

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Факультет физико-технический
Кафедра радиофизики и инфокоммуникационных технологий



УТВЕРЖДАЮ
проректор

П.А. Машаров
«29» марта 2024 г.

П.А. Машаров

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«WEB-ПРОГРАММИРОВАНИЕ»

Укрупненная группа направлений подготовки	10.00.00 Информационная безопасность
Программа высшего образования	Программа бакалавриат
Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Квалификация	Бакалавр
Форма обучения	очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «**Web-программирование**» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 (с изм. и доп.). Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:

Доцент
кафедры радиопизики
и инфокоммуникационных технологий

 М.В. Бабичева

Рабочая программа утверждена на заседании кафедры радиопизики и инфокоммуникационных технологий
Протокол от 26.03.2024 г. № 16

Заведующий кафедрой

 В.В. Данилов

СОГЛАСОВАНО:

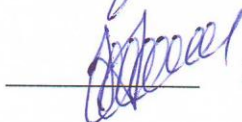
И.о. декана физико-технического факультета
28.03.2024 г.

 С.А. Фоменко

Учебно-методическая комиссия физико-технического факультета
Протокол от 27.03.2024 г. № 2
Председатель

 В. Н. Котенко

Руководитель основной профессиональной
образовательной программы
д-р тех. наук, проф.
26.03.2024 г.

 В.В. Данилов

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

Информатика, Информационные технологии, Языки программирования, Теория информации, Пакеты прикладных программ для обработки изображений, Модели и методы безопасного информационного обмена.

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Скриптовые языки программирования, Введение в искусственный интеллект, Модели и методы безопасного информационного обмена, Анализ безопасности web-проектов, Программно-аппаратные средства защиты информации.

Используются при написании выпускной квалификационной работы, Производственная практика: научно-исследовательская работа (обязательная). Производственная практика: преддипломная практика (обязательная).

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1.Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.03.01 Информационная безопасность (Программа бакалавриата Информационная безопасность)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.1.1 Web-программирование
Часть образовательной программы	Вариативная часть (дисциплины по выбору)
Количество зачетных единиц / всего часов	3 / 108

2.2.Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная, всего	3	5	34	34	-	40	108	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ

Овладение технологиями проектирования web-сайта как информационной системы, поддержки и сопровождения web-сайта на сервере, анализ уязвимостей, которые могут быть созданы при некорректной разработке сайта.

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1.Компетенции

Компетенции	Индикаторы	Результаты обучения
ПК-3 Способен осуществлять администрирование	ПК-3.2 Знает уязвимости и средства	Умеет выбирать, квалифицированно применять средства обеспечения информационной безопасности и

средств защиты информации прикладного и системного программного обеспечения. (06.032)	защиты web-приложений	целостности данных в соответствии с решаемыми прикладными задачами и создаваемых программных систем Умеет применять информационные технологии обработки, хранения и передачи данных, методы и средства управления проектами
---	-----------------------	--

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. DNS - система доменных имен.	1. Идея международной системы доменных имен. 2. NS – сервера. 3. Уязвимости протокола DNS. Атака отравление кеша. 4. Типы DNS записей. 5. Обработка DNS запросов. 6. Утилиты для формирования DNS запросов. 7. Понятие DNS зоны. Зон-трансфер.
2. HTTP - запросы.	1. История протокола HTTP. Достоинства и недостатки HTTP. 2. Структура HTTP запроса и ответа. 3. Методы анализа HTTP запросов. 4. Методы передачи HTTP запросов. 5. HTTP заголовки. 6. Утилиты для создания HTTP запросов. Перехват HTTP запросов.
3. Web - сервер.	1. Понятие web- сервера. Виды web- серверов. 2. Apache и Nginx, достоинства и недостатки. 3. Порты и сокеты. Создание простого TCP сервера. 4. Создание эхо-сервера. 5. Блокирующий ввод-вывод. Многопоточность. 6. Методы создания многопоточности. Создание HTTP сервера.
4. Структура клиент-серверного приложения.	1. Frontend и backend, общая архитектура. 2. Задачи frontend сервера. 3. Reverse proxy, настройка проксирования. 4. Application сервер и его задачи. 5. Протоколы запуска приложения. Переменные окружения. CGI, FastCGI и WCGI.
5. Основы PHP.	1. Серверные языки программирования. Open server. 2. Команда isset. Переменные и типы. 3. Динамическая типизация. 4. Ветвление, циклы, массивы, ассоциативные массивы. 5. Работа с файлами. 6. Суперглобальные переменные. Передача переменных HTML- PHP.
6. Формы и передача параметров.	1. Понятие формы. 2. Методы POST и GET для передачи параметров. 3. Глобальные переменные \$_POST, \$_GET и \$_REQUEST. 4. Уязвимости формы. Функции для обработки данных формы.

