, ключ шифрования, называются атаками типа Brute Force.

Угроза недостаточной аутентификации возникает, когда веб-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без процедуры должной аутентификации.

Небезопасное восстановление паролей - уязвимость возникает, когда веб-сервер позволяет атакующему несанкционированным путем получать, модифицировать или восстанавливать пароли других пользователей.

Атаки типа «авторизация» используются для определения наличия необходимых разрешений у пользователя, службы или приложения на совершение определенного действия. Многие сайты разрешают только определенным пользователям получать доступ к некоторому содержимому или функциям приложения. Используя широкий функционал своих

возможностей, злоумышленник может повысить свои полномочия и получить доступ к необходимым защищенным ресурсам или информационной системе в целом.

Предсказуемое значение идентификатора сессии (Credential/Session Prediction) - позволяет перехватывать активные сессии других пользователей.

Недостаточная авторизация (Insufficient Authorization) – возникает вследствие проведения веб-сервером некорректной процедуры авторизации пользователя, вследствие которой атакующий получает возможность доступа к важной информации или функциям, доступ к которым не должен иметь вовсе.

Отсутствие таймаута сессии (Insufficient Session Expiration) возникает в случае отсутствия таймеров для сессии каждого пользователя или его значение настолько велико, что злоумышленник может воспользоваться неактуальными данными для авторизации.

Атаки на клиентов (Client-side Attacks). Во время посещения сайта, между пользователем и сервером устанавливается доверительный контакт, как в технологическом, так и в психологическом планах. Пользователь подсознательно ожидает получения разрешенного содержимое, кроме того, не подозревая и не ожидая атак со стороны посещаемого сайта. Пользуясь таким доверием, атакующий может реализовать различные методы для проведения атак на клиентов.

Подмена содержимого (Content Spoofing) - используя эту технику, злоумышленник заставляет пользователя поверить, что страницы сгенерированы веб-сервером, а не переданы из внешнего источника.

Межсайтовое выполнение сценариев (Cross-site Scripting, XSS). Наличие уязвимости Cross-site Scripting позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя.

Внедрение SQL-кода является одной из распространённых вариаций взлома сайтов и программ, работающих с базами данных. Метод проведения

атаки основан на внедрении в серверный запрос произвольного SQL-кода.

Схема реализации данной атаки показана на рисунке 1.5.

Внедрение SQL, в зависимости от типа используемой СУБД и условий внедрения, может дать возможность атакующему выполнить запрос к базе данных, например, прочитать содержимое любых таблиц, удалить, изменить или добавить данные, а также получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере.

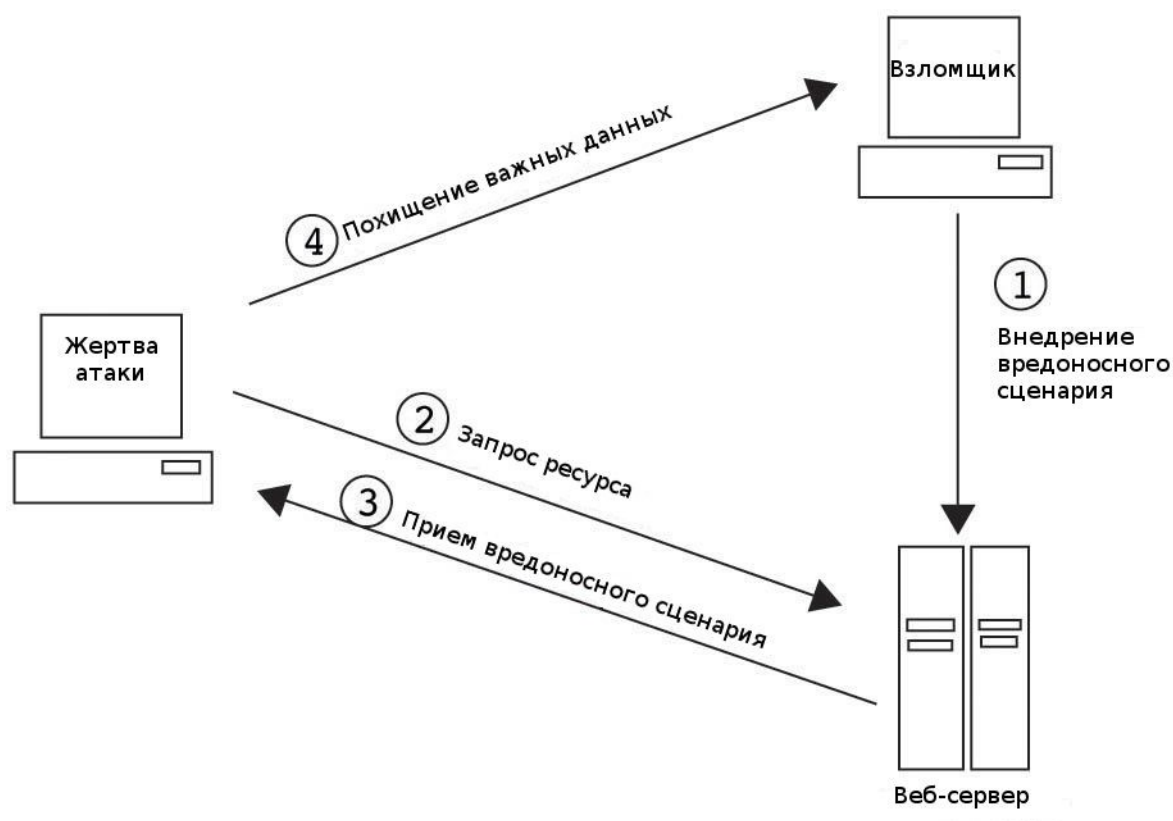


Рисунок 1.5 - Схема реализации SQL атаки

Расщепление HTTP-запроса (HTTP Response Splitting). Для успешной реализации данной уязвимости злоумышленнику необходимо послать серверу, специальный заранее сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа.

Выполнение кода (Command Execution) - атаки, использующие выполнение кода на веб-сервере. Все серверы используют данные, полученные от пользователя при обработке запросов. Эти данные

используются при составлении команд, применяемых для генерации динамического содержимого. Если при разработке не учитываются требования безопасности, злоумышленник получает возможность модифицировать исполняемые команды.

Переполнение буфера (Buffer Overflow) - переполнение буфера позволяет злоумышленнику изменить путь исполнения программы путем перезаписи данных в памяти системы.

Атака на функции форматирования строк (Format String Attack) - при использовании этих атак путь исполнения программы модифицируется методом перезаписи областей памяти с помощью функций форматирования символьных переменных.

Внедрение серверных сценариев (SSI Injection) - атаки данного класса позволяют злоумышленнику передать исполняемый код, который в дальнейшем будет выполнен на веб-сервере.

Внедрение операторов XPath (XPath Injection) - эти атаки направлены на веб-серверы, создающие запросы на языке XPath на основе данных, вводимых пользователем.

Разглашение информации (Information Disclosure) - атаки данного класса направлены на получение дополнительной информации о сайте. Используя эти уязвимости, злоумышленник может определить используемые дистрибутивы ПО, номера версий клиента и сервера и установленные обновления. В некоторых отдельных случаях, в утекающей информации может содержаться расположение временных файлов или резервных копий. Большинство серверов предоставляют доступ к чрезмерно большому объему данных, который необходимо минимизировать или вовсе устранить.

Утечка информации (Information Leakage) - эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например, комментарии разработчиков или сообщения об ошибках, которая может быть использована для компрометации системы.

Обратный путь в директориях (Path Traversal) служит для получения доступа к файлам, директориям и командам, находящимся вне основной директории веб-сервера.

Предсказуемое расположение ресурсов (Predictable Resource Location) позволяет злоумышленнику получить доступ к скрытым данным или функциональным возможностям.

Логические атаки (Logical Attacks) направлены на использование функций приложения или логики его функционирования с намерениями реализации собственных целей. Логика работы приложения представляет собой процесс функционирования программы при выполнении определенных действий. Примерами могут послужить восстановление паролей, регистрация учетных записей, транзакции с денежными средствами в банковских системах. Приложение может требовать от пользователя корректного выполнения нескольких последовательных действий для выполнения определенной задачи. Злоумышленник может обойти или использовать эти механизмы в своих целях.

Злоупотребление функциональными возможностями (Abuse of Functionality) направлено на использование функций веб-приложения с целью обхода механизмов разграничения доступа.

Отказ в обслуживании (Denial of Service) направлен на нарушение доступности сайта путем перегрузки трафика, поступающего на сервер. Схема реализации DDoS-атаки показана на рисунке 1.6.



Рисунок 1.6 - Схема реализации DDoS-атаки

Программные продукты так же могут быть случайно либо преднамеренно изменены или уничтожены самими программистами или пользователями. Создание резервных копий несет в себе угрозы нарушения работы программного обеспечения. Зачастую это связано с неотлаженной процедурой восстановления информации из резервных копий.

Присутствует определенный риск, что устанавливаемое ПО изначально является поврежденным или неработоспособным. Стоит учитывать тот факт, что чем больше используются ресурсы информационной системы, тем более уязвимой она становится.

1.4 Направления защиты веб-приложения

Современные методы защиты направлены на то, чтобы злоумышленник потратил больше времени, сил и ресурсов на получение

защищенной информации, чем себестоимость информации является в целом. С данной точки зрения следует рассматривать и планировать защиту информационного ресурса.

Также необходимость обеспечения безопасности данных связана со следующими причинами:

1. Непосредственные расходы на восстановление и простой. Такие расходы наиболее существенны и могут достигать таких значительных отметок, как расходы на уменьшение работоспособности (система защиты выстояла, но канал связи оказался переполнен запросами атакующего) и расходы на отвлечение персонала от их основной работы (крупные сбои могут задействовать на борьбу и восстановление большую часть персонала компании).

2. Снижение доверия клиентов. Крупные перебои в работе не удастся скрыть от общественности. Более популярные и более крупные компании привлекают больше внимания к себе как со стороны потребителей, так и конкурентов. А это создает опасность того факта, что клиенты перейдут к конкуренту и как следствие - частичная или полная потеря прибыли.

3. Опасностью судебного преследования. Нередко потеря денег клиентов или разглашение частной информации приводит к судебному разбирательству и значительным потерям на судебные издержки и возможные крупные компенсации.

4. Непосредственно потеря и/или разглашением секретных данных. Ущерб возникающий в следствии потери информации не поддается оценке, так как может быть огромен, вплоть до банкротства фирмы.

Инвестиции в обеспечение информационной безопасности в виде приобретаемых средств защиты, затрат на оплату труда специалистов, на проведение внешнего аудита безопасности, стремительно увеличивается из года в год, но как правило в большинстве случаев такие расходы не окупаются.

Главной причиной таких результатов в большинстве организаций происходит из-за того, что они продолжают придерживаться фрагментарного

подхода. Преимуществом обеспечения защиты с помощью такого подхода оправдывается только при слабой зависимости предприятия от ИТ и низком уровне рисков информационной безопасности в целом, но в наше время таких моделей организации уже не встречаются. ИТ сфера настолько расширилась, что стала неотъемлемой частью каждой компании.

Адекватный уровень информационной безопасности достигается путем комплексного подхода, предполагающего использование программно-технических и организационных мер защиты на единой концептуальной основе. При этом организационные меры играют первостепенную роль.

Эффективность самых сложных и дорогостоящих механизмов защиты сводится к нулю, в случае если пользователи игнорируют элементарные правила парольной политики, а сетевые администраторы нарушают установленные процедуры предоставления доступа к ресурсам корпоративной сети.

Наглядное изображение зависимости степени защищенности продукта от тщательного соблюдения правил пользования продуктом показаны на рисунке 1.7.

После идентификации угроз и рисков, направленных на систему, требуется изучить и определиться с контрмерами. Выбор методов противодействия должен производиться исходя из принципа разумной достаточности, то есть стоимость реализации контрмер не должна превышать количественную величину убытков.

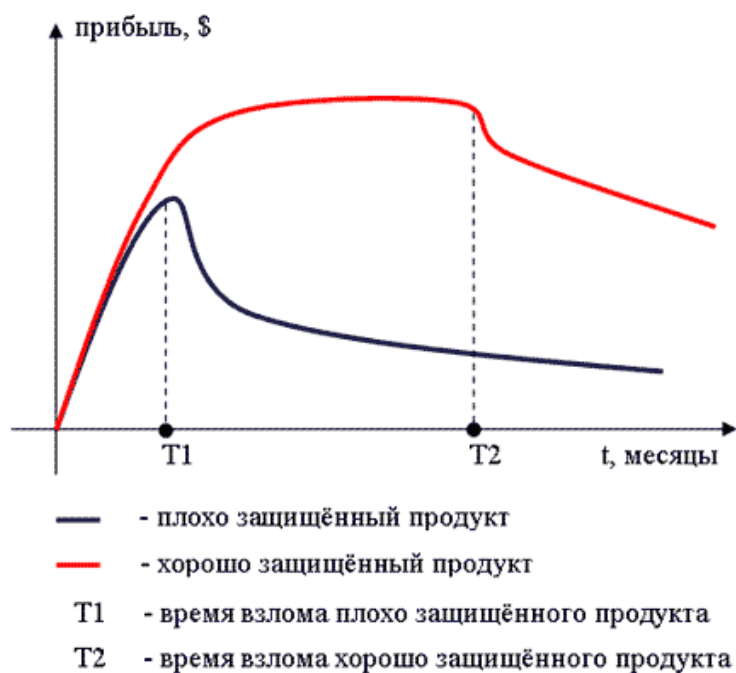


Рисунок 1.7 - Динамическая зависимость прибыли от степени защищенности продукта

Таким образом, после определения контрмер требуется принять решение о действии над риском:

- предотвратить его;
- ограничить;
- принять его - не предпринимая никаких мер для снижения

величины риска.

Система защиты должна обеспечивать следующие характеристики информации:

Конфиденциальность - гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации.

Целостность - гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения.

Доступность - состояние ресурсов, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

Аутентичность - гарантия того, что источником информации является именно то лицо, которое было заявлено как ее автор; нарушение этой категории называется фальсификацией автора ресурса.

