ъавтономное профессиональное образовательное учреждение Вологодской области

«Вологодский колледж связи и информационных технологий»

# СОГЛАСОВАНО:

Заместитель директора по методическому сопровождению и инновационной деятельности

С.В. Потылицына

« » 2022г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

**ПРОВЕРКА ЗАЩИЩЕННОСТИ WEB РЕСУРСА**

Группа: СС-418А, специальность 11.02.11 «Сети связи и системы коммутации»

|  |  |  |
| --- | --- | --- |
| Студент | *подпись* | \_ Д.И. Панов  *И.О.Фамилия* |
| 20 |  |  |
| Руководитель работы | *подпись* | \_ П.Е. Трошкин  *И.О.Фамилия* |
| 20 |  |  |
| Консультант по экономической части \_ С.Г.Оковитая | | |
|  | *подпись* | *И.О.Фамилия* |
| 20 |  |  |
| Нормоконтролер | *подпись* | \_ С.В.Потылицына  *И.О.Фамилия* |
| 20 |  |  |
| Рецензент | *подпись* | *И.О.Фамилия* |
| 20 |  |  |

Вологда, 2022 г.

# СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_bookmark0)  
РАЗДЕЛ1.WEB-РЕСУРС 5  
Понятие веб-ресурса...................................................................................................................... 5  
Структура веб-сайта 6  
Виды угроз для веб-ресурсов 8  
Способы защиты веб-ресурса   
РАЗДЕЛ2. ПРОВЕРКА ЗАЩИЩЕННОСТИ WEB-РЕСУРСА 6 Разработка структуры сайта 6  
Проектирование web – сайта 6  
Проверка на безопасность web-сайта 6  
РАЗДЕЛ3. ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РАБОТЫ 7  
Подсчет расходов на содержание веб-сайта 7  
ЗАКЛЮЧЕНИЕ 8  
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 9  
ПРИЛОЖЕНИЕ 10

# ВВЕДЕНИЕ

Веб-ресурс, или веб-сайт — это страница или несколько страниц, размещенных в сети Интернет. Такие страницы могут включать текстовую, графическую информацию или мультимедиа-компоненты.  
Страницы веб-ресурса могут быть как статическими, так и динамическими. У каждого веб-сайта есть [доменное имя](https://mosseo.team/uslugi/ehffektivnoe-prodvizhenie-i-tehnicheskaya-podderzhka-sajta/podrobnyj-seo-analiz-sajta/podrobnyj-seo-analiz-domena-sajta/), которое определяет его уникальный адрес

Необходимость проверки защищенности web ресурсов, это одна из основополагающих в нашем цифровом мире, которая предполагает собой защиту и способ нахождения уязвимостей от различного рода взломов Web-приложений и Web-сайтов.

# На современном этапе существует множество проверенных веб-ресурсов, которые не отвечают современным типам к безопасности. У них имеются слабые места, проще говоря уязвимости. Злоумышленники могут использовать их в своих целях, например, для кражи информации о пользователе.

# Безопасность web-ресурсов является основополагающей в нашем современном и цифровом мире. Базируясь на принципах конфиденциальности, доступности и целостности, оценка защищенности веб-ресурсов, способствует обеспечению сохранности данных, учетных записей, доступов и подключений пользователей.

Способов для обнаружения слабых мест существует большое количество, в моем дипломном проекте я расскажу о самых популярных из них, как они работают, а также какими способами можно защитить свой web-ресурс от несанкционированного взлома и как не допустить доступ информации третьим лицам.

Данная тема является актуальной, так как web-ресурсов с каждым днем становится все больше. Уровень защищенности веб-приложений продолжает постепенно расти, но все еще остается довольно низким. Не все из них соответствуют критериями безопасности. Методы и способы взлома веб-ресурсов, описанные в дипломной работе, помогут обезопасить web-ресурс

Объектом данной выпускной квалификационной работы является проверка безопасности и защищенности Web-ресурсов.

Предметом исследования выпускной квалификационной работы является нахождение уязвимости Web-ресурса.

Целью выпускной квалификационной работы является проверка и определение безопасности Web-ресурса

Для достижения поставленной цели были определены следующие задачи:

1. Описать технические характеристики web-ресурсов.
2. Основные методы тестирование на проникновение
3. Тестирование безопасности веб ресурсов
4. Анализ исходного интернет ресурса
5. Выявление уязвимостей
6. Расчет экономической эффективности защищенности web-ресурса

Методами исследования дипломной работы являются:

- Изучение структуры веб-сайтов,

- Изучение способов взлома Web-ресурсов,

- Конструирование веб-сайта,

- Рассмотрение способов защиты и взлома созданного веб-сайта

- обобщение полученной информации, формулирование выводов.

