

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

Машаров
«29» марта 2024 г.

П.А. Машаров

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ «АНАЛИЗ БЕЗОПАСНОСТИ WEB-ПРОЕКТОВ»

Укрупненная группа направлений подготовки	10.00.00 Информационная безопасность
Программа высшего образования	Программа магистратуры
Направление подготовки	10.04.01 Информационная безопасность
Магистерская программа	Информационная безопасность
Квалификация	Магистр
Форма обучения	очная; очно-заочная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «Анализ безопасности Web-проектов» для обучающихся по направлению подготовки 10.04.01 Информационная безопасность (Магистерская программа: Информационная безопасность), составлена на основании Федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации Приказ от 26 ноября 2020 г. № 1455(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

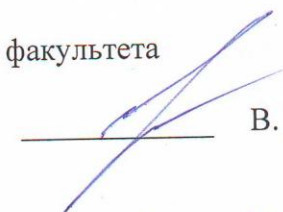
 В.В. Данилов

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:

дисциплины программы бакалавриата: web-программирование, Языки программирования, Программно-аппаратные средства защиты информации, Экспертные системы в информационной безопасности.

1.2. Освоение дисциплины обеспечивает формирование у студентов современных навыков профессиональной обработки информации, позволяет применить ранее изученные языки программирования, что находит отражение в процессе прохождения производственной и научной практики и работы над магистерской диссертацией.

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	10.04.01 Информационная безопасность (Магистерская программа: Информационная безопасность)
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.3.1 Анализ безопасности web-проектов
Часть образовательной программы	Вариативная часть: выбор студента
Количество зачетных единиц / всего часов	4 / 144

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	2	3	17	34	-	93	144	зачет
Очно-заочная, всего	2	4	5	10	-	129	144	зачет

3. ЦЕЛИ ДИСЦИПЛИНЫ

Изучить основные уязвимости web-приложений и методы их выявления.

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

4.1. Компетенции

Компетенции	Индикаторы	Результаты обучения
ПК-2 Разработка систем защиты информации автоматизированных систем (06.33).	ПК-2.1 Оценивание уровня безопасности компьютерных систем	Знает инструментальные программные средства доменного анализа, основных web-уязвимостей. Умеет выбирать, квалифицированно применять средства обеспечения информационной безопасности и целостности данных в соответствии с решаемыми прикладными задачами и создаваемых программных систем

		Умеет проводить аудит web-приложений и систем с целью обеспечения их безопасности.
--	--	--

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
1. Анализ окружения	<p>1.1. Активные и пассивные методы сбора информации.</p> <p>1.2. Методы с подключением к приложению и методы без подключения.</p> <p>1.3. Данные, которые могут быть получены при сборе информации о сайте.</p> <p>1.4. Программные средства для сбора информации.</p> <p>1.5. Поисковые системы.</p> <p>1.6. Специализированные сканеры уязвимостей.</p> <p>1.7. Инструментальные средства анализа защищенности сетей общего назначения.</p> <p>1.8. Инструментальные средства анализа защищенности сетей веб приложений. Dns/whois. Контент.</p> <p>1.9. Активный анализ: port scanning. Точки входа.</p>
2. HTTP-параметры	<p>2.1. Инструменты - анализ запросов</p> <p>2.2. Инструменты - создание запросов</p> <p>2.3. Представление данных. Заголовки http-запроса.</p> <p>2.4. Переменные серверного окружения.</p> <p>2.5. GET- параметры. POST-параметры.</p> <p>2.6. Парсеры http запросов.</p>
3. Цикл анализа	<p>3.1. Основные этапы анализа приложения.</p> <p>3.2. Обзор видов инвентаризации уязвимостей.</p> <p>3.3. Характеристика стадий анализа.</p> <p>3.4. Обзор инструментов, с помощью которых осуществляется инвентаризация.</p> <p>3.5. Характеристика отчёта.</p> <p>3.6. Протоколы семейства SSL/TLS.</p> <p>3.7. Клиент OpenSSL.</p> <p>3.8. Ошибки сервера. P</p> <p>3.9. Раскрытие данных.</p> <p>3.10. Локальное включение файлов.</p> <p>3.11. Инъекция команд.</p>
4. SQL инъекции	<p>4.1. Атака внедрения операторов SQL.</p> <p>4.2. Виды SQL- инъекций.</p> <p>4.3. Классическая, «слепая» типа boolean-based, «слепая» типа time-based, error-based, вложенная, фрагментированная.</p> <p>4.4. Недостаточная обработка входных недоверенных данных при формировании веб-приложением SQL-запросов.</p> <p>4.5. Эксплуатация уязвимостей к SQL- инъекциям.</p>
5. Защищенность механизма управления доступом	<p>5.1. Аутентификация по паролю.</p> <p>5.2. Двух и трехфакторная аутентификация.</p> <p>5.3. Дифференциальный анализ механизма управления доступом.</p> <p>5.4. Основной механизм защиты данных и методов, пришедших из разных источников. Same-Origin Policy.</p> <p>5.5. Анализ на уровнях представления, бизнес-логики и данных веб-приложения.</p>