Апеллируемость - гарантия того, что при необходимости можно доказать, что автором информации является именно заявленный человек и не никто другой. Отличие этой категории от аутентичности в том, что при подмене автора третье лицо пытается заявить, что оно - автор сообщения, а при нарушении апеллируемости - сам автор пытается отказаться от своего авторства.

Большинство инцидентов вызывают неудобство, но это не означает, что злоумышленник не сможет причинить компании серьезного ущерба. Поэтому следует применять меры по обеспечению безопасности своих ресурсов, оценив при этом уровень рисков и материальных затрат. Необходимо сопоставить возможные потери с теми преимуществами, которые предоставляет возможность выхода в Интернет.

В условиях ограниченных финансовых возможностей необходимо вкладывать средства в систему защиты наиболее уязвимых мест веб-ресурса. Можно выделить три уровня безопасности.

Уровень 1 - Минимальный уровень безопасности:

- модернизация имеющегося программного обеспечения;
- использование единых настроек для всего веб-ресурса.

Уровень 2 - Сопротивление вторжению:

- установка внешнего межсетевого экрана;
- ограничения на использование скриптов;
- обучение персонала.

Уровень 3 - Обнаружение атак и ослабление их воздействия:

- разделение привилегий;
- аппаратные системы защиты;

- системы обнаружения вторжений, размещаемые на серверах (хостах);
- использование решений, перечисленных в уровне 2.

Модернизация программного обеспечения является одним из наиболее простых, но вместе с тем наиболее эффективных способов уменьшения рисков. Все имеющиеся веб-ресурсы должны постоянно проверяться на предмет обновления установленного программного обеспечения.

Требование поддержания программного обеспечения в актуальной версии необходимо для минимизации риска того, что злоумышленник воспользуется ошибками и недочетами более ранних для проникновения в систему.

Обеспечение безопасности информации требует выделения отдельного ресурса под каждую задачу. В противном случае ошибка в системе безопасности может нарушить работу сразу нескольких сервисов. Нежелательно размещать сервер электронной почты, веб-сервер и сервер баз данных на одном и том же физическом устройстве. Однако каждый новый сервер должен быть оснащен системой защиты, иначе он может стать легкой мишенью для хакера.

Внешний Firewall.

Сетевой экран между внутренней сетью предприятия и веб-серверами общего доступа позволяет предотвратить проникновение случайных запросов в сеть организации. В случае проникновения на внешний веб-сервер, попадание в корпоративную сеть организации через firewall будет затруднительно.

Веб-сервер необходимо располагать отдельно от информационных серверов внутри корпоративной сети для того, чтобы снизить возможные шансы атакующего использовать захваченный ресурс в качестве плацдарма для дальнейшего продвижения в структуре системы, нарушения работоспособности и получения полного контроля над ней.

Ограничение использования скриптов.

Большинство веб-ресурсов содержат скрипты, которые запускаются при переходе на особую страницу. Злоумышленник может этим воспользоваться при помощи обнаруженных изъянов в коде для проникновения на сайт. Для обнаружения таких дыр не обязательно знать исходный код, поэтому скрипты необходимо тщательно проверить и защитить, прежде чем они будут внедрены в проект.

Обучение персонала.

Часто хакеры проникают в систему из-за халатного поведения администраторов сети. Зачастую они пренебрегают вопросами защиты или вовсе не владеют знаниями в области безопасности. Занимающим эту должность сотрудникам следует постоянно совершенствоваться, изучая системы безопасности сети и используя полученные знания на практике.

Разделение привилегий является прекрасным решением и структурированием работы всего штаба сотрудников и пользователей. Каждый пользователь или сотрудник имеет ограниченные права запуска только определенных скриптов, поэтому хакер, проникнувший в сеть по выявленным данным отдельного пользователя, сможет нанести системе лишь ограниченный вред. Хакер, добыв данные одного пользователя, окажется не в состоянии повлиять на прочие страницы и программное обеспечение.

Аппаратные решения.

Аппаратура, в плане разделения привилегий, имеет более высокий уровень безопасности, так как в отличие от программного обеспечения не так легко модифицируется. Но все же путем использования уязвимостей в программном обеспечении атакующий может получить доступ и к аппаратным средствам.

Установленные системы обнаружения вторжений на серверах, более эффективно справляются с поставленной задачей определения состояния сети, чем сетевые IDS. Обладая всеми возможностями сетевых IDS, серверные IDS лучше выявляют попытки нарушения защиты, так как обладают более высоким уровнем доступа к состоянию веб-сервера.

Но все же и этот способ имеет свои недостатки. Если хакер проникнет на веб-сервер, ему открывается возможность отключения серверных IDS, заблокировав тем самым получение сообщений об атаке для администраторов. Удаленные атаки на отказ сервиса также часто блокируют IDS на время выхода из строя сервера. А так как DoS-атаки позволяют злоумышленникам блокировать сервер без проникновения на него, то IDS, расположенный на сервере, должен быть дополнен сетевой системой обнаружения вторжений.

Ограничения существующих решений и дополнительные меры.

Специалисты в области информационной безопасности рекомендуют использовать защищенное программное обеспечение, но в некоторых случаях установить его невозможно из-за дороговизны или нехватки времени. Кроме того, безопасное программное обеспечение через некоторое время устаревает, и необходимо устанавливать новую версию. Поэтому использование устаревшего ПО и стандартных методов обеспечения безопасности не может служить гарантией защищенности серверов. Но устойчивость веб-приложения и сервера к атакам может быть достигнута при условии использования объективных решений по обеспечению безопасности совместно с надежным программным обеспечением, под которым, в данном случае, мы понимаем некоторое программное обеспечение, обладающее определенным уровнем безопасности.

Уровень безопасности программного обеспечения, может быть оценен путем анализа ранее совершенных атак на серверы, на которых было установлено такое же ПО. Количество атак показывает насколько устойчиво к ним ПО. Причем надежность программного обеспечения прямо зависит от его качества, так как учитывает все требования к системе безопасности.

Компании, специализирующиеся на создании систем безопасности в большинстве случаев, преувеличивают возможности своих продуктов, поэтому при дальнейшем проектировании системы безопасности необходимо учитывать это обстоятельство.

И наконец, оценка уровня безопасности программного обеспечения производится путем тестов на наличие уязвимостей. Существует множество компаний, занимающихся проверкой защищенности сервисов. Эти компании имеют в своем арсенале широкий выбор специализированного программного обеспечения, позволяющего выявлять различного рода «дыры» в системах безопасности веб-ресурса.

В первой главе были вынесены на рассмотрение вопросы касательно безопасности веб-приложений и онлайн ресурса, как единой информационной системы.

Прежде всего была рассмотрена актуальность темы исследования и принципы, на которых базируется политика информационной безопасности веб-приложения.

Для четкого понимания и определения направления дальнейшего развития исследования, в первую очередь было проведено изучение угроз информационной безопасности веб-приложения. В ходе работы были определены мотивы, руководствуясь которыми и совершается большинство атак на веб-ресурсы.

Для дальнейшего успешного развития работы была составлена классификация уязвимостей и атак, которым подвергаются защищаемые веб-приложения. Соответственно для того, чтобы предпринимать дальнейшие действия по улучшению качества защиты, были определены направления и основные идеи защиты веб-приложения.

2 ОБЕСПЕЧЕНИЕ ЗАЩИТЫ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ С ПОМОЩЬЮ ПРОТОКОЛА «WEBSOCKET»

2.1 Протокол WebSocket, как механизм защиты каналов передачи информации

На сегодняшний день технологии связи формируются, не просто развивая существующие стандарты. Зачастую расширение технологии сопровождается полным пересмотром самих основ, составляющих связи, поэтому первое время новая технология воспринимается неоднозначно.

Хорошо известный в наши дни протокол HTTP является изначально синхронным. Основан на модели «запрос - ответ» (рис 2.1).

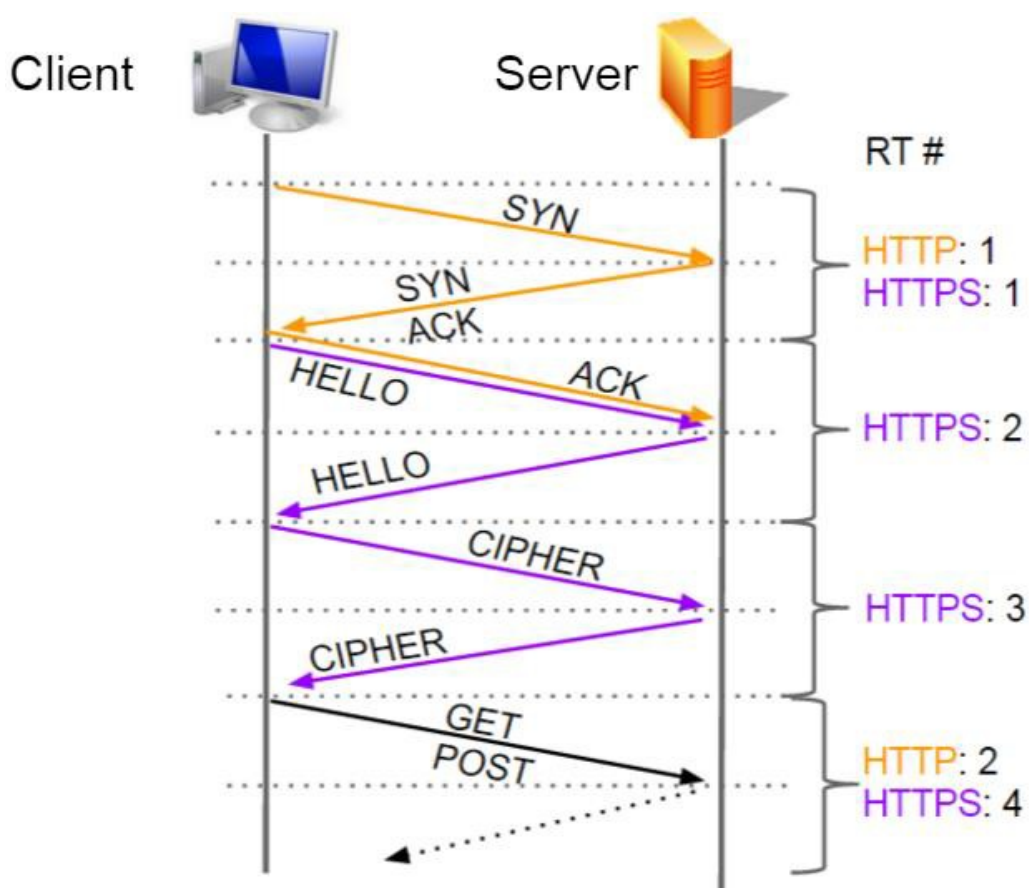


Рисунок 2.1 - Модель взаимодействия клиента и сервера с помощью протокола HTTP

Протокол «WebSocket» - это серьезное расширение HTTP, которое позволяет веб-приложениям поддерживать многопользовательское взаимодействие в режиме реального времени, что является хорошим преимуществом в сравнении с протоколом HTTP не только в плане функциональности, но и со стороны обеспечения должного уровня безопасности передаваемых данных.

Благодаря этому протоколу стирается тонкая грань клиента и сервера с фиксированными ролями, а вместо этого появляются два равноправных участника обмена данными (рис. 2.2).

При такой форме построения каждый из участников обмена работает сам по себе, и когда надо отправляет данные другому. Вторая сторона в свою очередь отвечает по мере необходимости, и только если эта необходимость возникнет.

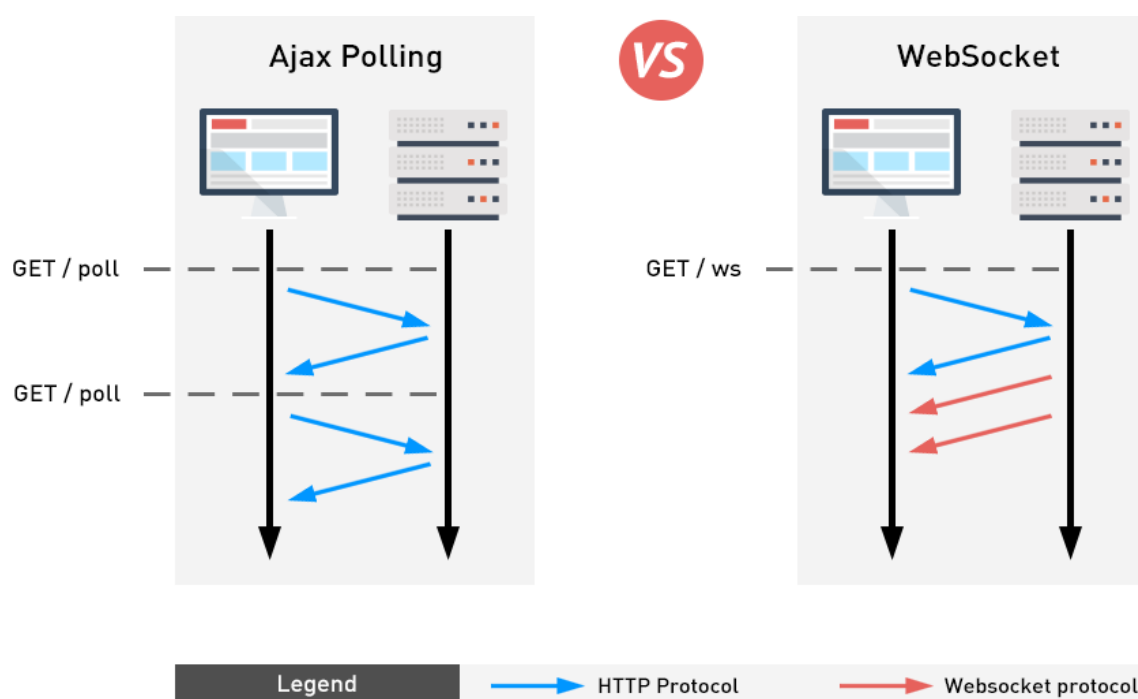


Рисунок 2.2 - Модель сравнения протокола HTTP с протоколом WebSocket

WebSocket - протокол полнодуплексной двунаправленной связи поверх TCP соединения, служит для обмена сообщениями между браузером и

сервером в режиме реального времени путем установления «равноправия» между клиентом и сервером.

Используя запросы XMLHttpRequest можно добиться нужного результата, но этот вариант является достаточно медленным, так как каждый раз необходимо создавать новое TCP соединение для каждого сообщения.