Теоретическая значимость данной дипломной работы заключается в обогащении научного раздела «Вычислительная техника».

Практическая значимость дипломной работы состоит в том, что методы взлома и защиты, представленные в работе, позволят людям оценить и понять защищенность своего web-ресурса.

Выпускная квалификационная работа состоит из введения, трёх разделов, заключения, списка использованных источников

**РАЗДЕЛ 1.WEB-РЕСУРС**

* 1. **Понятие веб-ресурса**

Интернет-ресурс– это совокупность интегрированных средств технического и программно-аппаратного характера, а также информации, предназначенной для публикации во Всемирной паутине. Интернет-ресурс может содержать информацию в текстовой, графической и мультимедийной форме. Каждый интернет-ресурс должен иметь уникальный адрес, который позволяет найти его в Сети.

К ресурсам также принято относить не только физические компоненты (элементы памяти и т.п.), но и виртуальные, например, файлы. Именно к виртуальной части ресурсов восходит идея веб- (интернет) ресурсов. В эпоху молодого Интернета в сети искали документы, а точнее файлы, которые имели специальный адрес. Вскоре под ресурсом в Интернете стали также понимать и связанную в сеть все информационную систему (например, электронные библиотеки и т.п.).

При использовании терминов в Интернете термин «ресурс» получил схожие характеристики (идентификацию и обозначения, адресацию и техническую обработку). Однако была и определенная специфика, которая вызвала длительные дискуссии среди специалистов. Самым известным сюжетом этой дискуссии был спор о классификации интернет-ресурсов. Однако в действительности, поводов для споров было больше. Помимо технических вопросов специалисты обсуждали социальные, языковые и даже философские аспекты.

Дальнейшее развитие Интернета привело не только к увеличению количества веб-сайтов, но и к разнообразию их функций и назначения. Вопросы о применении термина «интернет-ресурс» остались, но в обиходе он используется крайне редко.

Существуют определенные различия веб-ресурсов по видам:

по доступности сервисов:

1 открытые – когда каждому без исключения пользователю сети Интернет доступны все сервисы

1. полуоткрытые – когда необходимо пройти регистрацию, как правило, бесплатно
2. закрытые – частные и личные сайты, созданные для организаций и компний, куда ппасть можно только обладая специальным приглашением.
3. по физическому расположению:
4. общедоступные - открыты всем пользователям
5. локальные – открыты только в зоне доступа локальной сети (специальной компьютерной сети на достаточно небольшой территории).
6. по схеме представления информации:
7. информационные ресурсы – включают в себя тематические сайты (с узко направленной тематикой) и тематические порталы (обычно достаточно большие веб-ресурсы с исчерпывающей информацией, а также возможностью пользователям общаться в рамках ресурса).
8. интернет-представительства – как правило, сайты тех, кто владеет бизнесом. Существуют разные подвиды таких сайтов: сайт-визитка, промо-сайт, интернет-магазин и др.
9. веб-сервисы – также включают в себя различные подвиды (блоговый, видеохостинг, поисковые сервисы и др.) и созданы для выполнения определенного ряда задач в сети Интернет.
   1. **Структура веб-сайта**

Создание структуры сайта, как строительство фундамента — без него дом поставить можно, но насколько он будет надежным, большой вопрос. Сайт без продуманной структуры тоже будет худо-бедно работать, но о его эффективности можно забыть. Пользователи и роботы не понимают, куда им идти, страницы плохо индексируются, поведенческие факторы падают из-за большого процента отказов, поисковики не пускают ресурс в топ.

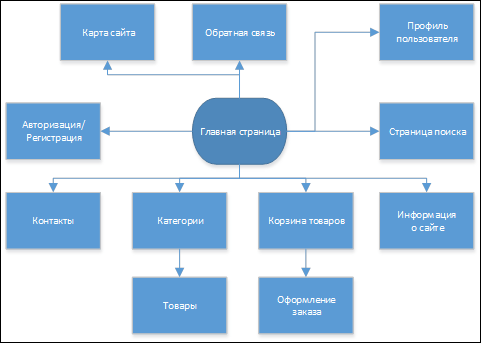


Рисунок 1. Пример разработки структуры сайта

Структура — это логика построения сайта, иерархическая организация взаимосвязей страниц. Ее проще всего представлять графически — в виде блок-схемы или майнд-карты, где наглядно видна иерархия, уровни вложенности страниц и их связи.

