МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Анализ защищенности систем»

Направление подготовки
10.03.01 «Информационная безопасность»

Профиль/специализация
«Безопасность компьютерных систем»

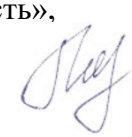
Квалификация
Бакалавр

Формы обучения
Очная

Москва, 2023 г.

Разработчик(и):

Преподаватель  /Г.Ф. Шипулин/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,
 А.Ю. Гневшев

Руководитель образовательной программы,
 А.Ю. Гневшев

Содержание

1 **Ошибка! Закладка не определена.**
2 **Ошибка! Закладка не определена.**
3 5
3.1 6
3.2 **Ошибка! Закладка не определена.**
3.3 7
3.4 7
3.5 7
4 **Ошибка! Закладка не определена.**
4.1 8
4.2 8
4.3 8
4.4 8
4.5 9
4.6 9
5 9
6 9
6.1 9
6.2 9
7 **Ошибка! Закладка не определена.**
7.1 9
7.2 10
7.3 10

1 Цели, задачи и планируемые результаты обучения по дисциплине

Целью преподавания дисциплины является формирование у студентов знаний в области анализа защищенности систем.
Задачи преподавания дисциплины:

- изучение методов управления информационной безопасностью;
- освоение методов и средств оценки информационных рисков в информационных системах;
- освоение методов и средств выявления угроз информационной безопасности;
- освоение средств контроля эффективности принятых мер по реализации частных политик информационной безопасности информационных систем.

В результате освоения дисциплины «Анализ защищенности систем» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:
знать:
- основные угрозы безопасности информации и модели нарушителя в информационных системах;
- основные методы управления информационной безопасностью;
- методы и средства контроля эффективности технической защиты информации;

уметь:
- разрабатывать модели угроз и нарушителей информационной безопасности информационных систем, определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, выявлять уязвимости информационно-технологических ресурсов информационных систем;
- оценивать информационные риски в информационных системах, разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем;
- контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем;

владеть:
- навыками анализа информационной инфраструктуры информационной системы и ее безопасности, методами выявления угроз информационной безопасности информационных систем;
- методами управления информационной безопасностью информационных систем, методами оценки информационных рисков;
- навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем, навыками участия в экспертизе состояния защищенности информации на объекте защиты.

Обучение по дисциплине «Анализ защищенности систем» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК—12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с	ИОПК-12.1. Знает основные угрозы безопасности информации и модели нарушителя в информационных системах; ИОПК-12.2. Умеет разрабатывать модели угроз и нарушителей информационной безопасности информационных систем, определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите,

нормативными и корпоративными требованиями; ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	выявлять уязвимости информационно-технологических ресурсов информационных систем; ИОПК-12.3. Владеет навыками анализа информационной инфраструктуры информационной системы и ее безопасности, методами выявления угроз информационной безопасности информационных систем. ИОПК-1.4.1. Знает основные методы управления информационной безопасностью; ИОПК-1.4.2. Умеет оценивать информационные риски в информационных системах, разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем; ИОПК-1.4.3. Владеет методами управления информационной безопасностью информационных систем, методами оценки информационных рисков. ИПК-3.1. Знает методы и средства контроля эффективности технической защиты информации; ИПК-3.2. Умеет контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; ИПК-3.3. Владеет навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем, навыками участия в экспертизе состояния защищенности информации на объекте защиты.

2 Место дисциплины в структуре образовательной программы

Дисциплина «Анализ защищенности систем» относится к числу профессиональных учебных дисциплин части, формируемой участниками образовательных отношений (Б1.2) основной образовательной программы (Б1.2.1).
Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы проектирования информационных систем», «Введение в аналитику информационной безопасности».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, т.е. 216 часов (лекции – 36 часов, лабораторные занятия – 72 часа, самостоятельная работа - 108 часов, форма контроля – экзамен) в 5 семестре.

Структура и содержание дисциплины «Инструментальные средства анализа защищённости и управления уязвимостями» по срокам и видам работы отражены в приложении

3.1 Виды учебной работы и трудоемкость

(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			5	
1	**Аудиторные занятия**	**108**	108	
	В том числе:			
1.1	Лекции	36	36	
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	**Самостоятельная работа**	**108**	108	
	В том числе:			
2.1	…			
3	**Промежуточная аттестация**			
	Зачет/диф.зачет/экзамен		Экзамен	
	Итого	**216**		

3.1.2 Очно-заочная форма обучения
Не предусмотрена

3.1.3 Заочная форма обучения
Не предусмотрена

3.2 Тематический план изучения дисциплины

(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1.						
1.1	Тема 1. Анализ безопасности серверной части веб-приложений	92	16		30		46
1.2	Тема 2. Анализ безопасности клиентской части веб-приложений	124	20		42		62
	Итого	**216**	**36**		**72**		**108**

3.2.2 Очно-заочная форма обучения
Не предусмотрена.