7. Работа с файлами.	1. Настройка php.ini. 2. Суперглобальный массив \$_FILES и его структура. 3. Загрузка одного и нескольких файлов. 4. Атаки на сайты, позволяющие загружать на них файлы. 5. Ограничение размера и типа файла. 6. Ограничение типа с учетом содержимого. Конфигурация .htaccess.
8. Сессии и куки.	1. Типы куки. Понятие сессии. 2. Открытие и закрытие сессии. Переменные сессии. 3. Суперглобальная переменная \$_SESSION. 4. Разница между куки и сессией. 5. Безопасность сессии. 6. Установка и удаление куки. Методы защиты куки.
9. Проверка корректности данных.	1. Ошибки, которые разработчики могут допускать при создании сайтов. 2. Хранение пароля в зашифрованном и зашифрованном виде. 3. Хранение секретных данных в текстовом файле. 4. Атака «Command Inclusion». 5. Проблемы безопасности, связанные с обработкой формы. Проблемы безопасности, связанные с сессиями. Подмена переменных сессии.
10. Базы данных.	1. Понятие базы данных. 2. Реляционные и нереляционные базы данных. 3. Поля и записи. 4. Популярные БД. 5. Настройка MySQL в OpenServer. 6. Интерфейс phpMyAdmin. 7. Приоритетный поиск. Предпросмотр. Подключение и выборка данных.
11. Запросы и их обработка.	1. Запросы. Язык SQL запросов. 2. Получение и удаление записей. 3. Запросы SELECT, UNION, GROUP. 4. Объединение данных при помощи атрибутов AND и OR. Получение всех записей таблицы.
12. Атаки на базы данных.	1. Понятие SQL инъекции. 2. Инъекция типа SELECT + ' . 3. Инъекция типа SELECT UNION. 4. Множественные запросы. 5. Экранирование ввода. Обход фильтрации символов. Инъекция типа -1 OR 1=1.
13. XSS -атаки.	1. Понятие XSS. Отраженные, хранимые, основанные на DOM XSS атаки. 2. Как определяют уязвимость к атаке. 3. Внедрение в HTML, URL и STYLE атрибуты. 4. Примеры эксплуатации XSS уязвимости. 5. Автоматизация тестирования приложений на уязвимость к XSS атакам при помощи Beef. Защита от XSS атак.

14. Методы аутентификации на сайтах.	1. Базовая аутентификация через http заголовки. 2. Digest аутентификация. 3. Сессионные JSON WEB Token. 4. PKI аутентификация. Сертификаты. 5. Создание сертификата при помощи Openssl. Подпись и хранение сертификатов.
15. Технология AJAX.	1. Асинхронный JS и XML. 2. Динамическое отображение и взаимодействие с пользователем. 3. Обмен и обработка данных. Утилита XMLHttpRequest.
16. Сканеры web-безопасности.	1. Сканеры web –безопасности и их возможности. 2. Acunetix – учебный сканер web-уязвимостей. 3. OWASP-ZAP и его возможности. On-line сервисы для проверки web-приложений на безопасность.
17. Размещение приложения на хостинге.	1. Платные и бесплатные хостинги, достоинства и недостатки. 2. Популярные бесплатные хостинги. 3. Регистрация. Загрузка сайта на хостинг. Отладка работы сайта.

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1.Форма обучения – очная, курс – 3, семестр – 5

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор	Практ.	СРС+К	Всего
DNS - система доменных имен.	2	2		4	8
HTTP - запросы.	2	2		4	8
Web - сервер.	2	2		4	8
Структура клиент-сервер-ного приложения.	2	2		2	6
Основы PHP.	2	2		2	6
Формы и передача параметров.	2	2		2	6
Работа с файлами.	2	2		2	6
Сессии и куки.	2	2		2	6
Проверка корректности данных.	2	2		2	6
Базы данных.	2	2		2	6
Запросы и их обработка.	2	2		2	6
Атаки на базы данных.	2	2		2	6
XSS -атаки.	2	2		2	6
Методы аутентификации на сайтах.	2	2		2	6
Технология AJAX.	2	2		2	6
Сканеры web-безопасности.	2	2		2	6
Размещение приложения на хостинге.	2	2		2	6
ИТОГО ЗА СЕМЕСТР / ЗА КУРС / ПО КОМПОНЕНТУ ОПОП	34	34		36,1+3,9	108
ИТОГО ПО КОМПОНЕНТУ ОПОП	34	34		40	108

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1.Контрольные вопросы

1.Система доменных имен.