Технически структура отражена в URL. У каждой страницы есть уникальный адрес, в котором прописан путь к ней с главной. Вложенность в URL обозначается слэшами (/).

При грамотной структуре ни одна страница ресурса не подвешена в воздухе, и ко всем, даже самым отдаленным закоулкам можно перейти хотя бы в три клика. Пользователь должен с ходу разобраться, как тут у вас все устроено, где он находится сейчас и куда отсюда можно перейти. Без структуры сайт становится запутанным лабиринтом. Пользователь быстро найдет из него выход, нажав на крестик на вкладке в своем браузере, а поисковый краулер будет блуждать и тормозить индексацию.

Говоря о разработке модели сайта, нужно понимать различия между внешней и внутренней структурой.

Внешняя — это композиция страницы, организация элементов на экране, графический макет.

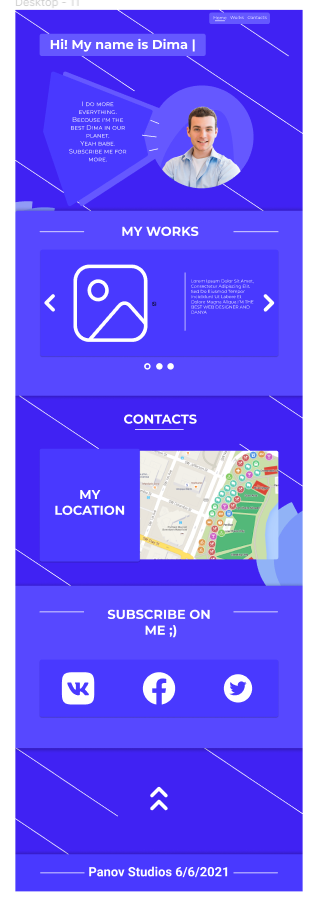
Внутренняя — это организация страниц внутри сайта: принадлежность к категориям или разделам, иерархия, схема переходов.

Рисунок 2. Готовая внешняя структура сайта.

Представим, что сайт — это здание театра. Здесь есть своя система организации пространства: гардероб, холл, проходы в партер и ложи, буфет и туалеты. Планировка здания — это и есть внутренняя структура, чем она продуманней, тем комфортнее зрителям во время визита в театр.

В идеале внешняя и внутренняя организация пространства вместе работают на комфорт посетителя и формируют положительный пользовательский опыт.

* 1. **Виды угроз для веб-ресурсов**

На сегодняшний день Web-портал компании, доступный в сети Интернет 24 часа 7 дней в неделю, может выступать в качестве одного из первых объектов, с которого злоумышленники начинают вторжение в корпоративную сеть, поэтому именно здесь должен быть расположен и первый бастион для защиты от возможных атак. Рассмотрим основные типы угроз безопасности Web-порталов, а также те инструменты, которые позволяют значительно снизить вероятность успешной атаки.

## DDOS-атаки

Очень часто Web-портал является инструментом для ведения бизнеса, остановка которого может привести к недополученной прибыли и прямым финансовым потерям. Это особенно характерно для банков, предприятий интернет-торговли, платежных систем и др. Хакеры знают о важности Web-порталов для коммерческих и государственных организаций и регулярно проводят взломы с помощью распределенных DDoS-атак, целью которых является нарушение работоспособности портала. Такие атаки могут осуществлять как вымогатели, которые требуют заплатить за прекращение атаки, так и конкуренты, пытающиеся затормозить развитие бизнеса компании. Как правило, современные DDoS-атаки организуются с помощью сети зараженных вредоносной программой компьютеров – бот-сети, ресурсы которой используются для нападения на портал. Цель атаки – исчерпать ресурсы входного канала связи, по которому подключен Web-портал, чтобы легитимные пользователи не могли получить доступ к соответствующим информационным ресурсам. Необходимо отметить, что DDoS-атаки часто используются для отвлечения внимания от основной атаки, которая осуществляется на компанию.

Защититься от такого нападения можно с помощью фильтрации постороннего трафика, который используется злоумышленниками для загрузки каналов связи. Для этого на рынке информационной безопасности представлены специализированные продукты, которые устанавливаются на стороне заказчика и выполняют функции фильтрации трафика. Примерами таких решений являются продукты компаний Arbor Networks, Radware и "МФИ Софт". Некоторый функционал защиты от DDoS также есть в решениях класса WAF (Web-Application Firewall). Кроме этого, существует возможность воспользоваться сервисами по фильтрации трафика, которые предполагают перенаправление входящего трафика на площадку компании, которая займется очисткой трафика, после чего он уже передается заказчику. Подобные услуги предлагают компании Qrator, "Лаборатория Касперского" и наиболее крупные операторы связи.