3.2.2 Заочная форма обучения
Не предусмотрена

3.3. Содержание дисциплины

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1	Раздел 1	
1.1	Анализ безопасности серверной части веб-приложений.	Методы и средства поиска веб-уязвимостей. Методы сбора информации о системе: активные и пассивные. Уязвимости класса Injections: поиск, эксплуатация, защита. Уязвимости класса Security Misconfiguration: поиск, эксплуатация, защита. Уязвимости класса Inclusion: поиск, эксплуатация, защита. RCE-уязвимости: поиск, эксплуатация, защита.
1.2	Анализ безопасности клиентской части веб-приложений.	Уязвимости класса XSS: виды, контекст, поиск, эксплуатация и защита. Уязвимости класса CSRF: поиск, эксплуатация, защита. Web Application Firewall: виды, настройка. Content Security Policy: версии, способы тестирования политик и внедрения.

3.4 Тематика семинарских/практических и лабораторных занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные занятия

№	Наименование лабораторной работы	Объем, час.
1	Выполнение лабораторной работы №1	8
2	Выполнение лабораторной работы №2	10
3	Выполнение лабораторной работы №3	12
4	Выполнение лабораторной работы №4	18
5	Выполнение лабораторной работы №5	12
6	Выполнение лабораторной работы №6	12
Итого		72

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по данной дисциплине учебным планом не запланировано.

4 Учебно-методическое и информационное обеспечение

4.4 Нормативные документы и ГОСТы

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность».

4.5 Основная литература

1. Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018 — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С.51
2. Никитин, В. Н. Проведение анализа защищённости информации в информационной системе : учебное пособие / В. Н. Никитин. — Хабаровск : ДВГУПС, 2020 — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179382 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 10
3. Корниенко, А. А. Система требований к обеспечению безопасности автоматизированных систем и значимых объектов критической информационной инфраструктуры : учебное пособие / А. А. Корниенко, В. С. , А. П. Глухов. — Санкт-Петербург : ПГУПС, 2022 — ISBN 978-5-7641-1837-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/329477 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 5

4.6 Дополнительная литература

1. Сельвесюк, Н.И. МЕТОДОЛОГИЯ АНАЛИЗА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ / Н.И. Сельвесюк, А.С. Островский, В.Д. Сливинский // Информатика и системы управления. — 2016 — № 2 — С. 17-24. — ISSN 1814-2400. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/journal/issue/300657 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 1
2. Каширская, Е. Н. Защита информации в информационно – управляющих системах : учебное пособие / Е. Н. Каширская, М. А. Макаров. — Москва : РТУ МИРЭА, 2020 — 67 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167621 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 3
3. Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018 — ISBN 978-5-7410-2297-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804 (дата обращения: 01.09.2023). — Режим доступа: для авториз. пользователей. — С. 59

4.7 Электронные образовательные ресурсы

1. ЭОР «Анализ защищенности систем» [Электронный ресурс] — URL: https://online.mospolytech.ru/course/view.php?id=11896 (дата обращения: 18.02.2023).

4.8 Лицензионное и свободно распространяемое программное обеспечение

1. Virtual Box
2. Виртуальная машина Metasploitable3
3. Дистрибутив ОС Kali Linux

4.9 Современные профессиональные базы данных и информационные справочные системы

1. OWASP Web Security Testing Guide [Электронный ресурс] — URL: https://owasp.org/www-project-web-security-testing-guide/ (дата обращения: 18.02.2023).

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.
Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.4 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.5 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической и практической подготовки студентов являются лекции и лабораторные работы.
В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

7 Фонд оценочных средств

7.4 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:
- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

7.5 Шкала и критерии оценивания результатов обучения

Форма промежуточной аттестации: экзамен.
По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.6 Оценочные средства

7.3.1 Текущий контроль
Оценочные средства для текущей аттестации
- Защита отчетов о выполнении лабораторных работ

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации
- Экзамен

Список вопрос для проведения экзамена по дисциплине:
1.Методы и средства поиска веб-уязвимостей.
2.Активные методы сбора информации о системе.
3. Пассивные методы сбора информации о системе.
4. Уязвимости класса Injections: поиск, эксплуатация и защита (SQL-injection, HTML-injection).
5. Уязвимости класса Injections: поиск, эксплуатация и защита (XPath-injection, iFrame-injection).
6. Уязвимости класса SecurityMisconfiguration: поиск, эксплуатация, защита.
7. Поиск и эксплуатация RCE-уязвимостей.
8. Защита от RCE-уязвимостей.
9. Уязвимость Self XSS: контекст, поиск, эксплуатация и защита.
10. Уязвимость Blind XSS: контекст, поиск, эксплуатация и защита.
11. Уязвимость Stored XSS: контекст, поиск, эксплуатация и защита.
12. Уязвимость Reflected XSS: контекст, поиск, эксплуатация и защита.
13. Уязвимость DOM-based XSS: контекст, поиск, эксплуатация и защита.
14. Поиск и эксплуатация CSRF-уязвимостей.
15. Защита от CSRF-уязвимостей.
16. Настройка и внедрение WAF.
17. Детектирование и обход WAF.
18. Content Security Policy: версии, их функциональные отличия.
19. Content Security Policy: способы тестирования политик и внедрения.

Пример билета.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий
Кафедра: Информационная безопасность
Дисциплина: Анализ защищенности систем
Бакалавры. Курс 3, семестр 1

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Уязвимость Self XSS: контекст, поиск, эксплуатация и защита.
2. Уязвимости класса Injections: поиск, эксплуатация и защита (SQL-injection, HTML-injection).

Преподаватель _____ / Шипулин Г.Ф. /