2. Атака отравление кеша. Типы DNS записей. Обработка DNS запросов.
3. Утилиты для формирования DNS запросов. Понятие DNS зоны. Зон-трансфер.
4. HTTP запросы. Структура и методы.
5. Методы передачи HTTP запросов. HTTP заголовки. Утилиты для создания HTTP запросов.
6. Перехват HTTP запросов.
7. Что такое сервер? Какие сервера вы знаете?
8. Что такое web сервер. Какие они бывают?
9. На каком уровне работает протокол TCP? Как он работает?
10. В чем отличие протоколов tcp и udp? На каком уровне работают эти протоколы? С какими протоколами уровня приложения они работают?
11. Чем порт отличается от сокета? Как создать сокет на языке Python?
12. На каком уровне работает протокол HTTP? Как он работает?
13. Чем отличается синхронный сервер от асинхронного?
14. Сравните multithread и prefork технологии. Достоинства и недостатки.
15. Что такое сокет? Какие три атрибута должен иметь сокет?
16. Что означают команды socket.AF_INET и socket.SOCK_STREAM?
17. Чем отличаются TCP клиент и TCP сервер?
18. Чем метод socket.send отличается от метода socket.sendall ?
19. Что такое эхо-сервер? Что означает list(10) recv(1024)?
20. Чем синхронный сервер отличается от асинхронного?
21. Что означает serv_sock.bind(('', 53210))?
22. Какие методы создания многопоточных серверных приложений вы знаете?
23. Как запустить, остановить сервер nginx? Посмотреть работает ли он? В какую директорию он устанавливается? Какие файлы отвечают за его настройку?
24. Что такое виртуальные хосты? Как они должны настраиваться? Что такое файл конфигурации сервера и что в нем прописано?
25. Что такое location в конфигурационном файле сервера? Какие правила для приоритетов location при выдаче статических документов существуют?
26. Какой еще сервер по умолчанию установлен в Kali?
27. Где хранятся конфигурационные файлы виртуальных хостов для сайтов?
28. Какова структура конфигурационного файла для виртуального хоста? Что надо записывать в файл hosts?
29. Что такое фреймворк и какие фреймворки вы знаете?
30. Преимущества и возможности OpenServer.

7.2. ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Донецкий государственный университет

Физико-технический факультет

Кафедра радиофизики и инфокоммуникационных технологий

Программа высшего образования Программа бакалавриата

Направление подготовки 10.03.01 Информационная безопасность

Профиль подготовки Информационная безопасность

Форма обучения Очная

Семестр Первый

Дисциплина Web-программирование

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

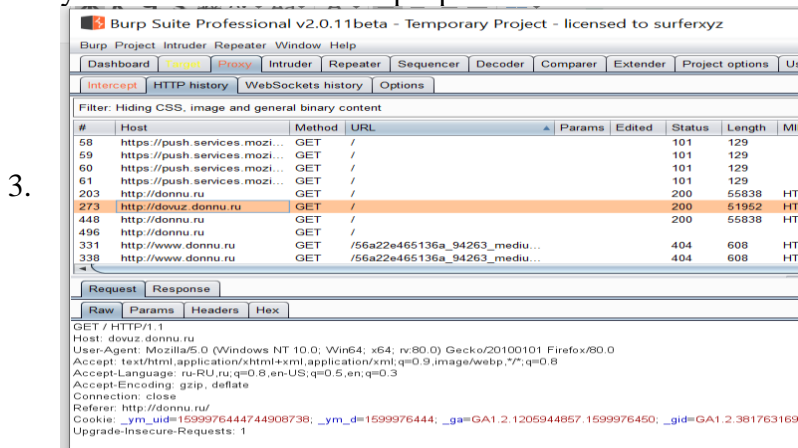
- Что означают следующие заголовки HTTP-запросов и ответов: Expires, Date, Age и If-Modified-..., Do Not Track, Cache-Control, Transfer-Encoding, ETag, X-Frame-Options?
- На рисунке представлен уязвимый код. Объясните, где уязвимость и как ее можно поэксплуатировать.

```

6  <?php
7  if(isset($_GET['ip'])){
8      $target=$_GET['ip'];
9      echo ' <div style="width:30%; float:left">';
10     print shell_exec('ping ' . $target);
11     echo '</div>';
12 }
13 ?>

```

На картинке представлен интерфейс программы для исследования сайтов на уязвимость. Что это за программа и что означают вкладки?