В отличие от XMLHttpRequest WebSocket устанавливает одно TCP соединение и подтверждает, что сервер может общаться с WebSocket, делая специальные проверки.

Как только страница браузера потребовала открыть WebSocket соединение на сервер, создается специальный JavaScript-объект. Все происходит как в обычном HTTP запросе. Браузер подключается по протоколу TCP по порту сервера 8080, но делает необычный GET запрос, как показано на рисунке 2.3. В случае поддержки сервером протокола WebSocket, клиенту поступает ответ, после чего сервер и клиент могут отправлять текстовые сообщения через установленное соединение при необходимости. Соединение постоянно поддерживается в открытом состоянии, но не передаёт лишних HTTP заголовков. При этом WebSocket не имеет ограничений на количество соединений.

С помощью данного протокола так же можно передавать изображения, только с использованием другого дата-фрейма. Был предусмотрен следующий алгоритм для избегания ограничений на длину передаваемого сообщения и для рационального расхода байт.

Каждый байт в указании длины рассматривается по частям - самый старший бит указывает, является ли этот байт последним (0) или же за ним есть другие (1), а младшие 7 битов содержат собственно данные.

При получении признака бинарного дата фрейма 0x80, берется следующий байт и откладывается в отдельную «копилку», потом берется следующий байт - если у него установлен старший бит, то переносится в «копилку». И так до тех пор, пока не встретится байт со старшим битом - 0. Это означает что этот байт - последний в указателе длины. Он также

складывается в «копилку». Теперь из всех байтов в «копилке» убираются старшие биты и соединяется в единый целый остаток. Вот это и будет длина тела сообщения.

КПД такого протокола стремится к 95%. Разница будет особенно заметна, если делать частый обмен небольшими блоками данных, ведь все уже готово: соединение открыто, остается переслать байты.

```
1 GET /chat HTTP/1.1
2 Host: server.example.com
3 Upgrade: websocket
4 Connection: Upgrade
5 Origin: http://server.example.com
6 Sec-WebSocket-Key: Iv8io/9s+lYFgZWcXczP8Q==
7 Sec-WebSocket-Version: 13
```

Рисунок 2.3 - GET - запрос на порт сервер 8080

В протоколе WebSocket предусмотрены несколько видов пакетов - «фреймов». Они делятся на два больших типа:

- фреймы с данными - «data frames»;
- управляющие - «control frames», предназначенные для проверки связи и закрытия соединения.

Фрейм, согласно стандарту, а именно первые 32 бита имеют вид (рис. 2.4). Сначала идёт бит FIN, затем биты RSV1, RSV2, RSV3, затем «опкод», «МАСКА» и «Длина тела», которая занимает 7 бит. Затем, если «Длина тела» равна 126 или 127, идёт «Расширенная длина тела», потом (на следующей строке, то есть после первых 32 бит) будет её продолжение, ключ маски, и потом данные.

Одно очень длинное сообщение, которое может состоять из множества фреймов, можно передать одним вызовом send. У всех фреймов, кроме последнего, этот фрагмент установлен в 0, у последнего - в 1.

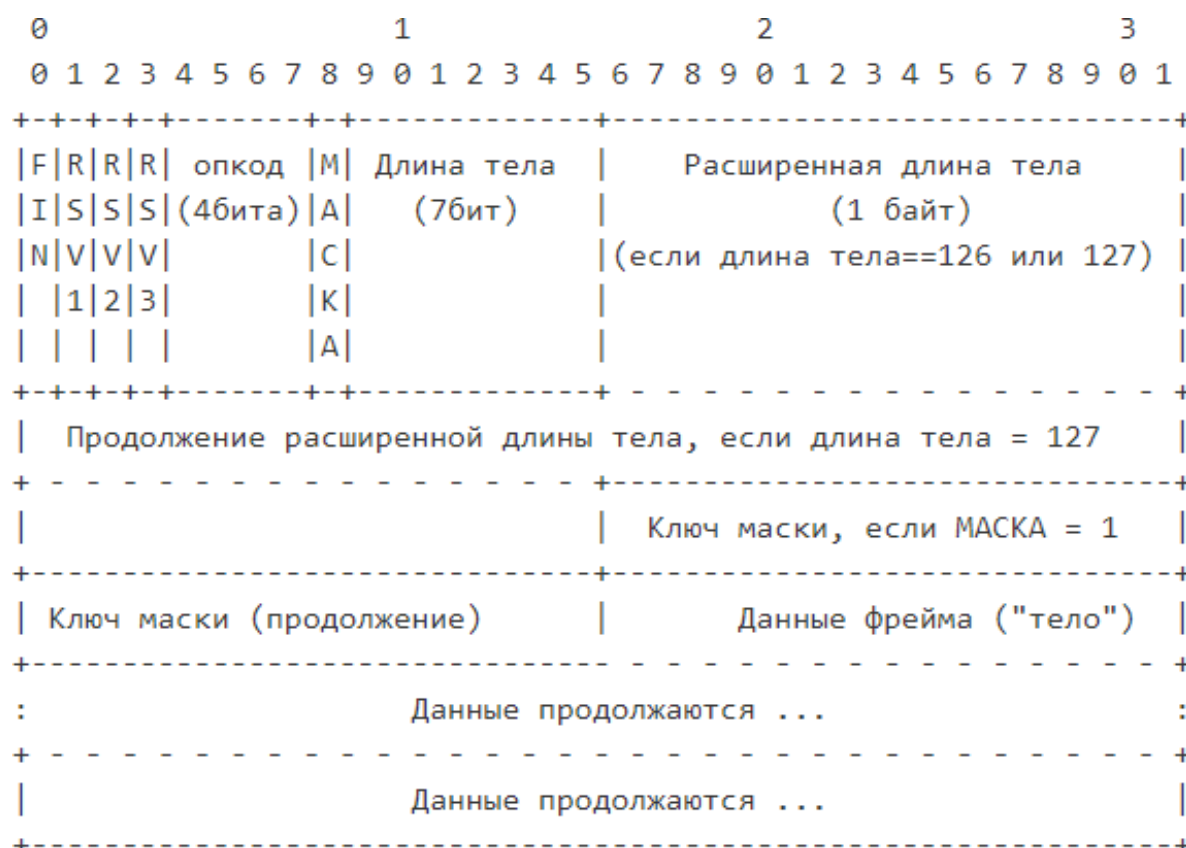


Рисунок 2.4 – Структура фрейма первых 32х бит протокола WebSocket

FIN: 1 бит.

Если сообщение состоит из одного-единственного фрейма, то FIN в нём равен 1.

Длина RSV1, RSV2, RSV3 равна 1 биту. Обычно значения равны 0, так как предназначены для расширений протокола, которые записываются в эти биты свои значения.

Опкод, длиною в 4 бита, задаёт тип фрейма, который позволяет интерпретировать находящиеся в нём данные. Возможные значения могут принимать такую форму:

- 0x1 - текстовый фрейм;
- 0x2 - двоичный фрейм;
- 0x3-7 - зарезервированы для будущих фреймов с данными;
- 0x8 - обозначает закрытие соединения этим фреймом;

- 0x9 - обозначает PING;
- 0xA - обозначает PONG.
- 0xB-F - зарезервированы для будущих управляющих фреймов.
- 0x0 - фрейм-продолжение для фрагментированного сообщения.

Он интерпретируется, исходя из ближайшего предыдущего ненулевого типа.

Маска длиной 1 бит, показывает наличие маскировки данных фрейма.

Длина тела: 7 битов, 7+16 битов или 7+64 битов:

- значение в интервале 0-125 - обозначает длину тела;
- значение 126 - следующие 2 байта интерпретируются как 16-битное без знаковое целое числа, содержащее длину тела;
- значение 127 - следующие 8 байт интерпретируются как 64-битное без знаковое целое, содержащее длину.

Данная схема применяется в качестве минимизации накладных расходов. Для сообщений длиной 125 байт и меньше хранение длины потребует всего 7 битов, для больших (до 65536) - 7 битов + 2 байта, а для ещё больших - 7 битов и 8 байт. Этого хватит для хранения длины сообщения размером в гигабайт и более.

Данные фрейма состоят из «данных расширений» и «данных приложения», которые идут за ними. Данные расширений определяются конкретными расширениями протокола и по умолчанию отсутствуют.

WebSocket - современное средство коммуникации, кросс-доменное и универсальное, но как и любая технология, на текущий момент имеет свои недостатки.

2.2 Недостатки протокола WebSocket и пути их устранения

Проблемы безопасности, связанные с WebSocket API, имеют фундаментальную основу, состоящую в возможности установить соединение между сторонами, не спрашивая разрешения у пользователя; кроме того, запрос посылается без оповещения самого пользователя.

Атакующему же в такой ситуации достаточно выполнить JavaScript код на стороне жертвы, чтобы заставить его установить соединение с произвольным сервером по протоколу WebSocket. Соединение может быть использовано атакующим для обмена данными с жертвой. Таким образом, происходит нарушение требования безопасности "Безопасное управление сессиями" и "Контроль доступа", а также становится возможным нарушение требования безопасности "Безопасное кэширование". Поскольку не все прокси - сервера корректно понимают протокол WebSocket, злоумышленник может заставить прокси кэшировать навязанные ему данные. В дальнейшем данная уязвимость применяется для нарушения других требований безопасности, путем навязывания JavaScript кода клиенту жертвы.

Фундаментальная проблема порождает несколько угроз. Для данных угроз приводятся сценарии атаки, показывающие то, как атакующий может ими воспользоваться.

Удаленная командная строка. WebSocket можно использовать для установления удаленной командной оболочки от сервера к клиенту. Соединение постоянно поддерживается в открытом состоянии, пока клиент не будет закрыт. Это нарушает требования безопасности "Безопасная обработка сессий".

Для этого сценария атаки предполагается, что атакующий может обманом заставить пользователя посетить его вредоносный сайт, либо эксплуатировать XSS - уязвимость в посещаемом пользователем веб-приложении описанную ранее в работе.

После того, как атакующий сможет запустить JavaScript код в клиенте пользователя, он сможет установить соединение по протоколу WebSocket. После установления соединения он получает полный доступ к клиенту жертвы и может запустить вредоносный JavaScript код. Кроме этого, злоумышленник получает доступ ко всем данным пользователя, а также возможность перенаправить клиент жертвы на другие зараженные сайты. Соединение

действует до момента закрытия пользователем клиента, однако в течении этого времени злоумышленник может полностью контролировать ситуацию.

Ботнет на базе Всемирной паутины. WebSocket позволяет серверу установить удаленное соединение и командную строку ко многим клиентам одновременно. Сервер может использовать эти интерфейсы для построения ботнетов, что в свою очередь нарушает требования безопасности «Безопасная обработка сессий» и «Защита клиента».

Для реализации данной атаки необходимо проделать те же самые действия, что и в ситуации с удаленной командной строкой. Существенное отличие состоит в том, что атакующий должен иметь возможность обманом завлечь большое число пользователей на свой сайт, либо воспользоваться данной уязвимостью на очень популярных сайтах с большим потоком клиентов. Отличным примером использования такой уязвимости может стать проведение масштабных DDoS атак, а самое главное, что выявление первоначального источника атаки будет практически невозможно, поскольку явными источниками атаки будут клиенты пользователей.

Отравление кэша. Кэш некоторых веб-прокси серверов может быть «отравлен» из-за неправильной трактовки процедуры рукопожатия WebSocket. Это нарушает требование безопасности «Безопасное кэширование».

Возможность отравления кэша прозрачного прокси существует не из-за изъянов в протоколе WebSocket. Причина заключается в том, что прокси не понимает рукопожатия данного протокола и действует лишь на основании доменного имени, указанного в поле Host заголовка, которое заведомо ложно.

Во второй главе было принято решение по использованию протокола WebSocket в качестве основного механизма защиты каналов передачи информации.

В ходе проведения работы прежде всего был проведен сравнительный анализ предложенного решения с хорошо известным протоколом HTTP.

Положительные результаты сравнения в пользу протокола WebSocket подтвердили правильность выбранного решения.

Для успешного формирования механизма защиты, обеспечивающего высокий уровень безопасности передаваемой информации, был изучен сам протокол WebSocket. Но, как и любая технология, протокол не совершенен, имеет свои недостатки.

Для дальнейшего успешного развития работы была выявлена причина возникновения данных недостатков, а также были рассмотрены угрозы и сценарии атак, возникающие в следствии успешного использования недостатков протокола.

3 СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

3.1 Механизм защиты от успешной реализации XSS уязвимости

Большинство уязвимостей напрямую зависит от некорректной обработки получаемых данных или недостаточно строгой их проверкой. Межсайтовое выполнение сценариев (Cross Site Scripting - XSS) является одной из таких уязвимостей, которая позволяет атакующему передать серверу исполняемый код и перенаправлять пользователя на зараженный ресурс, вставке в веб-ресурс вредоносного кода, краже COOKIE файлов и прочей информации.

Для успешного противостояния XSS уязвимости прежде всего следует тщательно соблюдать и выполнять требования в организации работы веб-приложения.

Первое, что необходимо выполнить - проверить наличие кодировки на каждой веб-странице (рис. 3.1). Для каждой веб-страницы необходимо указывать кодировку (ISO-8859-1 или UTF-8) до каких-либо пользовательских полей.

```
1  <!DOCTYPE html>
2  <html lang="en">
3
4  <head>
5      <meta charset="UTF-8">
6      <meta name="viewport" content="width=device-width, initial-scale=1.0">
7      <meta http-equiv="X-UA-Compatible" content="ie=edge">
8
9      <link rel="stylesheet" href="css/main.css">
10     <script src="js/index.js" defer></script>
11     <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
12
13     <title>sayHi Chat</title>
14 </head>
```

Рисунок 3.1 - Проверка наличия кодировки на веб-странице

Если в мета тегах кодировка не указана, браузер пытается сам определить кодировку страницы. Стандарт HTML 5 не рекомендует использовать кодировки, которые включают JIS_C6226-1983, JIS_X0212-1990, JOHAB (Windows code page 1361), а также кодировки, основанные на ISO-2022 и EBCDIC. Эти кодировки никогда не предназначались для веб-контента.

В случае если тег расположен до тега и заполняется пользовательскими данными, злоумышленник может вставить вредоносный html код в кодировке UTF-7, обойдя, таким образом, фильтрацию символов.