6. Уязвимости сессии.	6.1. Последовательность HTTP- запросов и соответствующих им HTTP-ответов, ассоциированных с конкретным пользователем. 6.2. Основные атаки на механизмы управления сессиями: фиксация сессии, подбор идентификатора сессии, перехват идентификатора сессии, кража идентификатора сессии. 6.3. Основные требования безопасности к реализации механизма управления сессиями.
7. Уязвимости к CSRF и XSS атакам.	7.1. Атака Cross-Site Request Forgery причины уязвимости и методы обнаружения. 7.2. Cross-Site Scripting (XSS) атака на веб-приложение, использующая недостатки неправильной обработки данных. 7.3. Классификация по вектору и способу воздействия. 7.4. По вектору: отраженные (reflected), устойчивые (persistent) и основанные на объектной модели документа (DOM-based). 7.5. По способу- активные и пассивные. 7.6. Что может получить злоумышленник, проведя XSS атаку. XSS: использование.
8. Пост-эксплуатация	8.1. Поиск и эксплуатация грубых недостатков, допущенных на этапах реализации или конфигурации. 8.2. Эксплуатация хорошо известных уязвимостей. 8.3. Подбор паролей онлайн и офлайн. 8.4. Перманентный доступ: backdoors

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 2, семестр – 3

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
1. Анализ окружения	2	4	-	10	16
2. HTTP-параметры	2	4	-	10	16
3. Цикл анализа	2	4	-	10	16
4. SQL инъекции	2	4	-	10	16
5. Защищенность механизма управления доступом	2	4	-	11	17
6. Уязвимости сессии.	2	4	-	14	20
7. Уязвимости к CSRF и XSS атакам.	2	4	-	14	20
8. Пост-эксплуатация	3	6	-	14	23
ИТОГО ЗА СЕМЕСТР	17	34	-	93	144

6.2. Форма обучения – очно-заочная, курс – 2, семестр – 4

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
1. Анализ окружения	0,6	2	-	16	18,6
2. HTTP-параметры	0,6	1	-	16	17,6
3. Цикл анализа	0,6	1	-	16	17,6
4. SQL инъекции	0,6	1	-	17	18,6
5. Защищенность механизма управления доступом	0,6	1	-	16	17,6
6. Уязвимости сессии.	0,6	1	-	16	17,6
7. Уязвимости к CSRF и XSS атакам.	0,6	1	-	16	17,6
8. Пост-эксплуатация	0,8	2	-	16	18,8
ИТОГО ЗА СЕМЕСТР	5	10	-	129	144

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

7.1. Контрольные вопросы

1. Активные и пассивные методы сбора информации.
2. Методы с подключением к приложению и методы без подключения.
3. Данные, которые могут быть получены при сборе информации о сайте.
4. Программные средства для сбора информации.
5. Поисковые системы. Google Hacking.
6. Специализированные сканеры уязвимостей.
7. Инструментальные средства анализа защищенности сетей общего назначения.
8. Инструментальные средства анализа защищенности сетей вебприложений.

Dns/whois.

9. Активный анализ: port scanning. Точки входа.
10. Инструменты для анализа и создания http запросов
11. Представление данных.
12. Заголовки http-запроса. Переменные серверного окружения.
13. GET- параметры. POST-параметры. Парсеры http запросов.
14. Основные этапы анализа приложения.
15. Обзор видов инвентаризации уязвимостей. Характеристика стадий анализа.
16. Обзор инструментов, с помощью которых осуществляется инвентаризация.
17. Протоколы семейства SSL/TLS. Клиент OpenSSL.
18. Ошибки сервера. Раскрытие данных.
19. Локальное включение файлов.
20. Инъекция команд.
21. Атака внедрения операторов SQL. Виды SQL- инъекций.
22. Классическая, «слепая» типа boolean-based, «слепая» типа time-based, error-based, вложенная, фрагментированная. недостаточная обработка входных недоверенных данных при формировании веб-приложением SQL-запросов.
23. Эксплуатация уязвимостей к SQL- инъекциям и защита.