- Определите ip адрес целевого сервера и проверьте его доступность при помощи соответствующих команд.
- Практическое задание: Создайте приложение, устанавливающее куки с именем user и значением – ваше имя. Если поменять значение куки user на admin, должно выводиться приветствие.
- Выполните практическое задание по указанному преподавателем адресу

Утверждено _____ Зав. _____
 на заседании кафедры РФ и ИКТ _____ В.В. Данилов
 № _____ от _____
 _____ 204 г. Экзаменатор _____ М.В.Бабичева

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

Номера разделов	Виды работ	Максимальное количество баллов
тема 1-17	Текущий контроль	10
	Контрольная работа	10
	Лабораторные работы	30
ИТОГО		50
Экзамен		50
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) для лиц с нарушениями опорно-двигательного аппарата:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - письменные задания выполняются на компьютере;
 - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- 1) для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в корпусе №4 ДонГУ (г. Донецк, пр. Театральный, 13). Для проведения лекционных и практических занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для проведения лабораторных занятий требуется лаборатория, оснащенная компьютерами с установленным специальным программным обеспечением, указанным в пункте 13.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.405).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Прохоренок, Н. А. HTML, JavaScript, PHP и MySQL : джентльменский набор Web-мастера / Николай Прохоренок. - 3-е изд. - Санкт-Петербург : БХВ-Петербург, 2010. - 890 с. + электрон. опт. диск (CD-ROM).

2. Альбитц, Пол. DNS и BIND : Рук. для системных администраторов / Пол Альбитц, Крикет Ли ; Пер. с англ. М. Зислица. - 4-е изд. - СПб. : Символ-Плюс, 2002. - 689 с.

3. Ломов, А. Ю. Apache, Perl, MySQL: практика создания динамических сайтов : самоучитель / Артемий Ломов. - СПб. : БХВ-Петербург, 2007. - 354 с. + 1 электрон. опт. диск (CD-ROM).

4. Колисниченко, Д. Н. PHP 5/6 и MySQL 6 : разработка Web-приложений / Д. Н. Колисниченко. - 2-е изд. - Санкт-Петербург : БХВ-Петербург, 2010. - 540 с. + 1 электрон. опт. диск (CD-ROM).

11.2. Дополнительная литература

5. Red Hat Enterprise Linux/Scientific Linux : полное руководство пользователя / [сост.: О. Буденкова и др. ; под общ. ред. О. Садова]. - Санкт-Петербург : БХВ-Петербург, 2007. - 469 с. + электрон. опт. диск (CD-ROM).

6. Основы Web-технологий : учеб. пособие для студентов вузов, обучающихся по специальности 351400 "Прикладная информатика" / П. Б. Храмцов, С. А. Брик, А. М. Русак, А. И. Сурин. - 2-е изд. - М. : Интернет-Ун-т информ. технологий : БИНОМ. Лаб. знаний, 2007. - 374 с.

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Курс по PHP программированию URL: <https://webformymself.com/minikurs/secretphp/index-subscribe.html> – Режим доступа: свободный. – Текст : электронный;

2. Web-программирование URL: <http://confident.org.ua/index.php/stati-po-teme/170-tekhnicheskaya-zashchita-informatsii.html> – Режим доступа: свободный. – Текст : электронный;

3. Курс PHP / MySQL URL: <https://beonmax.com/courses/php-and-mysql/> – Режим доступа: свободный. – Текст : электронный;

4. Простой учебник PHP URL: <https://www.php.net/manual/ru/tutorial.php> – Режим доступа: свободный. – Текст : электронный;

5. Все о PHP, MySQL и не только URL: <http://www.php.su/> – Режим доступа: свободный. – Текст : электронный;

6. Техническая библиотека URL: <http://techlibrary.ru/> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный;

7. Научные журналы ФГБОУ ВО «ДонГУ» URL: <http://donnu.ru/science/journals> (дата обращения: 31.03.2023). – Режим доступа: свободный. – Текст : электронный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Яндекс Браузер (свободно распространяемое ПО)
4. Текстовый редактор Notepad++ (свободно распространяемое ПО)
5. Open Server (свободно распространяемое ПО)