Так же во избежание «просачивания кода» через поля ввода воспользуемся подходом «белых списков». Подход работает по принципу «что не разрешено, то запрещено». Это стандартный механизм проверки правильности полей для проверки всех входных данных, включая заголовки, строки запросов, скрытые поля и поля форм, а также их длину полей форм, тип, допустимые символы прежде чем принять данные, которые будут сохранены и отображены на сайте.

Для полей ввода пользовательских данных при авторизации в службе мгновенных сообщений применим собственный фильтр для проверки вводимых данных пользователями. Пример работы подсказки для пользователя показан на рисунке 3.2.

Для поле ввода логина и пароля разрешим только буквы, дефис и цифры, а все остальные символы отклоним. Лучше отклонить достоверную информацию и потом через службу поддержки ее изменить, чем принять заведомо вредоносные данные.

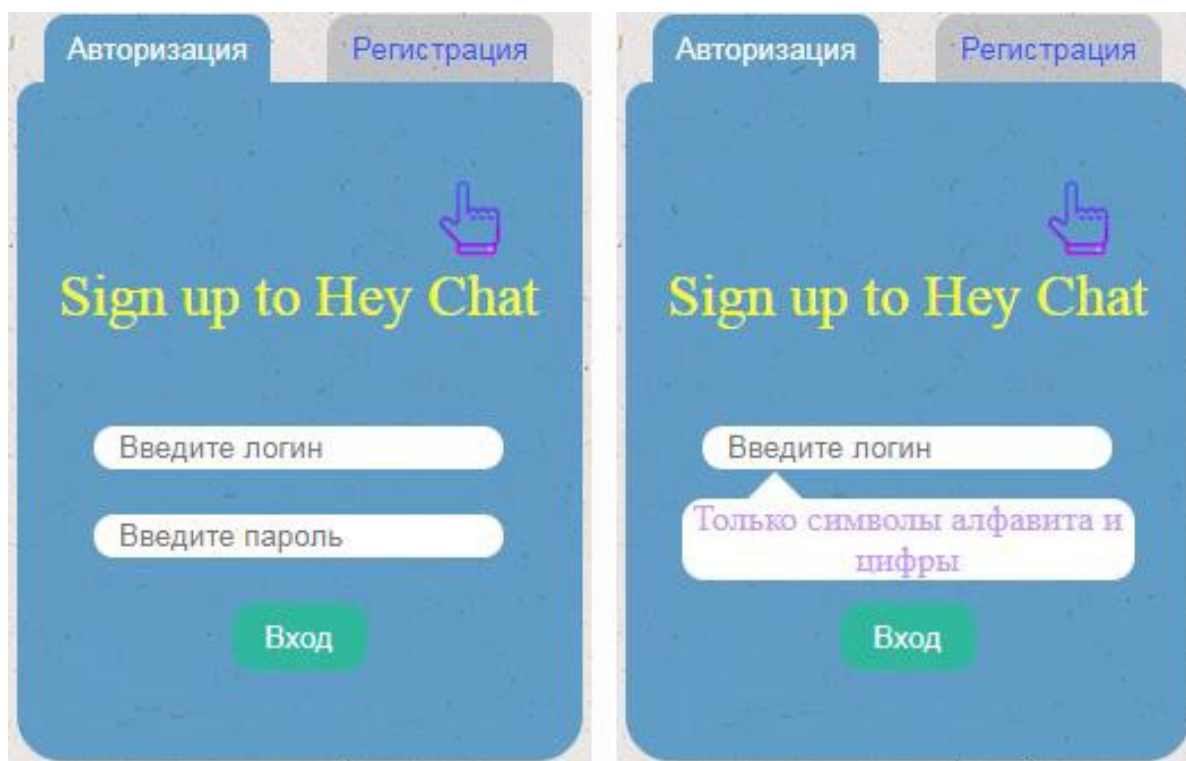


Рисунок 3.2 - Видимая для пользователя подсказка о наличии фильтра ввода данных

Значительным преимуществом собственно созданного фильтра является возможность корректировки и изменения его по мере необходимости. Таким образом, со временем методы фильтрации будут усовершенствованы.

Так же в качестве дополнительно защиты от уязвимости был разработан механизм проверки активности пользователя и его активного нахождения на сайте (рис. 3.3). Данное решение позволит избежать поддержки фоновой активности пользователя, тем самым как можно больше уменьшить период времени, который позволит злоумышленнику получить доступ ко всем данным пользователя, а также возможность перенаправить клиент жертвы на другие зараженный сайты.

Функция «connection» на стороне сервера играет в пинг-понг с каждым своим клиентом, с которым установлено соединение. Каждую секунду проверяется активное наличие пользователя на веб-ресурсе. Если же на

стороне пользователя не происходит отправка ответа, сервер пытается установить соединение еще раз, в случае неудачной попытки, в журнал событий регистрируется ошибка (рис. 3.4) от том, что не удалось установить соединение и закрывает его.

```
121 function connection() {  
122     var web = new WebSocket("ws://localhost:3001");  
123     web.addEventListener("error", function(e) {  
124         setTimeout(() => {  
125             WEB = connection();  
126         }, 1000);  
127     });  
128  
129     web.addEventListener("close", function(e) {  
130         setTimeout(() => {  
131             try {  
132                 WEB = connection();  
133             } catch (err) {  
134                 console.log(err);  
135             }  
136         }, 1000);  
137     });  
138     return web;  
139 }
```

Рисунок 3.3 - Программная реализация функции «Connection»

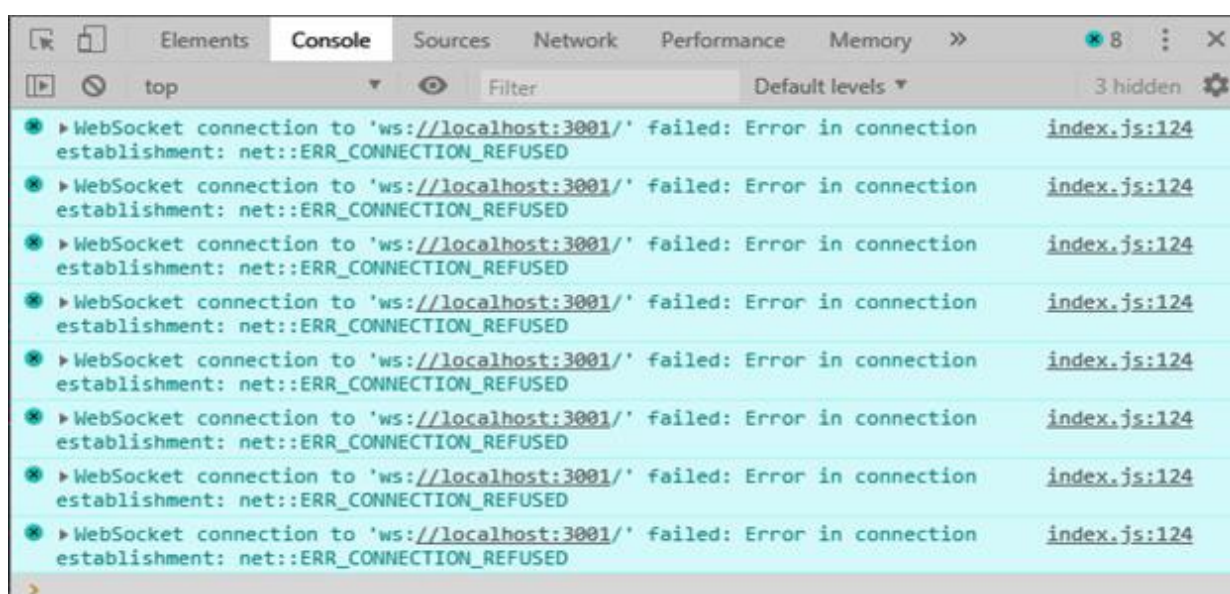


Рисунок 3.4 - Отчет консоли браузера о разрыве соединения с сервером

Данные механизмы защиты направлены на максимально возможное снижение риска успешной атаки посредством реализации XSS уязвимости. Невозможно гарантировать полную защиту от данной угрозы путем безопасной реализации серверной стороны. Для этого также необходимо провести комплексную работу на клиентской стороне вроде ручного отключения поддержки протокола WebSocket.

3.2 Защита паролей с использованием методов шифрования

Для защиты пользовательских данных, а именно паролей был выбран метод одностороннего шифрования. Это лучший способ для сохранения паролей. «Одностороннее шифрование» подразумевает возможность преобразовать данные в зашифрованную строку, но благодаря запутанным алгоритмам и высшей математике обратное преобразование невозможно.

С помощью этого метода легко можно хранить пароли пользователей, а им в свою очередь не нужно волноваться о том, что кто-то еще знает их пароли. В то же время легко можно проверить правильность ввода просто сравнив хеш введенного пароля с сохранённым в БД, а также при необходимости изменить пароль.

Хеширование - процесс создания хеш-последовательности из исходной строки.

В веб-приложениях данные функции используются для безопасного хранения паролей в базе данных. Хеш-функция становится последней границей защиты, если атакующий успешно провел локальную атаку на систему аутентификации.

Предоставленная далее классификация содержит требования, которым должен удовлетворять хеш в базе данных:

- устойчивость к атакам перебора – методы прямого и обратного перебора, перебор по словарю;
- невозможность поиска одинаковых паролей по хешу.

Успешное выполнение первого требования достигается использованием стойких в настоящее время хеш-функций.

Для выполнения второго требования к паролю перед хешированием добавляется случайная строка – соль. Таким образом, у двух пользователей с паролем «1234» будут разные соли - «соль1» и «соль2», а соответственно и хеш-функции от «1234соль1» и «1234соль2» в базе тоже будут разные.

Чтобы усложнить процесс перебора во время атаки следует дописать «соль» к шифруемому паролю. Так как хеш-функция вычисляется последовательно по строке, то злоумышленнику при переборе «соленых» хешей, будет проще, когда хеш-выражение начинается с соли. Атакующий может вычислить заранее хеш и далее считать (хеш и соль) + (хеш и пароль) достаточно быстрее для всех последующих паролей, которые подвергнутся перебору.

При выборе метода хеширования, помимо трудозатрат, задаются вопросом производительности. Более стойкие алгоритмы потребляют больше ресурсов. Наглядное сравнение скорости перебора хешей, полученных на видео карте AMD Radeon 7990 показано на рисунке 3.5. Единицы измерения - мегахэши в секунду, то есть количество хешей в секунду.

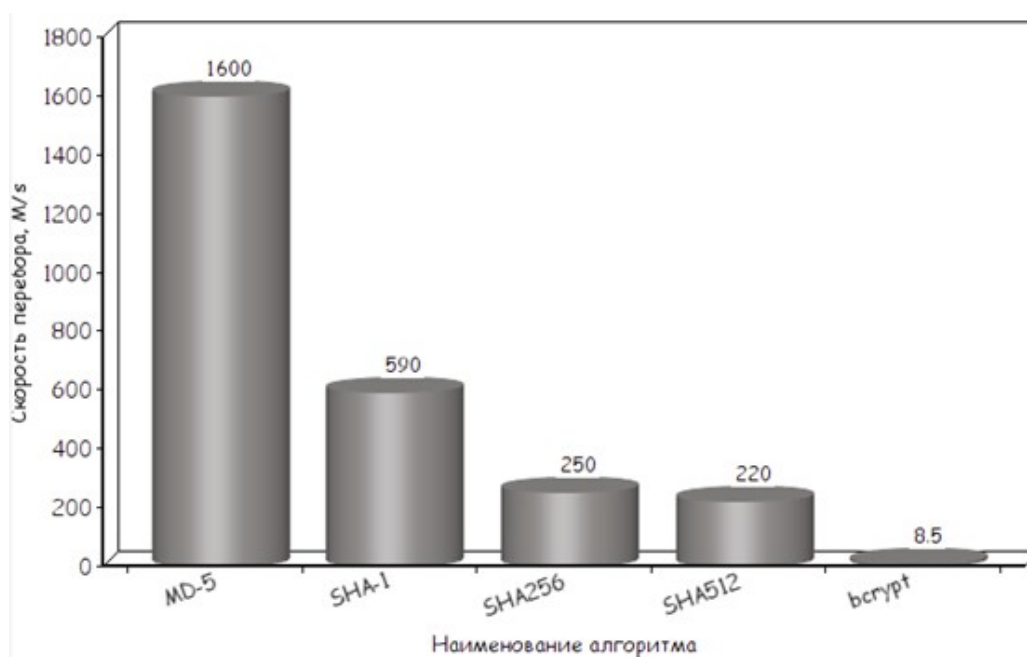


Рисунок 3.5 – График скорости перебора хешей в секунду

Исходя из приведенной диаграммы можно сделать вывод, что функция `bcrypt` лидирует с огромным отрывом.

Для того чтобы еще усложнить жизнь атакующему предлагается ввести еще одну дополнительную составляющую - локальный параметр.

«Вторая соль» дописывается ко всем выражениям (пароль + соль), как показано на рисунке 3.6 и является одинаковой для всех хешей в базе. Преимущество состоит в том, что локального параметра в базе нет. Это константа системы, которая хранится в памяти приложения, куда она попадает из настроек ПК пользователя.

Очень простая и действенная мера, которая позволяет практически полностью исключить атаку перебора по данным только одного хеш хранилища.

```
var bcrypt = require("bcrypt");
// пароль пользователя
var passwordFromUser = "test_user_pass";
// создаем соль
var salt = bcrypt.genSaltSync(10);

exports.cryptPassword = function(passwordFromUser, callback) {
  bcrypt.genSalt(10, function(err, salt) {
    if (err) {
      return callback(err);
    } else {
      // шифруем пароль
      return (passwordToSave = bcrypt.hashSync(passwordFromUser, salt));
    }
  });
};
```

Рисунок 3.6 - Реализация программного кода функции хеширования паролей

3.3 Защита JavaScript кода с помощью обфускации

Немало важную роль в защите веб-приложения играет уровень защищенности самого исполняемого кода - JavaScript кода. На данный момент не существует универсального способа, позволяющего полностью скрыть код

от глаз посетителя, но существуют методы приведения исходного текста программы к виду, сохраняющему ее функциональность, но значительно затрудняющему анализ и понимание логики работы исполняемого кода.