## Атаки на web-приложения

Web-приложения традиционно базируются на одном из сценарных языков: PHP, Python, Ruby и других, которые являются интерпретируемыми. У злоумышленника есть возможность с помощью специальных символов встроить свой код в запрос к серверу (например, в поисковой строке или в любой другой строке, которая подразумевает ввод данных пользователем) и заставить интерпретатор выполнить посторонний сценарий. Такой метод атаки называется "инъекция" (например, PHP-инъекция, если встраиваются команды для интерпретатора PHP). Поскольку большинство Web-порталов базируется на СУБД с поддержкой интерпретируемого языка SQL, то и команды этого языка также можно навязать к исполнению. Такую атаку называют SQL-инъекцией – она позволяет манипулировать данными в базе, например, связанными с аутентификацией пользователей.

Защититься от большинства видов атак на Web-приложения можно с помощью фильтрации входного потока данных, т.е. HTTP-запросов пользователей и его профилировании (система сперва обучается и далее начинает понимать, какие типы данных ожидать на вход, а также их длину и другие параметры). Для этого, например, можно использовать так называемые экраны Web-приложений WAF. В частности, решения подобного класса предлагают компании Positive Technologies, Imperva, F5 и др. Кроме этого, исходный код Web-приложения при его добавлении на Web-сервер целесообразно проверять специальным сканером кода, который позволяет обнаружить наиболее часто встречающиеся ошибки, допущенные на этапе разработки приложения, и выдать рекомендации по их устранению. Такие сканеры могут быть как бесплатными, так и коммерческими – в качестве примера можно привести сканеры MicroFocus Fortify, Infowatch ApperCut и Solar InCode.

## Атаки на по web-портала

Web-приложение в некоторых случаях позволяет обратиться напрямую к операционной системе, на которой работает Web сервер, и выполнить команды от его имени. Для этого используются более сложные атаки на переполнение буфера или другие манипуляции с памятью серверов. Так могут быть атакованы и база данных, и ПО Web-сервера, и любая другая компонента многоуровневого Web-портала.

В качестве средств защиты от таких атак, помимо вышеперечисленных решений, рекомендуется использовать сетевой сканер безопасности, который тестирует все Web-приложение целиком на наличие известных уязвимостей во всех компонентах. Такие сканеры можно использовать либо для аудита текущей конфигурации Web-портала с помощью анализа конфигурационных файлов, либо для имитации внешних сетевых атак и выявления таким образом имеющихся уязвимостей. В качестве примера сетевых сканеров можно привести решения Maxpatrol, Qualys и Nessus.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Безопасность веб-приложений Django [Электронный ресурс]. – Режим доступа: <https://developer.mozilla.org/ru/docs/Learn/Server-side/Django/web_application_security>
2. Буйначев С.К. Основы программирования на языке Python : учебное пособие / Буйначев С.К., Боклаг Н.Ю.. — Екатеринбург : Уральский федеральный университет, ЭБС АСВ, 2014. — 92 c. — ISBN 978-5-7996-1198-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/66183.html (дата обращения: 09.06.2021). — Режим доступа: для авторизир. Пользователей
3. Защита WEB приложений [Электронный ресурс]. – Режим доступа: https://www.infosec.ru/uslugi/zashchita-web-prilozheniy/
4. Кириченко А.А. Разработка электронного портала. Создание Web-представительства. Контент-инжениринг : учебное пособие / Кириченко А.А.. — Москва : Евразийский открытый институт, Московский государственный университет экономики, статистики и информатики, 2005. — 106 c. — ISBN 5-7764-0537-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/10809.html (дата обращения: 09.06.2021). — Режим доступа: для авторизир. Пользователей
5. Основные угрозы безопасности сайта [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/post/279787/>
6. Структура веб-сайта [Электронный ресурс]. – Режим доступа: <https://developer.mozilla.org/ru/docs/Learn/HTML/Introduction_to_HTML/Document_and_website_structure>
7. Сычев А.В. Web-технологии : учебное пособие / Сычев А.В.. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 407 c. — ISBN 978-5-4497-0292-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/89412.html (дата обращения: 09.06.2021). — Режим доступа: для авторизир. Пользователей
8. Уязвимости веб-приложений [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/company/pentestit/blog/526878>
9. Уязвимости веб-сайтов [Электронный ресурс]. – Режим доступа: <https://www.anti-malware.ru/threats/site-vulnerability>
10. Что такое веб ресурс-электронный ресурс [Электронный ресурс]. – Режим доступа: <https://php.zone/post/veb-resurs-chto-eto-takoe>