7.2. Темы докладов

1. Сбор информации о веб-приложении.
2. Сканирование уязвимостей веб-приложений
3. Дорки и Google Hacking.
4. Анализ HTTP-запросов
5. Перехват HTTP-запросов
6. Тестирование защищенности транспортного уровня.
7. Тестирование защищенности прикладного уровня.
8. Тестирование на устойчивость к атакам отказа в обслуживании.
9. Поиск уязвимостей к атакам SQL-injection.
10. Тестирование защищенности механизма управления доступом.
11. Тестирование защищенности механизма управления сессиями.
12. Поиск уязвимостей к атакам RCE.
13. Тестирование на наличие уязвимостей в логике приложений.
14. Поиск уязвимостей к атакам CSRF.
15. Поиск уязвимостей к атакам XSS.
16. Бэkdоры.
17. Безопасная аутентификация.

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.).

8.1. Семестр 3

Номера разделов	Виды работ	Максимальное количество баллов
1-8	Текущий контроль:	5
	Лабораторные работы	34
	Доклад по выбранной теме	11
ИТОГО		50
Зачет		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, обеспеченная персональными компьютерами.

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. Корт, С. С. Теоретические основы защиты информации : Учеб. пособие для студентов вузов, обучающихся по группе спец. в обл. информ. безопасности / С. С. Корт. - М. : Гелиос АРВ, 2004. - 233 с.

2. Информационная безопасность открытых систем [Текст] : учебник для студентов вузов, обучающихся по специальности 075500 (090105) - "Комплексное обеспечение информационной безопасности автоматизированных систем" : [в 2 т.]. Т. 1 : Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. - М. : Горячая Линия-Телеком, 2006. - 535 с.

3. Гаевский, А. Ю. 100% самоучитель по созданию Web-страниц и Web-сайтов. HTML и JavaScript / А. Ю. Гаевский, В. А. Романовский. - М. : Технолоджи-3000 : Триумф, 2008. - 457 с.

11.2. Дополнительная литература

5. Хорев, П. Б. Криптографические интерфейсы и их использование / П. Б. Хорев. - М. : Горячая Линия-Телеком, 2007. - 277 с.

5. 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).

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Анализ безопасности веб-проектов [Электронный ресурс]. – Режим доступа: <https://stepik.org/lesson/19928/step/3?unit=4735>.

2. Основы анализа безопасности веб-проектов [Электронный ресурс]. – Режим доступа: <https://ezhvsalate.ru/posts/osnovy-analiza-bezopasnosti-veb-proektov/>

3. CTF на Физтехе [Электронный ресурс]. – Режим доступа: <https://github.com/xairy/mipt-ctf>

4. PentesterAcademy Courses and Online Labs [Электронный ресурс]. – Режим доступа: <https://www.pentesteracademy.com/>

5. Open security training.info [Электронный ресурс]. – Режим доступа: <http://opensecuritytraining.info/>

6. Natas. [Электронный ресурс]. – Режим доступа: <https://overthewire.org/wargames/natas/>: 5. Национальная электронная библиотека (НЭБ): федеральная государственная информационная система / Министерство Культуры РФ; Российская государственная библиотека. – Москва, 2019- . – URL: <https://rusneb.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный, подписка. Необходима установка программного обеспечения. – Текст: электронный.

7. eLIBRARY.RU: научная электронная библиотека: сайт. – Москва, 2000- . – URL: <https://elibrary.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

8. Научная электронная библиотека «КиберЛенинка»: сайт / Ассоциация «Открытая наука». – Москва, 2014- . – URL: <https://cyberleninka.ru/>. – Режим доступа: свободный. – Текст: электронный.

9. Электронно-библиотечная система «Лань»: [сайт]. – URL: <https://e.lanbook.com> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

10. ЭБС Юрайт: электронная библиотечная система: сайт. – Москва, 2013. – URL: <https://biblio-online.ru> (дата обращения: 01.09.2023). – Режим доступа: для авторизов. пользователей. – Текст: электронный.

11. Электронно-библиотечная система ДонГУ: сайт / ФГБОУ ВО «ДонГУ». – Донецк, 2016- . – URL: <http://library.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный. – Текст: электронный.

12. Электронный каталог Научной библиотеки ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://library.donnu.ru/catalog/> (дата обращения: 01.09.2023). – Режим доступа: поиск свободный, электронные документы – для пользователей ДонГУ.

13. Электронный архив ДонГУ: раздел сайта / НБ ДонГУ. – Текст: электронный // ЭБС ДонГУ: сайт. – URL: <http://repo.donnu.ru/> (дата обращения: 01.09.2023). – Режим доступа: свободный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Yandex-браузер (свободно распространяемое ПО).