Главным преимуществом обфускации является модифицирование исходного кода таким образом, чтобы его невозможно было подвергнуть обратному процессу. Это значительно снижает шансы атакующего на успешную реализацию уязвимостей и помогает предотвратить кражу собственности.

Существует несколько инструментов для обфускации, которые также сжимают код и уменьшают время, требуемое для загрузки кода в браузер, что позволяет добавить оптимизации в работу веб-ресурса.

С точки зрения безопасности обфусцированный JavaScript может избегать обнаружения антивирусами, также усложняя процесс понимания кода.

Существует множество доступных по сети инструментов, которые позволяют уменьшить читаемость JavaScript кода, такие как минификаторы и обфускаторы. Минификаторы созданы, чтобы облегчать код путем удаления неиспользуемых частей и замены символов, что позволяет уменьшить время загрузки этого кода браузером.

Для достижения поставленной цели воспользуемся JavaScript Obfuscator. В результате проделанной программой работы, на выходе получаем рабочий, но вовсе не читабельный исполняемый код (рис. 3.7), который не подлежит обратной операции.

Для наглядного примера работы JavaScript Obfuscator был выбран случайный участок исполняемого кода веб-приложения. В целях повышения уровня защиты JavaScript кода, изменениям подвергается полный программный код.

```

document.forms[0].userName.addEventListener("input", function() {
    this.classList.remove("error");
});
document.forms[0].userPass.addEventListener("input", function() {
    this.classList.remove("error");
});
document.querySelector(".btn-menu").onclick = function() {
    document.querySelector(".online-bar").classList.toggle("width");
    document.querySelector(".s2").classList.toggle("big-width");
    setTimeout(function() {
        document.querySelector(".a").classList.toggle("hidden");
    }, 80);
};
document.querySelector(".btn-exit").onclick = function(event) {
    document.querySelector(".s1").classList.remove("hidden");
    document.querySelector(".s2").classList.add("hidden");
    document.querySelector("body").classList.remove("home");
    document.querySelector("body").classList.add("start");
};
document.querySelector(".btn-drop").onclick = function(event) {
    document.querySelector(".btn-drop").classList.toggle("trick");
};
document.querySelector(".btn-status").onclick = function(event) {
    console.log(event);
    var STATUS = document.querySelector(".btn-status");
    var data = document.querySelector(".btn-status").getAttribute("data");
    if (data == "1") {
        STATUS.innerHTML = "ONLINE";
        STATUS.style.color = "green";
        STATUS.setAttribute("data", "2");
    } else if (data == "2") {
        STATUS.innerHTML = "OFFLINE";
        STATUS.style.color = "red";
        STATUS.setAttribute("data", "3");
    } else {
        STATUS.innerHTML = "STATUS";
        STATUS.style.color = "white";
        STATUS.setAttribute("data", "1");
    }
};

```

Рисунок 3.7 - Участок кода до работы обфускатора

В результате работы JavaScript Obfuscator, исполняемый программный код приобрел вид, изображенный на рисунке 3.8. Читательность кода и

понимание логики работы программы стало невозможным, однако сохранена полная работоспособность веб-приложения.

```
var _0xa1da=
["\x69\x6E\x70\x75\x74","\x65\x72\x72\x6F\x72","\x72\x65\x6D\x6F\x76\x65"
,"\x63\x6C\x61\x73\x73\x4C\x69\x73\x74","\x61\x64\x64\x45\x76\x65\x6E\x74"
"\x4C\x69\x73\x74\x65\x6E\x65\x72","\x75\x73\x65\x72\x4E\x61\x6D\x65","\x6"
"\x6F\x72\x6D\x73","\x75\x73\x65\x72\x50\x61\x73\x73","\x6F\x6E\x63\x6C\x"
"\x69\x63\x6B","\x2E\x62\x74\x6E\x2D\x6D\x65\x6E\x75","\x71\x75\x65\x72\x79\x"
"\x53\x65\x6C\x65\x63\x74\x6F\x72","\x77\x69\x64\x74\x68","\x74\x6F\x67\x67"
"\x6C\x65","\x2E\x6F\x6E\x6C\x69\x6E\x65\x2D\x62\x61\x72","\x62\x69\x67\x2"
"\x77\x69\x64\x74\x68","\x2E\x73\x32","\x68\x69\x64\x64\x65\x6E","\x2E\x6"
"\x61\x64\x64","\x68\x6F\x6D\x65","\x62\x6F\x64\x79","\x73\x74\x61\x72\x74","\x2E\x62\x74"
"\x6E\x2D\x64\x72\x6F\x70","\x74\x72\x69\x63\x6B","\x2E\x62\x74\x6E\x2D\x7"
"\x3\x74\x61\x74\x75\x73","\x6C\x6F\x67","\x64\x61\x74\x61","\x67\x65\x74\x4"
"\x1\x74\x74\x72\x69\x62\x75\x74\x65","\x31","\x69\x6E\x6E\x65\x72\x48\x54\x"
"\x4D\x4C","\x4F\x4E\x4C\x49\x4E\x45","\x63\x6F\x6C\x6F\x72","\x73\x74\x79\x"
"\x6C\x65","\x67\x72\x65\x65\x6E","\x32","\x73\x65\x74\x41\x74\x74\x72\x69\x"
"\x62\x75\x74\x65","\x4F\x46\x46\x4C\x49\x4E\x45","\x72\x65\x64","\x33","\x5"
"\x3\x54\x41\x54\x55\x53","\x77\x68\x69\x74\x65"];
```

Рисунок 3.8 – Участок пода после работы обфускатора

В случае необходимости внесения изменений в проект, в частности в программный код, используется оригинал кода, который был до преобразования. Вносятся необходимые изменения, после создается копия файла, которая снова подвергается изменениям программой JavaScript Obfuscator.

В третьей главе была проведена работа над улучшением и устранением уязвимостей протокола WebSocket с целью дальнейшего повышения уровня безопасности передаваемой информации по каналам связи.

Для успешного противостояния XSS уязвимости прежде всего были применены меры по соблюдению и выполнению требований в организации работы веб-приложения со стороны обсуживающего персонала.

В качестве решения проблем безопасности был разработан собственный, универсальный фильтр с возможностью дальнейшего внесения корректировок для проверки вводимых данных пользователем.

Так же в качестве дополнительной защиты от уязвимости был разработан механизм проверки активности пользователя и его активного нахождения на сайте.

На стороне сервера для защиты пользовательских данных, а именно паролей был реализован метод одностороннего шифрования для сохранения паролей пользователей в базе данных.

В качестве дополнительной меры защиты от постороннего вмешательства, исполняемый код веб-приложения был подвергнут обфускации. Данное решение послужит дополнительной мерой защиты кода не только от внешнего вмешательства, но и от попыток изучить его структуру и логику работы, при это сохраняя полную работоспособность веб-приложения.

4 ЭКОНОМИЧЕСКАЯ ЧАСТЬ

4.1 Актуальность темы с позиции маркетинга

Защита информации и проблема обеспечения целостности и конфиденциальности приобретает актуальность для очень многих людей, в том числе, чья деятельность находится вне области, где эти вопросы решают государственные органы.

В наши дни основным информационным ресурсом является глобальная сеть интернет, соответственно возрастает число веб-приложений в международной виртуальной сети и количество каналов передачи информации, а также их разнообразие.

Защита каналов передачи информации должна предоставлять сохранность пересылаемых данных от широкого круга различных угроз, таких, как утечка информации, несанкционированные воздействия, копирование и незаконное использование.

Программные продукты являются результатом труда специалистов высокой квалификации. Процесс проектирования и создания новых программных продуктов сопровождается значительными финансовыми и трудовыми затратами, основан на использовании наукоемких технологий и инструментов, требует применения соответствующего уровня дорогостоящей техники. Это влечет за собой необходимость принятия мер по защите интересов разработчика, его программного продукта, не только внутри фирмы, но и за ее пределами от несанкционированного копирования и использования.

Исследуя рынок технологий, необходимо учитывать тот факт, что услуги связи не являются однородными по качеству, полезности и цене для всех категорий потребителей. Поэтому одним из важных направлений маркетинговых исследований является определение качественных и количественных характеристик рынка конкретной услуги, уточнение его структуры с целью эффективной реализации собственных возможностей и

готовой продукции. Анализ структуры рынка услуг связи за 2016 год показал, что прежде всего оцениваются объемы и структура в соответствии с приведенной схемой (рис. 4.1).

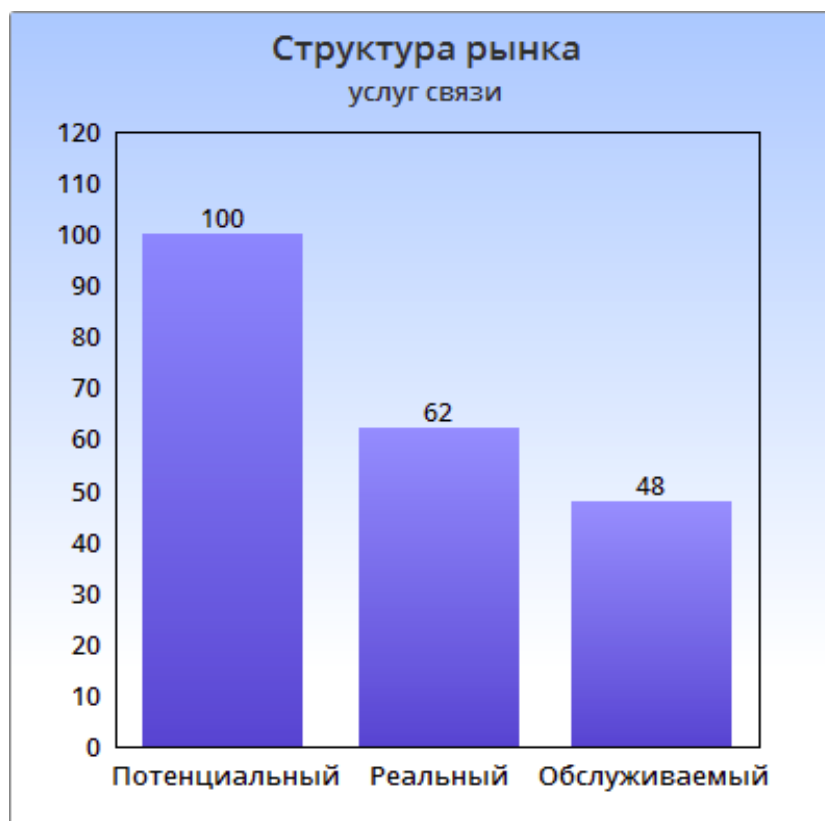


Рисунок 4.1 - Схема определения объема и структуры рынка услуг связи

Потенциальный рынок является той частью потребителей услуг связи, проявляющих интерес к приобретению соответствующей услуги. Эта часть может быть определена в ходе наблюдений или опросов.

Реальный, рынок определяется долей потребителей, принявших решение о покупке той или иной услуги связи.

Обслуживаемый рынок - часть настоящего рынка, получающая услуги у данного производителя.

Согласно исследованиям, в Украине активно пользуются услугами связи почти 21,5 млн человек по данным на 2016 год. Подобное структурирование рынка дает важную информацию о потенциальных

возможностях фирмы на рынке, состояние маркетинговой сферы, эффективность мероприятий фирмы по рекламе и продвижению своих услуг, использования прогрессивных средств стимулирования сбыта.

4.2 Расчет сметы затрат на практическую реализацию проекта

В составе расходов на реализацию проекта учитывается стоимость всех ресурсов, необходимых для реализации комплекса работ.

С целью определения затрат на реализацию проекта составляем смету расходов, приведенных в таблице 4.1.

Таблица 4.1 - Смета затрат на реализацию проекта

Статья расходов	Сумма	
	грн	%
Заработная плата персонала	118000	49%
Отчисления на единый социальный взнос	25960	10.7%
Специальное оборудование	95000	39.3%
Расходы на услугу сторонних фирм	1576	0.9%
Расходы на общехозяйственные затраты	696	0.1%
Общая сумма расходов	241232	100%

Смета затрат показала, что наибольшую долю составляют выплаты заработной платы и отчисления на единый социальный взнос. Так же немаловажную часть занимают затраты на приобретение техники, необходимой для реализации проекта.

4.3 Расчет заработной платы

Расходы по статье выплат заработной платы составляются исходя из планового фонда заработной платы всех категорий работающих, задействованных при реализации проекта. Расчет расходов производится на основе данных о трудоемкости работы (таблица 4.2).

Количество месяцев работы над проектом составляется исходя из сроков реализации проекта. В данном случае ожидаемое время реализации проекта составляет не более 4 месяцев. Результаты расчетов приводятся в таблице 4.2.

Таблица 4.2 - Смета затрат на выплату заработной платы участникам проекта

Исполнитель	Количество дней	Зарплата плата грн / месяц	Заработная плата, грн
Руководитель проекта	120 дней	18000	72000
Системный аналитик	30 дней	10000	10000
Программист	90 дней	12000	36000
Итого			118000

4.4 Расчет отчислений на единый социальный взнос

Расходы по данной статье рассчитываются в размере 22% от основной и дополнительной заработной платы. Расчет приведен в таблице 4.3.

Таблица 4.3 - Смета затрат по отчислениям на единый социальный
взно́с

Исполнитель	Заработная плата за весь период, грн	Отчисления по ЕСВ, грн
Руководитель проекта	72000	15840
Системный аналитик	10000	2200
Программист	36000	7920
Итого	118000	25960

4.5 Расчет расходов на оборудование

Для выполнения задач по моделированию и программированию информационных систем нам понадобится следующее оборудование, представленное в таблице 4.4.

Таблица 4.4 - Смета затрат на специальное оборудование

Оборудование	Количество, шт	Стоимость, грн
Компьютер	2	70000
Ноутбук	1	25000
Итого	3	95000

В качестве специальной оснастки в данном случае будет выступать ОС Windows.

Установленное программное обеспечение является полностью бесплатным, или свободно предоставляемым разработчиками на ограниченный срок.

Стоимость специального оборудования и специальной оснастки закладывается в стоимость компьютерного оборудования и составляет 95000 грн.

4.6 Расчет расходов на услуги сторонних организаций

В раздел расходов включается оплата работ и производственных услуг, проведенных другими организациями при выполнении данной исследовательской работы в соответствии с заключенными договорами.

К статье принадлежат расходы на доступ в сеть Интернет с помощью сторонних организаций, а именно, Интернет-провайдера «Фрегат». Провайдер не взимает первоначальный взнос за подключение, а ежемесячная стоимость за услуги провайдера – 144 гривны.

Сумма расходов на срок 4 месяца составит: $144 \cdot 4 = 576$ грн.

Также предусмотрен вызов мастера технической поддержки для проведения профилактики работы компьютеров раз в два месяца. Стоимость услуги составляет 500 грн за вызов. Вызов мастера предусмотрен два раза на период выполнения работы: $500 \cdot 2 = 1000$ грн

Общая сумма расходов по данной статье на срок 4 месяца составит: $576 + 1000 = 1576$ грн.

4.7 Расчет расходов на общехозяйственные затраты

Общехозяйственные расходы рассчитываются в случае если они непосредственно связаны с выполнением данных работ.

К данным расходам относятся расходы на электроэнергию. По ставке Запорожьеоблэнерго за 1 кВт/час и ежемесячном потреблении электроэнергии порядка 150 кВт/час, затраты составят:

- 0,9 грн за киловатт при использовании до 100кВт·ч/месяц;
- 1,68 грн за киловатт при потреблении более 100кВт·ч/месяц.

Таблица 4.5 - Смета расходов на электроэнергию

Количество	Количество	Стоимость за 1 месяц, грн	Расходы за 4 месяца, грн
до 100 - 0,9 грн за киловатт	100 кВт	90	360
свыше 100 - 1,68 грн за киловатт	50 кВт	84	336
Итого			696

Таким образом общехозяйственные расходы по срокам реализации проекта составят 696 грн.

4.8 Расчет на амортизацию объектов основных средств и нематериальных активов

Амортизация - это процесс переноса стоимости основных средств и нематериальных активов по мере их физического или морального износа по частям на себестоимость производимой продукции. В процессе производства ряд ресурсов (оборотные средства - сырьё и материалы) полностью

преобразуются или списываются при каждом цикле производства. Стоимость полностью входит в состав себестоимости конечной продукции.

Другая часть ресурсов (основные средства - оборудование, здания, сооружения), участвуют в нескольких производственных циклах, зачастую длительно сохраняя при этом свою натуральную форму. Но через некоторое время основные средства будут нуждаться в ремонте, модернизации или замене, в том числе из-за морального износа.

Амортизация - в широком смысле - бухгалтерская и налоговая концепции, используемые для оценки потери величины стоимости активов с течением времени.

Амортизация объектов основных средств.

Компьютер. Первоначальная стоимость 35000 грн. Полный срок его полезного использования 4 года (48 месяцев). Для расчета коэффициента амортизации воспользуемся формулой 4.1.

$$K = 1/N \cdot 100\% \quad (4.1)$$

Согласно формуле 4.1, коэффициент амортизации: $1/48 \cdot 100\% = 2,08\%$. Амортизационные отчисления на один компьютер за один месяц будут составлять: $35000 \cdot 2,08\% = 728$ грн.

Так как будут использоваться 2 компьютера в течении 4 рабочих месяцев, амортизационные отчисления по одному компьютеру составят: $728 \cdot 4 = 2912$ грн.

Амортизационные отчисления на два компьютера составят $2912 \cdot 2 = 5824$ грн.

Ноутбук. Первоначальная стоимость 25000 грн. Полный срок его полезного использования 4 года (48 месяцев). Для расчета коэффициента амортизации воспользуемся формулой 4.1. Согласно формуле 4.1, коэффициент амортизации: $1/48 \cdot 100\% = 2,08\%$. Амортизационные отчисления на один ноутбук за один месяц будут составлять: $25000 \cdot 2,08\% =$

= 520 грн. Так как будет использоваться ноутбук в течении одного рабочего месяца, амортизационные отчисления рассчитываются на весь период реализации проекта: $520 \cdot 4 = 2080$ грн.

Полные амортизационные отчисления в период выполнения работ за 4 месяца составят: $\Sigma = 5824 + 2080 = 7904$ грн.

4.9 Бальная оценка экономической эффективности проекта

Маркетинговые исследования, проектные разработки, прямой подсчет экономической эффективности по которым не представляется возможным, оценивают с помощью балльной системы.

Бальная оценка проводится по следующим важнейшим показателям:

- важность разработки - K_1 ;
- возможность использования результатов разработки - K_2 ;
- теоретическая значимость и степень новизны исследования - K_3 ;
- сложность разработки - K_4 .

Таблица 4.6 - Шкала для оценки важности разработки K_1

№	Показатель	Баллы
1	Инициативная работа, не является частью комплексной программы	1
2	Работа, выполняемая по договору о научно-техническую помощь	3
3	Работа представляет часть ведомственной программы	5
4	Работа представляет часть ведомственной комплексной программы	7
5	Работа представляет часть международной комплексной программы	8

Разработка K_1 составила 5 баллов.

Шкала оценок возможности использования результатов разработки K_2 , оценки теоретической значимости и степени новизны, оценки показателей сложности приведены в таблицах 4.7, 4.8, 4.9.

Таблица 4.7 - Шкала оценки возможности использования результатов разработки K_2

№	Показатель	Баллы
1	В данном подразделе	1
2	В данной организации	3
3	Во многих организациях	5
4	В масштабах страны	8

Разработка K_2 составила 5 баллов.

Таблица 4.8 - Шкала оценки теоретической значимости и уровня новизны исследования K_3

№	Показатель	Баллы
1	Анализ, обобщение и классификация известной информации. Подобные результаты были известны в исследуемой области	2
2	Получение новой информации, дополняющей знания о сущности исследуемых процессов, не известны в исследуемой области	3
3	Получение новой информации, меняет представление о сущности изучаемых процессов, не известной ранее	5

Продолжение таблицы 4.8 - Шкала оценки теоретической значимости и уровня новизны исследования К₃

№	Показатель	Баллы
4	Создание новых теорий, методик	6
5	Получение информации, способствующей формированию направлений, неизвестных ранее	8

Разработка К₃ составила 3 балла.

Таблица 4.9 - Шкала оценки показателей сложности исследования К₄

№	Показатель	Баллы
1	Работа выполняется одним подразделением, расходы менее 10000 грн.	1
2	Работа выполняется одним подразделением, расходы 10000-50000 грн.	3
3	Работа выполняется одним подразделением, расходы 50000-250000 грн.	5
4	Работа выполняется с участием многих подразделений, расходы 250000-500000 грн.	7
5	Работа выполняется несколькими организациями, расходы более 500000 грн.	8

Разработка К₄: 5 балла.

Общая оценка устанавливается произведением коэффициентов: $5 \cdot 5 \cdot 3 \cdot 5 = 375$;

Удельный эффект на каждый балл - 20 000 грн. Общий эффект от разработки составляет: $A = I_n \cdot 20000 = 375 \cdot 20000 = 7\,500\,000$ грн;

Экономическая эффективность от реализации проекта определяется с помощью коэффициента эффективности, характеризующий долю общего эффекта от разработки, приходится на одну грн. расходов (себестоимости НИР) согласно формуле 4.2.

$$K = \frac{A}{\Sigma} \quad (4.2)$$

Экономическая эффективность от реализации проекта приходящаяся на одну грн. расходов согласно формуле 4.2, составит:

$$K = \frac{7500000}{241232} = 31,1$$

В результате проведенных расчетов, можно сказать, что реализация проекта принесет доход в 7500000 грн, что при затратах в 241232 грн и 4 месяца на выполнение задания является экономически выгодным вложением и необходимым в плане улучшения защиты каналов связи.

5 ОХРАНА ТРУДА И БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

5.1 Анализ потенциальных опасностей

Процесс работы программиста происходит в офисном помещении в окружении других сотрудников компании и напрямую связан с использованием определенных инструментов окружающей среды таких, как вычислительные устройства, оргтехника и компьютер. В результате такого взаимодействия сотрудник может подвергаться воздействию различных факторов, пагубно влияющих в той или иной степени на организм.

Условия труда подразделяют на четыре класса: оптимальные (I), допустимые (II), вредные (III) и опасные или экстремальные (IV).

Первые два класса не превышают предельно допустимые величины ПДВ - условия труда являются безопасными. Для III класса факторы превышают ПДВ, возможно профессиональное заболевание. В случае IV класса риск профессионального заболевания очень высок. Оценка класса условий труда производится на основе инструментальных измерений факторов производственной среды и сравнения их с ПДВ.

ПДВ фактора - это минимальная или максимальная величина, при которой человек может работать нормальную рабочую смену весь трудовой период до выхода на пенсию и при этом у него не возникает отклонений здоровья, вызванных этим фактором. Превышение допустимых значений является нарушением правил охраны труда и требует принятия мер по их снижению, либо доплат за риск.

При эксплуатации персонального компьютера на программиста могут оказывать действие следующие опасные и вредные производственные факторы:

1. Опасность поражения электрическим током в следствии несоблюдения правил электробезопасности или выхода из строя электроприборов.

2. Напряжение в электрической цепи, замыкание которой может произойти через тело человека.
3. Электромагнитное излучение от ПК, экранов мониторов и другой оргтехники.
4. Нарушение работы костно-мышечного аппарата в результате длительных статических нагрузок при работе с ПК.
5. Неудовлетворительные эргономические характеристики рабочего места, нерационального планирования рабочего места, что может привести к получению механических травм, поражений электрическим током и нарушений костно-мышечного аппарата.
6. Повышенная яркость светового изображения, напряжение зрения, внимания, длительные статические нагрузки.
7. Негативное влияние недостаточного освещения рабочей зоны на зрение и производительность работающего, вследствие неисправности осветительных приборов или неправильного проектирования осветительной системы.
8. Нервно-психические перегрузки вследствие постоянного контакта с клиентами и коллегами по работе, контакт с начальством при решении поставленных задач и вопросов, которые могут носить конфликтный характер и приводить к эмоциональному дискомфорту, внутреннему раздражению работника, эмоциональной нестабильности и заболеваниям нервной системы работающего.
9. Негативное влияние повышенного уровня шума на психоэмоциональное состояние сотрудника, связанный с использованием устаревшей периферийной техники, кондиционеров, осветительных приборов.
10. Негативное влияние неудовлетворительных параметров воздушной среды рабочей зоны на здоровье работающего, вследствие неправильного проектирования системы вентиляции или ее неисправности.

11. Опасность возгорания в связи с неисправностью электрического оборудования, несоблюдение или нарушение правил противопожарной безопасности обслуживающим персоналом, может привести к пожару.

12. Неправильные и несогласованные действия персонала в чрезвычайных ситуациях.

При эксплуатации электрооборудования опасным производственным фактором является электрический ток. Предельно допустимая величина переменного тока 0,3 мА. При увеличении тока до 0,6-1,6 мА человек начинает ощущать его воздействие.

Виды поражения электрическим током:

- электрический удар (паралич сердца и дыхания);
- термический ожог;
- технические повреждения;
- электро-офтальмия - воспаление глаз вследствие действия электротока.

5.2 Мероприятия по обеспечению безопасности

Офисное помещение, в котором находятся и работают программисты, относятся к помещениям без повышенной опасности поражения электрическим током. Оборудование, используемое в таких помещениях, является потребителем электроэнергии переменного тока 220В от сети с заземленной нейтралью, и относится к электроустановкам до 1000В закрытого исполнения.

В помещении размещена электропроводка с напряжением в сети 220В. При этом существует опасность поражения током при электрическом пробое на корпус, который может произойти как в системном блоке компьютера, так и в периферийных устройствах.

По способу защиты человека от поражения электрическим током соответствует ГОСТ 12.2.007.0-75(2001) "ССБТ. Изделия электротехнические. Общие требования безопасности».

I группа - стационарные компьютеры, и II группа - осветительные приборы, кондиционеры, отопительные устройства, ноутбуки, сканеры.

Согласно «Правилам устройства электроустановок» («ПУЭ») выполнены следующие группы мероприятий по электробезопасности:

Конструктивные меры обеспечивают защиту от случайного прикосновения к токоведущим частям с помощью их изоляции и защитных оболочек. Согласно ГОСТ 12.1.009-76 (1999) «ССБТ. Электробезопасность. Термины и определения» в приборах II класса защиты используется двойная изоляция - электрическая изоляция, состоящая из рабочей и дополнительной изоляции. Так как согласно НПА ОП 40.1-1.32-01 «Правила устройства электроустановок. Электрооборудование специальных установок» офисные помещения в большинстве своем относятся к классу пожароопасных зон П-Па, помещения, в которых содержатся твердые горючие вещества, поэтому предусмотренный уровень защиты изоляции оборудования IP44.

Схемно-конструктивные меры предназначены для обеспечения защиты от поражения электрическим током при прикосновении к металлическим оболочкам, которые могут оказаться под напряжением в результате аварий. Согласно ГОСТ 12.1.030-81 (2001) «ССБТ. Электробезопасность. Защитное заземление, зануление» в помещениях устраивается зануление.

В случае, если напряжение электроустановки меньше 1000В, используются следующие схемы трехфазных сетей: трехфазная трехпроводная сеть с изолированной нейтралью и трехфазная четырехпроводная сеть с изолированной нейтралью.

Сотрудник офиса может соприкоснуться с трехфазной схемой по двум сценариям: однофазному и двухфазному включениям. Двухфазное включение человека в электрическую цепь наиболее опасно.

Работающая аппаратура, а также её периферийное оборудование являются источниками электромагнитных полей различных частот. Степень воздействия электромагнитных полей на человека зависит от:

- интенсивности излучения;
- диапазона частот (НЧ, ВЧ, УВЧ);
- продолжительности воздействия;
- характера излучения;
- размеров облучаемой поверхности;
- индивидуальных особенностей человека, что является наиболее важным фактором.

Электромагнитные поля оказывают два вида воздействия на человека:

- тепловое - возникают ионные токи в организме человека. Может также возникать перегрев и ожоги;
- биологическое - возникает опасность для слизистой оболочки глаз и гортани.

Нормирование электромагнитных полей регламентирует ГОСТ 12.1.006.84.

Средствами защиты сотрудника является защитная изоляция токоведущих частей оборудования и частей, которые могут оказаться под напряжением, а также проводов и кабелей.

Для работы на персональных компьютерах рекомендуется использование специальных спектральных очков для защиты глаз от напряжения и мерцания монитора.

Для предотвращения статистической нагрузки при использовании ПК рекомендуется делать перерывы в работе на 5-10 минут через каждые два часа работы перед монитором.

Синдром запястного канала или туннельный синдром запястья, который может быть следствием хронической травмы, случается у людей в результате длительной работы с мышью - постоянное напряжение и сдавливание приводит к микротравмам, сдавливание нерва прилегающими

окружающими тканями, что приводит к возникновению отека. Чтобы туннельный синдром вас не беспокоил, нужно придерживаться несколько правил организации рабочего места:

- оптимальная высота клавиатуры от пола - 65-75 см;
- наличие эргономичных и удобных лично для вас мыши и клавиатуры;
- возможность регулировки высоты и наклона клавиатуры (расстояние от поверхности стола до середины клавиатуры - не более 30 мм, угол подъема клавиатуры - от 2° до 15°);
- наличие у клавиатуры подставки для рук;
- наличие коврика для мыши с защитой от туннельного синдрома - специальный выступ обеспечивает правильное положение кисти;
- наличие стула или кресла с подлокотниками.

Площадь на одно рабочее место, оборудованное компьютером для пользователей должна составлять не менее 6м², а объем не менее - 20м³.

Рабочее место, оборудованное персональным компьютером по отношению к световым проемам должно располагаться так, чтобы естественный свет падал сбоку, желательно слева.

Схемы размещения рабочих мест должны учитывать расстояния между рабочими столами с мониторами:

- расстояние между боковыми поверхностями мониторов не менее 1,2 м;
- расстояние между экраном монитора и тыльной частью другого монитора не менее 2 м.

При работе с мышкой и клавиатурой также следует придерживаться определенных правил. Когда вы набираете текст, рука должна быть согнута в локте под прямым углом, а при работе с мышкой следите, чтобы кисть была прямой и лежала на столе как можно дальше от края. Также при работе с компьютером, время проведения за ним следует ограничить до действительно необходимого. Также, чтобы предупредить туннельный

синдром нужно делать специальные упражнения для кистей - чем чаще, тем лучше. Эти упражнения помогут улучшить кровообращения в мышцах и растянуть их. Комплекс упражнений нужно повторять примерно каждые 45 минут, продолжительность одного упражнения - 1-2 мин.

Самая страдающая часть тела программиста - глаза. Именно глаза больше всего подвержены негативному воздействию работы за компьютером.

Современная техника улучшается с каждым днем и уже не встречаются мерцающие экраны с вредным излучением, но тем не менее, глаза устают. А с ними приходит головная боль и ощущение тяжести. Неподвижность глазных яблок, уставленных в экран, практически в одну точку, приводит к напряжению мышц глаз. Атрофирование мышц глаза может впоследствии привести к снижению остроты зрения, поэтому, не стоит пренебрегать пятиминутными перерывами для выполнения глазной гимнастики. Делать гимнастику, как удобно и интересно, главное - делать. Это очень помогает избавиться от усталости глаз.

Неправильная осанка и проблемы с позвоночником также преследуют офисного сотрудника и программиста, в частности. Если целый день сидеть, сгорбив спину, позвоночник будет постоянно находиться в искривленном состоянии. При этом пережимаются важные нервные окончания, расстояние между позвонками уменьшается, подвижность и гибкость позвоночника снижается. Возникают боли между позвонками.

Наш позвоночник - самая гибкая кость и он обязан двигаться. Кроме того, он - основа скелета и держит на себе мышцы тела. При отсутствии движения позвоночника получаем не только плохую осанку и боли в спине, но и как следствие - плохое состояние скелетных мышц.

От постоянной статичности и однообразной позы в теле появляется ощущение вялости и усталости. Поэтому необходимо ежедневно растягивать позвоночник, выполняя простые упражнения:

1. Станьте ровно, медленно наклоните голову вниз, прижимая подбородок к груди. Ощутите, как происходит натяжение позвоночника.

2. Нужно максимально вытянуть шею, тянуться макушкой вверх, плечи при этом максимально опущены вниз, копчик, направлен вниз, прогиба в спине нет. Должно быть ощущение растягивания позвоночника.

3. Выполняйте движения грудной клеткой вперед-назад, влево-вправо. Ваша задача - прогнуть грудной отдел позвоночника.

4. Поворачивайте корпус влево-вправо, ноги и таз при этом остаются на месте, а позвоночник скручивается.

Эти упражнения можно вполне делать в офисе в перерывах между работой, много времени это не занимает, а пользу для организма приносит огромную. При ходьбе старайтесь максимально выравнивать спину. Огромным плюсом станет привычка заниматься спортом. Вид спорта не важен, главной задачей является обеспечить позвоночнику подвижность. Усталость - это прежде всего затёкшие неподвижные мышцы и суставы.

Нервное напряжение влияет на сердечно-сосудистую систему, увеличивая артериальное давление и частоту пульса, а также на терморегуляцию организма и эмоциональные состояния сотрудника. Особую роль в предотвращении усталости работников играют профессиональный отбор, организация рабочего места, правильное рабочее положения, ритм работы, использования эмоциональных и материальных стимулов, внедрение рациональных режимов труда и отдыха.

Борьба с усталостью, в первую очередь, сводится к улучшению санитарно-гигиенических условий производственной среды - ликвидация загрязнения воздуха, шума, вибрации, нормализация микроклимата, рациональное освещение рабочего места и помещения в целом.

5.3 Мероприятия производственной санитарии и гигиены труда

Главным объектом охраны труда является человек в процессе труда и при разработке требований производственной санитарии используются результаты исследований ряда медицинских и биологических дисциплин.

Успех в решении проблем охраны труда в большой степени зависит от качества подготовки специалистов, от их умения принимать правильные решения в сложных условиях современного производства.

Организация и улучшение условий труда на рабочем месте является одним из важнейших резервов производительности труда и экономической эффективности производства, а также дальнейшего развития самого сотрудника. Для поддержания длительной работоспособности человека большое значение имеет режим труда и отдыха.

Физиологически рациональным режимом труда и отдыха является такое чередование периодов работы с периодом отдыха, при котором достигается высокая эффективность общественно-полезной деятельности человека, хорошее состояние здоровья, высокий уровень работоспособности и производительности.

После установления нормального производственного процесса, сменный режим труда и отдыха рабочих становится эффективным средством предупреждения утомления работающих.

Рациональная организация труда на рабочем месте связана с проблемой правильной организации работы в течение всей недели, что обеспечивается систематической научной организацией производства. Для поддержания длительной работоспособности человека имеет большое значение не только суточный и недельный режим труда и отдыха, но и месячный, ежегодный.

Для создания оптимальных условий труда на рабочем месте необходимо устанавливать оптимальные показатели условий для каждого вида производства характеризующих производственную среду. Для получения доступа к работе сотрудники должны пройти медицинский осмотр.

Немало важным факторов в работе программиста является производственное освещение, которое бывает:

Естественным - обусловлено прямыми солнечными лучами и рассеянным светом небосвода. Меняется в зависимости от географической широты, времени суток, степени облачности.

Искусственным - создаётся искусственными источниками света (лампы, светильники). Применяется при отсутствии или недостатке естественного. По назначению бывает - рабочим, аварийным, эвакуационным, охранным, дежурным. Устраивать одно местное освещение нельзя. При недостаточности естественного освещения используется совмещенное (комбинированное) освещение - при котором в светлое время суток используется одновременно естественный и искусственный свет.

Значение освещенности на поверхности рабочего стола в зоне размещения документов составляет 300-500лк. В качестве источников искусственного освещения в помещении применяются люминесцентные лампы типа ЛБ.

Показатели микроклимата в офисных помещениях соответствуют установленным санитарно-гигиеническим требованиям ДСН 3.3.6-042-99 «Санитарные нормы микроклимата производственных помещений», ГОСТ 12.1.005-88 (1991) «ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны» и ГН 2152-80 «Санитарно-гигиенические нормы допустимых уровней ионизации воздуха производственных и общественных помещений».

Работа программиста в помещении относится к категории Ib - легкая работа, поэтому установлены следующие оптимальные значения параметров микроклимата:

в холодный период года:

- температура - 21-23С;
- относительная влажность - 40-60%;
- скорость перемещения воздуха - 0,1 м / с;

в теплый период года:

- температура - 22-24С;
- относительная влажность - 40-60%;
- скорость перемещения воздуха - 0,2 м / с.

На любом предприятии, независимо от масштаба производства, должны быть предусмотрены административные и бытовые помещения:

- санитарно-бытовые (гардеробные, душевые, туалеты, места для курения, помещения для обогрева);
- здравоохранения (медпункты, помещения для отдыха в рабочее время и психологической разгрузки);
- общественного питания (буфеты, комнаты принятия пищи);
- культурного обслуживания (помещения для собраний, учреждения культуры, спортивные сооружения);
- административные (помещения управления, общественных организаций, охраны труда, конструкторских бюро).

Требования по составу, размещению, размеров и оборудование административных и бытовых помещений изложены в ДБН В.2.2-28: 2010 "Здания и сооружения. Дома административного и бытового назначения".

Расчет необходимого количества санитарно-бытовых помещений и специальных бытовых приборов (кранов, душевых, сеток) для работников офиса проводится в соответствии с количеством работающих в наиболее многочисленной смене.

Стены и перегородки помещений душевых, пред-душевых, уборных, курительных помещений необходимо выполнять высотой 2 м от пола в светлых тонах из материалов, допускающих их легкую чистку и мытьё водой с применением моющих средств.

Пол санитарно-бытовых помещений должны быть влагостойкими и в то же время иметь нескользкую поверхность. Особенно это важно для душевых, пред-душевых, умывальных и гардеробных помещений.

Проектировать душевые, пред-душевые, умывальные, туалеты, гардеробные необходимо отдельно для мужчин и женщин.

Методика и алгоритм расчета площадей административных и хозяйственных помещений: группы рабочих процессов: 1а, 1б.

$$N_{\text{человек}} = 120; N_{\text{комп}} = 35; N_p = 75; N_{\text{ин}} = 30; N_{\text{упр.}} = 15; k_m : k_{\text{ж}} \Rightarrow 0.7 : 0.3.$$

1.1 : Для расчета ожидаемого количества мужчин и женщин на предприятии воспользуемся формулами 5.1 и 5.2:

$$N_M = k_M \cdot N \quad (5.1)$$

$$N_{\text{ж}} = k_{\text{ж}} \cdot N \quad (5.2)$$

Расчет ожидаемого количества мужчин и женщин на предприятии проводится согласно формулам 5.1 и 5.2:

$$N_M = 0.7 \cdot 120 = 84 \text{ человек};$$

$$N_{\text{ж}} = 0.3 \cdot 120 = 36 \text{ человек.}$$

1.2: Для расчета ожидаемого максимального количества программистов в смене воспользуемся формулами 5.3 и 5.4:

$$N_{\text{МП}} = k_M \cdot N \quad (5.3)$$

$$N_{\text{жП}} = k_{\text{ж}} \cdot N \quad (5.4)$$

Расчет ожидаемого максимального количества программистов в смене проводится согласно формулам 5.3 и 5.4:

$$N_{\text{МП}} = 0.7 \cdot 75 = 53 \text{ человек};$$

$$N_{\text{жП}} = 0.3 \cdot 75 = 22 \text{ человек.}$$

1.3 : Для расчета ожидаемого среднего количества программистов в смене воспользуемся формулами 5.5 и 5.6:

$$N^{\text{ЗММ}} = k_M \cdot N \quad (5.5)$$

$$N^{\text{ЗМЖ}} = k_{\text{ж}} \cdot N \quad (5.6)$$

Расчет ожидаемого среднего количества программистов в смене проводится согласно формулам 5.5 и 5.6:

$$N^{3MM} = 0.85 \cdot 53 = 45 \text{ человек};$$

$$N^{3MJ} = 0.85 \cdot 22 = 19 \text{ человек}.$$

1.4: Для расчета площади гардеробных помещений воспользуемся формулами 5.7 и 5.8:

$$S_{\text{ч}} = 0.9 \cdot N_{\text{м}} \quad (5.7)$$

$$S_{\text{ж}} = 0.9 \cdot N_{\text{ж}} \quad (5.8)$$

Расчет площади гардеробных помещений проводится согласно формулам 5.7 и 5.8:

$$S_{\text{ч}} = 0.9 \cdot 84 = 77.4 \text{ м}^2;$$

$$S_{\text{ж}} = 0.9 \cdot 36 = 32.4 \text{ м}^2;$$

1.5: Для расчета количества душевых на предприятии воспользуемся формулами 5.9 и 5.10:

$$n_{\text{Дм}} = N^{3MM} / 7 \quad (5.9)$$

$$n_{\text{Дж}} = N^{3MJ} / 7 \quad (5.10)$$

Расчет количества душевых на предприятии проводится согласно формулам 5.9 и 5.10:

$$n_{\text{Дм}} = 45 / 7 = 3 \text{ шт};$$

$$n_{\text{Дж}} = 19 / 7 = 3 \text{ шт}.$$

1.6: Для расчета количества умывальников на предприятии воспользуемся формулами 5.11 и 5.12:

$$n_{УМ} = N^{зММ} / 7 \quad (5.11)$$

$$n_{УЖ} = N^{зМЖ} / 7 \quad (5.12)$$

Расчет количества умывальников на предприятии проводится согласно формулам 5.11 и 5.12:

$$n_{УМ} = 45 / 7 = 3 \text{ шт.};$$

$$n_{УЖ} = 19 / 7 = 3 \text{ шт.}$$

1.7: Для расчета количества туалетов на предприятии воспользуемся формулами 5.13 и 5.14:

$$n_{ТМ} = N_{МП} / 15 \quad (5.13)$$

$$n_{ТЖ} = N_{ЖП} / 15 \quad (5.14)$$

Расчет количества туалетов на предприятии проводится согласно формулам 5.13 и 5.14:

$$n_{ТМ} = 53 / 15 = 4 \text{ шт.};$$

$$n_{ТЖ} = 22 / 15 = 2 \text{ шт.}$$

1.8: Для расчета площади для курения воспользуемся формулой 5.15:

$$S = 0.03 \cdot N_{МП} + 0.01 \cdot N_{ЖП} \quad (5.15)$$

$$S = 1.59 + 0.22 = 1.81 \text{ м}^2 \Rightarrow 2 \text{ м}^2.$$

1.9: Для расчета площади отдыха воспользуемся формулой 5.16:

$$S = 0.2 \cdot 64 = 13\text{м}^2 \quad (5.16)$$

Расчет площади отдыха производится согласно формуле 5.16:

$$S = 0.2 \cdot 64 = 13\text{м}^2.$$

Уровни звукового давления, уровни звука и эквивалентные уровни звука на рабочих местах в помещении нормируются согласно СанПиН 3.3.2.007-98 «Государственные санитарные правила и нормы работы с визуальными дисплейными терминалами электронно-вычислительных машин» и ДСН 3.3.6.037-99 «Санитарные нормы производственного шума, ультразвука и инфразвука». Снижение уровня шума в помещении осуществлено с помощью:

- использование более современного оборудования;
- расположение принтеров и различного оборудования коллективного пользования на значительном расстоянии от большинства рабочих мест работников;
- перевод жесткого диска в режим сна, если компьютер не работает в течение определенного времени;
- использование блоков питания ПК с вентиляторами на резиновых подвесках.

5.4 Мероприятия по пожарной безопасности

Закон Украины «О пожарной безопасности» определяет общие правовые, экономические и социальные основы обеспечения пожарной безопасности на территории Украины, регулирует отношения

государственных органов, юридических и физических лиц в этой области независимо от вида их деятельности и форм собственности.

Пожарная безопасность - состояние объекта, при котором с регламентируемой вероятностью исключается возможность возникновения и развития пожара и воздействия на людей его опасных факторов, а также обеспечивается защита материальных ценностей.

Для обеспечения пожарной безопасности в учреждениях проводят пожарную профилактику, которая включает в себя комплекс организационных и технических мероприятий, направленных на обеспечение безопасности людей, на предотвращение пожара, ограничения его распространения, а также на создание условий для успешного тушения пожара.

Для ликвидации пожара в начальной стадии его развития силами персонала объектов применяются первичные средства пожаротушения: огнетушители, пожарный, системы автоматического пожаротушения.

Первичные средства пожаротушения, в зависимости от категории помещений, могут располагаться как отдельно, так и в составе пожарных щитов.

В зависимости от агрегатного состояния и особенностей горения различных горючих веществ и материалов пожара по ГОСТ В.1.1.7-2002 «Пожарная безопасность объектов строительства» делятся на соответствующие классы.

В офисном помещении находится деревянная мебель, электронная аппаратура, бумажные носители информации. Класс пожара в офисном помещении (согласно с ДБН В.1.1.7-2002 «Защита от пожара. Пожарная безопасность») - пожара твердых веществ, горение которых сопровождается тлением (древесина, бумага, пластмасса) - определяется как класс А.

Определение типа и расчет количества первичных средств пожаротушения по ДБН В.1.1.7-2002 «Защита от пожара. Пожарная безопасность объектов строительства» - для офисного помещения категории пожара-опасности А и применяется 4 порошковых огнетушителя типа ОП 5, а

также 2 углеродных огнетушителя ОУ-7 (ВВК-5) (НАПБ Б.03.002-2007 «Нормы определения категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности», ДБН В.1.1.7-2002 «Пожарная безопасность объектов строительства»).

Согласно ДБН В.2.5-56: 2014 «Системы противопожарной защиты» в помещении установлены комбинированные оптико-тепловые датчики СПД-3.5. В случае срабатывания сигнала тревоги подается на ППКП и передается на звуковые и световые извещатели здания.

Согласно ДБН В.1.1-7-2002. «Пожарная безопасность объектов строительства» на случай пожара предусмотрены пути эвакуации работающих - проходы, проезды, эвакуационные выходы. Два эвакуационных выхода расположены рассредоточено. Коридоры и проходы, предназначенные для эвакуации, должны иметь как можно меньшую длину и минимальное количество поворотов. На всем протяжении прохода нет порогов или промежуточных ступеней. Согласно п. 13 «Рекомендаций по составлению планов эвакуации людей в случае пожара» план эвакуации размером формата А4 размещен на видном месте под стеклом.

Согласно НАПБ Б.02.005-2003 «Типовое положение об инструктажах, специальном обучении и проверке знаний по вопросам пожарной безопасности на предприятиях, в учреждениях и организациях Украины» работники прошли инструктаж по пожарной безопасности и ознакомлены с эвакуационными мероприятиями при пожаре.

5.5 Меры безопасности в чрезвычайных ситуациях

Вследствие чрезвычайных ситуаций в населенных пунктах страны и на предприятиях могут возникнуть разрушения, заражение местности радиоактивными и химическими веществами. Люди могут в завалах, в поврежденных и горящих домах, других непредвиденных ситуациях. В связи

с этими обстоятельствами потребуются проведение мероприятий по спасению людей, оказанию им помощи, локализации аварий и устранения повреждений.

При решении этих проблем исходят из того, что в очагах поражения и районах бедствия будут проводиться не только сугубо спасательные работы, но и некоторые неотложные, не связанных со спасением людей.

Спасательные и другие неотложные работы (СИНР) проводятся с целью спасения людей и оказания помощи пораженным, локализации аварий и устранения повреждений, создания условий для последующего проведения восстановительных работ. При проведении СИНР большое значение имеет соблюдение определенных условий:

- своевременное создание группировок, сил для проведения СИНР;
- своевременное ведение разведки, быстрое движение и ввода сил в очаг поражения, непрерывное проведение СИНР до их полного завершения;
- твердое и оперативное управление силами, привлекаемых к проведению СИНР, и всестороннее обеспечение их деятельности.

Мероприятия, относящиеся к спасательным работам:

- разведка маршрутов, по которым вводятся или выводятся формирования ГО;
- локализация и тушение пожаров;
- поиск и спасение людей из-под завалов;
- открытие разрушенных защитных сооружений и спасение людей;
- подача воздуха в заваленные защитные сооружения;
- предоставление пострадавшим первой медицинской помощи и их эвакуация;
- санобработка людей и обеззараживания их одежды;
- обеззараживания местности, сооружений, техники.

Кроме спасательных работ, в очагах поражения проводятся неотложные работы, к которым относятся:

- прокладка маршрутных путей на зараженных территориях и строительство проездов в завалах;

- локализация аварий на коммунально-энергетических сетях, линиях связи и их восстановления;
- закрепление или ликвидация конструкций сооружений, угрожающих падением и препятствуют проведению спасательных работ;
- ликвидация боеприпасов и других взрывоопасных предметов (баллоны с газом, бочки с бензином).

При авариях на объектах народного хозяйства, учреждениях, если их последствия не выходят за пределы объектов защитных зон, руководство работами проводится администрацией предприятий.

Возникновения стихийных бедствий, а также аварий и катастроф можно в некоторых случаях прогнозировать. Прогнозы закладываются в планы ГО предприятий, учреждений, предусматривающие предупредительные меры, которые должны уменьшить последствия аварий и катастроф. Характер и объем таких мероприятий зависят от вида и уровня аварии или стихийного бедствия, масштабов и времени их возникновения.

Всего таких мероприятий:

- приведение в готовность средств защиты;
- проверка готовности систем оповещения;
- подготовка и выдача населению средств индивидуальной защиты и личной профилактики;
- проведение санитарно-эпидемиологических мероприятий;
- подготовка к эвакуации или отселения и их проведения;
- вывоз материальных ценностей;
- защита продуктов питания и источников воды;
- герметизация помещений.

Способы и последовательность проведения этих работ зависят от обстоятельств, сложившихся в районе аварии или катастрофы, и наличия сил и средств для проведения таких работ.

Ликвидация последствий чрезвычайной ситуации проводится для восстановления работы предприятий, организаций, учебных заведений.

ВЫВОДЫ

В ходе проведения исследований в области каналов передачи информации стояли задачи по нахождению новых способов совершенствования защиты.

Были разработаны и предложены методы защиты, среди которых представлен собственный фильтр для проверки вводимых данных пользователями, механизм проверки активности пользователя и его пользования веб-приложением, а также способы защиты пароля и программного кода.

В первой главе были вынесены на рассмотрение вопросы касательно безопасности веб-приложений и онлайн ресурса, как единой информационной системы.

Прежде всего была рассмотрена актуальность темы исследования и принципы, на которых базируется политика информационной безопасности веб-приложения.

Для четкого понимания и определения направления дальнейшего развития исследования, в первую очередь было проведено изучение угроз информационной безопасности веб-приложения. В ходе работы так же были определены мотивы, руководствуясь которыми и совершается большинство атак на веб-ресурсы.

Для дальнейшего успешного развития работы была составлена классификация уязвимостей и атак, которым подвергаются защищаемые веб - приложения. Соответственно для того, чтобы предпринимать дальнейшие действия по улучшению качества защиты, были определены направления и основные идеи защиты веб-приложения.

Во второй главе было принято решение по использованию протокола WebSocket в качестве основного механизма защиты каналов передачи информации.

В ходе проведения работы прежде всего был проведен сравнительный анализ предложенного решения с хорошо известным протоколом HTTP. Положительные результаты сравнения в пользу протокола WebSocket подтвердили правильность выбранного решения.

Для успешного формирования механизма защиты, обеспечивающего высокий уровень безопасности передаваемой информации, был изучен сам протокол WebSocket. Но, как и любая технология, протокол не совершенен, имеет свои недостатки.

Для дальнейшего успешного развития работы была выявлена причина возникновения данных недостатков, а также были рассмотрены угрозы и сценарии атак, возникающие в следствии успешного использования недостатков протокола.

В третьей главе была проведена работа над улучшением и устранением уязвимостей протокола WebSocket с целью дальнейшего повышения уровня безопасности передаваемой информации по каналам связи.

Для успешного противостояния XSS уязвимости прежде всего были применены меры по соблюдению и выполнению требований в организации работы веб-приложения со стороны обсуживающего персонала.

В качестве решения проблем безопасности был разработан собственный, универсальный фильтр с возможностью дальнейшего внесения корректировок для проверки вводимых данных пользователем.

Так же в качестве дополнительной защиты от уязвимости был разработан механизм проверки активности пользователя и его активного нахождения на сайте.

На стороне сервера для защиты пользовательских данных, а именно паролей был реализован метод одностороннего шифрования для сохранения паролей пользователей в базе данных.

В качестве дополнительной меры защиты от постороннего вмешательства, исполняемый код веб-приложения был подвергнут обфускации. Данное решение послужило дополнительной мерой защиты кода

не только от внешнего вмешательства, но и от попыток изучить его структуру и логику работы, при этом сохраняя полную работоспособность веб-приложения.

В качестве результата работы был представлен наиболее эффективный альтернативный вариант передачи информации, а также предложены методы и рекомендации по повышению уровня безопасности в исследуемой области, направленные на совершенствование защиты действующих каналов передачи информации, что позволит в дальнейшем совершенствовать и расширять методику передачи данных. Также разработана и внедрена реализация системы защиты на примере службы мгновенных сообщений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. ДСТУ 3396.0-96 Государственный стандарт Украины. «Защита информации. Техническая защита информации».
2. Безопасность сайта. Проблема и решение. [Электронный ресурс] – Режим доступа: <https://bit.ly/2DQl6NR>
3. Метод оценки защищенности web-сайта. Анализ методов продвижения и мониторинга посещаемости и улучшение защищенности сайта. [Электронный ресурс] – Режим доступа: <https://bit.ly/2zmjDej>
4. Научная электронная библиотека “eLibrary”. Журнал: «Защита информации» Издательский дом «Афина» №5 – 83, 2018. [Электронный ресурс] – Режим доступа: <https://bit.ly/2DAIJdr>
5. «Веб-разработка с применением Node и Express. Итан Браун» ООО «Питер пресс», 192102, Санкт-Петербург, ул. Андреевская, 3. Тираж 1200, 2017
6. «Metanit.com». Сайт о программировании. Руководство JavaScript. [Электронный ресурс] – Режим доступа: <https://bit.ly/2zlSeZX>
7. Основные угрозы информационной безопасности сайта. Блог компании «Pentestit» [Электронный ресурс] – Режим доступа: <https://bit.ly/2BsXWPX>
8. Современный учебник JavaScript. [Электронный ресурс] – Режим доступа: <https://bit.ly/1ZICdAN>
9. Статья: «Технологии обеспечения безопасности информации при передаче в сети Интернет». И. В. Рыбаков, 2011. [Электронный ресурс] – Режим доступа: <https://bit.ly/2AddwZo>
10. Основные положения стеганографии. Журнал "Защита информации. Конфидент", №3, 2000. [Электронный ресурс] – Режим доступа: <https://bit.ly/2DPoNTK>
11. 9 советов по улучшения состояния защищенности сайта. [Электронный ресурс] – Режим доступа: <https://bit.ly/2EM7AHJ>

12. Статья: «Методы защиты сайта от спама». [Электронный ресурс] – Режим доступа: <https://bit.ly/2DSBkWA>
13. Ресурсы для разработчиков от разработчиков. MDN Web Docs. [Электронный ресурс] – Режим доступа: <https://mzl.la/2FOkaLN>
14. Защита сайта примитивными методами. Лаборатория защиты [Электронный ресурс] – Режим доступа: <https://bit.ly/2Acqpmr>
15. Всемирное исследование мошенничества. PWC, Ukraine – 2018. [Электронный ресурс] – Режим доступа: <https://pwc.to/2SdHV19>
16. Публикация: «Защита пароля при передаче. Информационная безопасность». [Электронный ресурс] – Режим доступа: <https://bit.ly/2BqZQeR>
17. Методические указания для выполнения экономической части дипломных и магистерских проектов для студентов всех форм обучения. Составители: Бобровникова Р.Г., Кругликова В.В. – Запорожье, ЗНТУ, 2012. – 18 с.
18. ГОСТ 12.1.009-76 (1999) «ССБТ. Электробезопасность. Термины и определения»
19. ГОСТ 12.1.030-81 (2001) «ССБТ. Электробезопасность. Защитное заземление, зануление»
20. НПАОП 40.1-1.32-01 «Правила устройства электроустановок. Электрооборудование специальных установок»
21. ГОСТ 12.1.005-88 (1991) «ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны»