МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Гусев П.Ю./

28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Анализ уязвимостей компьютерных систем и сетей»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ Е.С. Соколова

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ К.А. Разинкин

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины изучение студентом основных видов уязвимостей, методов и средств их анализа и устранения.

1.2. Задачи освоения дисциплины

✓ формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;

✓ формирование навыков анализа программных реализаций на предмет наличия уязвимостей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Анализ уязвимостей компьютерных систем и сетей» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Анализ уязвимостей компьютерных систем и сетей» направлен на формирование следующих компетенций:

ПК-4.1 - Способен анализировать защищённость и оценивать уровень безопасности компьютерных систем и сетей

ПК-4.5 - Способен анализировать уязвимости и угрозы информационной безопасности в компьютерных системах и сетях

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4.1	знать уязвимости компьютерных систем и сетей
	уметь разрабатывать предложения по устранению выявленных уязвимостей
	владеть навыками формулирования предложений по устранению выявленных уязвимостей компьютерных сетей
ПК-4.5	знать основные классы и виды уязвимостей программного обеспечения
	уметь анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем
	владеть методиками разработки практических рекомендаций по устранению выявленных уязвимостей и навыками формирования планов мероприятий по нейтрализации угроз безопасности компьютерных сетей

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Анализ уязвимостей компьютерных систем и сетей» составляет 9 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	126	54	72
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	54	18	36
Самостоятельная работа	126	18	108
Часы на контроль	72	36	36
Виды промежуточной аттестации - экзамен	+	+	+
Общая трудоемкость: академические часы зач.ед.	 324 9	 108 3	 216 6

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	Введение в анализ уязвимостей	Понятие угрозы и уязвимости и атаки. Классификация и классификаторы уязвимостей. Понятия "уязвимость кода", "уязвимость конфигурации", "уязвимость архитектуры", "организационная уязвимость", "многофакторная уязвимость". База данных общеизвестных уязвимостей информационной безопасности CVE (англ. Common Vulnerabilities and Exposures). Обзор банка данных угроз безопасности информации Федеральная служба по техническому и экспортному контролю ФСТЭК России. Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России. Стандарт Common Vulnerability Scoring System (CVSS). ГОСТ Р 56546-2015. ГОСТ Р 58142-2018 МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045 Классификация уязвимостей информационных систем. Классификация эксплойтов. Анализ стандартов и методик тестирования на проникновение. Уязвимости нулевого дня.	12	8	20	40

		Обзор наиболее распространенных и критических уязвимостей.				
2	Аппаратные уязвимости	Аппаратная уязвимость категории утечка по стороннему каналу (Meltdown). Группа аппаратных уязвимостей – Spectre. Уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости. Уязвимости в портативных технических средствах. уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании. уязвимости в средствах защиты информации.	12	8	20	40
3	Программные уязвимости	Уязвимости в общесистемном (общем) ПО. Уязвимости в прикладном ПО. Уязвимости в специальном ПО	12	8	20	40
4	Методы и инструменты анализа уязвимостей в сфере информационной безопасности	Методы: экспертный и статистический анализ, анализ документации, сканирование уязвимостей, моделирование атак, тестирование на проникновение, визуализация данных. Методология тестирования на проникновение: разведка, сканирование и перечисление, получение доступа, повышение привелеги, поддержание доступа, заметание следов, составление отчёта. Получение отпечатка сбор информации: разведка по открытым источникам, использование общих ресурсов, запрос сведений о регистрации, анализ записей DNS, получение сведений о маршрутизации, автоматизированные инструменты для снятия отпечатков и сбора информации. Методы сканирования и уклонения: сканирование портов, сетевые сканеры, автоматическое сканирование уязвимостей. Тестирование web-приложений: веб-анализ, межсайтовые сценарии, SQL – иньекция. Тестирование беспроводных сетей на проникновение: разведка в беспроводной сети, инструменты тестирования, анализ беспроводного трафика. Мобильное тестирование на проникновение с Kali NetHunter. Инструменты анализа уязвимостей Kali Linux.	36	30	66	132
		Итого	**72**	**54**	**126**	**252**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»; «не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-4.1	знать уязвимости компьютерных систем и сетей	обучающийся перечисляет классы уязвимостей согласно common weakness enumeration (cwe);	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь разрабатывать предложения по устранению выявленных уязвимостей	обучающийся умеет подбирать метод реагирования под конкретную уязвимость	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками формулирования предложений по устранению выявленных уязвимостей компьютерных сетей	обучающийся владеет навыками оформления предложения в виде связного текста/таблицы, разделения их по важности, указанием что конкретно сделать	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-4.5	знать основные классы и виды уязвимостей программного обеспечения	обучающийся описывает механизмы возникновения уязвимостей (переполнение буфера, sql-инъекции, xss); приводит примеры уязвимостей из каждой классификационной группы.	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем	обучающийся анализирует фрагмент кода или схему архитектуры на предмет уязвимостей; выявляет не менее трёх потенциально опасных мест в заданной архитектуре; сопоставляет выявленные недостатки с требованиями нормативных документов (фстэк, гост).	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методиками разработки практических рекомендаций по устранению выявленных уязвимостей и навыками формирования планов мероприятий по нейтрализации угроз безопасности компьютерных сетей	обучающийся составляет план первоочередных мероприятий для устранения выявленных уязвимостей. для каждой уязвимости подбирает метод защиты (обновление, настройка, замена компонента). обосновывает выбор методики устранения уязвимости с точки зрения затрат и эффективности.		

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9, 10 семестре для очной формы обучения по четырехбалльной системе:

«отлично»; «хорошо»; «удовлетворительно»; «неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПК-4.1	знать уязвимости компьютерных систем и сетей	Тест	Выполнение теста на 90-100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь разрабатывать предложения по устранению выявленных уязвимостей	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками формулирования предложений по устранению выявленных уязвимостей компьютерных сетей	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
ПК-4.5	знать основные классы и виды уязвимостей программного обеспечения	Тест	Выполнение теста на 90-100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены
	владеть методиками разработки практических рекомендаций по устранению выявленных уязвимостей и навыками формирования планов мероприятий по нейтрализации угроз безопасности компьютерных сетей	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстр ирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстр ирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. **Что такое эксплойт?**

а)компьютерная программа, нейтрализующая уязвимости в программном обеспечении

б) компьютерная программа, использующая уязвимости в программном обеспечении и применяемая для проведения атаки на вычислительную систему

в) компьютерная программа, содержащая уязвимости

2. **К какому классу относится уязвимость, появившаяся в результате разработки программного обеспечения без учета требований по безопасности информации?**

а) уязвимость архитектуры

б) уязвимость кода

в) многофакторная уязвимость

3. **К какому классу относится уязвимость, появившаяся в результате выбора, компоновки компонентов программного обеспечения, содержащих уязвимости?**

а) уязвимость архитектуры

б) уязвимость кода

в) многофакторная уязвимость

4. **Common Vulnerabilities and Exposures (CVE) это...**

а) база данных угроз информационной безопасности

б) база данных общеизвестных уязвимостей

в) база данных эксплоитов

г) база данных наиболее крупных атак на вычислительные системы в мире

5. **Что такое CVE Numbering Authority (CNA)?**

а) идентификатор уязвимости

б) организации, которым разрешено назначать CVE ID уязвимостям в согласованных за ними областях

в) эксплоит уязвимости

г) количество уязвимостей одного типа

6. **Что такое Primary CAN?**

а) идентификатор уязвимости

б) организации, которым разрешено назначать CVE ID уязвимостям в согласованных за ними областях

в) эксплоит уязвимости

г) организация, курирующая ведение CVE

7. **Для чего используется CVSS?**

а) для оценки угроз

б) для оценки потенциала нарушителя

в) для оценки уязвимостей

8. **Какая версия стандарта CVSS является актуальной?**

а) первая

б) вторая

в) третья

г) четвертая

9. **Какие метрики используются для оценки уязвимостей в CVSS?**

а) базовые

б) стандартные

в) контекстные

г) временные

д) постоянные

10. **В описании угрозы в Банке данных угроз безопасности информации в качестве источника угрозы указаны...**

а) минимальные возможности внешнего или внутреннего нарушителя, необходимые для реализации угрозы

б) максимальные возможности внешнего или внутреннего нарушителя, необходимые для реализации угрозы

в) минимальные возможности внутреннего нарушителя, необходимые для реализации угрозы

г) максимальные возможности внешнего нарушителя, необходимые для реализации угрозы

7.2.2 Примерный перечень заданий для решения стандартных задач

1. К какому классу уязвимостей относится возможность внедрения произвольного SQL-кода в запрос к базе данных?

А) Межсайтовый скриптинг (XSS)

Б) SQL-инъекция

В) Неправильная конфигурация сервера

Г) Недостатки аутентификации

2. Что означает аббревиатура CVE в контексте анализа защищенности?

А) Common Vulnerabilities and Exposures (общеизвестные уязвимости и риски)

Б) Central Vulnerability Exploit (центральный эксплойт уязвимости)

В) Certified Virtual Environment (сертифицированная виртуальная среда)

Г) Closed Virtual Examination (закрытая виртуальная проверка)

3.Уязвимость, связанная с выходом за границы буфера в памяти программы, чаще всего приводит к:

А) Замедлению работы сети

Б) Отказу в обслуживании или выполнению произвольного кода

В) Потере данных в базе данных

Г) Подмене DNS-записей

4. Какой тип уязвимости описан в ситуации: «Злоумышленник отправляет жертве ссылку, при переходе по которой в контексте доверенного сайта выполняется вредоносный сценарий в браузере жертвы»?

А) Подделка межсайтовых запросов (CSRF)

Б) Межсайтовый скриптинг (XSS)

В) Внедрение команд ОС

Г) Небезопасная десериализация

5. Сканер уязвимостей (например, OpenVAS или Nessus) обнаружил открытый порт 23/tcp. Какая служба работает на этом порту и чем она опасна?

А) SSH — опасен слабыми паролями

Б) Telnet — передаёт данные в открытом виде (нешифрованный трафик)

В) FTP — опасен анонимным доступом

Г) HTTP — опасен XSS-уязвимостями

6.При анализе безопасности сети обнаружено, что сервер использует протокол SMBv1. Какое действие следует рекомендовать в первую очередь?

А) Разрешить SMBv1 для совместимости со старыми клиентами

Б) Отключить SMBv1 и использовать SMBv2 или SMBv3

В) Установить антивирус на сервер

Г) Закрыть все порты, кроме 80 и 443

7. В логах межсетевого экрана наблюдается множество запросов с одного IP-адреса на разные порты в короткий промежуток времени. Что это может означать?

А) Некорректная настройка маршрутизации

Б) Сканирование портов (разведка перед атакой)

В) Перегрузка процессора сервера

Г) Сбой в работе протокола DHCP

8. Веб-приложение уязвимо для атак путем подбора паролей (брутфорс). Какое предложение по устранению будет наиболее эффективным?

А) Сменить IP-адрес сервера

Б) Внедрить механизм CAPTCHA и блокировку после нескольких неудачных попыток

В) Установить сертификат SSL

Г) Обновить версию PHP

9. На рабочей станции пользователя обнаружено программное обеспечение с известной уязвимостью, для которой производитель уже выпустил обновление (патч). Ваши действия по устранению:

А) Удалить программу

Б) Заблокировать программу в брандмауэре

В) Установить обновление безопасности (патч)

Г) Очистить кэш браузера

10. Анализ конфигурации сервера показал, что разрешена аутентификация по протоколу NTLMv1. Какое предложение по усилению безопасности является верным?

А) Отключить аутентификацию полностью

Б) Отключить NTLMv1 и оставить только NTLMv2 или Kerberos

В) Разрешить только гостевой доступ

Г) Включить запись всех логов NTLMv1 для анализа

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Анализ лога веб-сервера. В логе веб-сервера обнаружена следующая запись:

```
192.168.1.45 - - [28/Feb/2026:10:15:23] "GET /index.php?id=1 UNION
SELECT username,password FROM users HTTP/1.1" 200 4532
```

Что пытался сделать злоумышленник?

А) Межсайтовый скриптинг (XSS)

Б) SQL-инъекцию

В) Подбор паролей (брутфорс)

Г) DDoS-атаку

2. **Анализ конфигурации FTP-сервера.** В конфигурации FTP-сервера (vsftpd) обнаружена строка:

```
anonymous_enable=YES
```

Какую угрозу создает данная настройка?

А) Разрешает анонимную загрузку и скачивание файлов без пароля

Б) Отключает шифрование трафика

В) Блокирует всех локальных пользователей

Г) Включает режим отладки

3. Анализ DNS-запросов

Система мониторинга зафиксировала множественные DNS-запросы с внутреннего IP-адреса на внешний DNS-сервер к домену malware-domain[.]com.

О чем это свидетельствует?

А) О корректной работе DNS-кэширования

Б) О возможном заражении рабочей станции вредоносным ПО

В) О попытке подмены DNS-записей

Г) О нормальной работе браузера

4. Анализ результатов Nmap

Выполнено сканирование сети. Результат:

```
Nmap scan report for 10.0.0.15
PORT      STATE     SERVICE
22/tcp    open      ssh
445/tcp   open      microsoft-ds
3389/tcp  filtered  ms-wbt-server
```

Что означает статус "filtered" для порта 3389?

А) Порт открыт и доступен

Б) Порт закрыт

В) Межсетевой экран блокирует пакеты, статус порта не определен

Г) Сервис работает, но не отвечает

5. Приоритезация уязвимостей

По результатам сканирования получены три уязвимости:

SSL-сертификат истек 2 года назад

Открытый порт Telnet (23/tcp)

Используется устаревшая версия Apache 2.2.3 (известны RCE-уязвимости)

Какую уязвимость необходимо устранить в первую очередь?

А) Истекший SSL-сертификат

Б) Открытый порт Telnet

В) Устаревшую версию Apache с RCE

Г) Все одновременно

6. Анализ заголовков HTTP

При анализе веб-приложения обнаружено, что в ответах сервера отсутствует заголовок Content-Security-Policy.

К каким атакам это делает приложение более уязвимым?

А) SQL-инъекции

Б) Межсайтовому скриптингу (XSS)

В) Подбору паролей

Г) Отказу в обслуживании

7. Устранение уязвимости шифрования

При анализе Wi-Fi сети офиса обнаружено использование протокола WPA2 с CCMP (AES). Это считается безопасным, но в логах точки доступа зафиксированы попытки деаутентификации клиентов.

Что следует предпринять?

А) Перейти на WEP для совместимости

Б) Включить защиту от деаутентификации (802.11w) если поддерживается

В) Отключить Wi-Fi полностью

Г) Сменить SSID

8. Реагирование на инцидент безопасности

Пользователь сообщил, что при переходе на сайт банка браузер выдал предупреждение о несоответствии SSL-сертификата (домен в сертификате не совпадает с сайтом).

Что произошло вероятнее всего?

А) Атака типа "человек посередине" (MITM)

Б) Сбой в работе браузера

В) Устаревшая версия Windows

Г) Вирус на компьютере пользователя

9. Анализ прав доступа

В результате аудита выяснилось, что обычные пользователи имеют права на запись в системную директорию C:\Windows\System32.

Чем это опасно?

А) Пользователи могут случайно удалить важные файлы

Б) Злоумышленник может разместить вредоносный DLL-файл, который подгрузит система

В) Замедлением работы компьютера

Г) Невозможностью установить обновления

10. Оценка эффективности защиты

Администратор настроил межсетевой экран на блокировку всех входящих подключений, кроме порта 80 (HTTP) и 443 (HTTPS).

От каких атак эта конфигурация НЕ защищает?

А) От сканирования портов извне

Б) От атак на веб-приложения (SQL-инъекции, XSS)

В) От попыток подключения к закрытым портам

Г) От DDoS-атак на сетевом уровне

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень вопросов для подготовки к экзамену

1.Понятие угрозы и уязвимости и атаки.

2.Классификация и классификаторы уязвимостей.

3.Понятия "уязвимость кода", "уязвимость конфигурации", "уязвимость архитектуры", "организационная уязвимость", "многофакторная уязвимость".

4.База данных общеизвестных уязвимостей информационной безопасности CVE (англ. Common Vulnerabilities and Exposures).

5.Обзор банка данных угроз безопасности информации Федеральная служба по техническому и экспортному контролю ФСТЭК России.

6.Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.

7.Стандарт Common Vulnerability Scoring System (CVSS). ГОСТ Р 56546-2015. ГОСТ Р 58142-2018 МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

8.Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045

9. Классификация уязвимостей информационных систем.

10. Классификация эксплойтов.

11.Анализ стандартов и методик тестирования на проникновение.

12. Уязвимости нулевого дня. Обзор наиболее распространенных и критических уязвимостей.

13.Аппаратная уязвимость категории утечка по стороннему каналу (Meltdown).

14.Группа аппаратных уязвимостей - Spectre.

15.Уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости.

16.Уязвимости в портативных технических средствах. уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании. уязвимости в средствах защиты информации.

17.Уязвимости в общесистемном (общем) ПО. Уязвимости в прикладном ПО. Уязвимости в специальном ПО

18.Методы: экспертный и статистический анализ, анализ документации, сканирование уязвимостей, моделирование атак, тестирование на проникновение, визуализация данных.

19.Методология тестирования на проникновение: разведка, сканирование и перечисление, получение доступа, повышение привелеги, поддержание доступа, заметание следов, составление отчёта.

20.Получение отпечатка сбор информации: разведка по открытым источникам, использование общих ресурсов, запрос сведений о регистрации, анализ записей DNS, получение сведений о маршрутизации, автоматизированные инструменты для снятия отпечатков и сбора информации.

21.Методы сканирования и уклонения: сканирование портов, сетевые сканеры, автоматическое сканирование уязвимостей.

22.Тестирование web-приложений: веб-анализ, межсайтовые сценарии, SQL - иньекция.

23.Тестирование беспроводных сетей на проникновение: разведка в беспроводной сети, инструменты тестирования, анализ беспроводного трафика.

24.Мобильное тестирование на проникновение с Kali NetHunter.

25. Инструменты анализа уязвимостей Kali Linux.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение в анализ уязвимостей	ПК-4.1	Тест, практические работы, вопросы к экзамену
2	Аппаратные уязвимости	ПК-4.1;ПК-4.5	Тест, практические работы, вопросы к экзамену
3	Программные уязвимости	ПК-4.1;ПК-4.5	Тест, практические работы, вопросы к экзамену
4	Методы и инструменты анализа уязвимостей в сфере информационной безопасности	ПК-4.1;ПК-4.5	Тест, практические работы, вопросы к экзамену

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Информационная безопасность. Практические аспекты: учебник / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург: Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/161340

Алешкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности): учебное пособие / А. С. Алешкин, С. А. Лесько, Д. О. Жуков. — Москва: РТУ МИРЭА, 2020. — 152 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600

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. — https://e.lanbook.com/book/182299

Дополнительная литература

Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва: Издательство Юрайт, 2026. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/586060

Давидюк, Н. В. Мониторинг безопасности информационных систем: учебное пособие / Н. В. Давидюк, И. М. Космачева. — Санкт-Петербург: Интермедия, 2020. — 116 с. — ISBN 978-5-4383-0204-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/161352

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asphttps://cchgeu.ru/education/cafedras/kafsibUdocs

http://www.eios.vorstu.ru (ЭИОС ВГТУ)

https://e.lanbook.com/ (ЭБС Лань)

https://www.iprbookshop.ru/ (ЭБСIPRbooks)

https://urait.ru/ (ЭБС Юрайт)

https://cve.mitre.org CVE (Common Vulnerabilities and Exposures) — главный международный словарь уязвимостей

https://nvd.nist.gov NVD (National Vulnerability Database) — база уязвимостей США с метриками CVSS

https://www.cvedetails.com CVE Details — удобный агрегатор уязвимостей с поиском по продуктам

https://www.wireshark.org Wireshark — анализатор трафика

https://www.metasploit.com Metasploit Framework — тестирование на проникновение

https://www.hackthebox.com HackTheBox — платформа для пентеста

https://www.vulnhub.com VulnHub — уязвимые виртуальные машины

https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27001 — стандарт информационной безопасности

https://www.pcisecuritystandards.orgPCI DSS — стандарт безопасности платежных карт

https://spy-soft.net/tools-to-find-vulnerabilities (инструменты для поиска уязвимостей сайтов)

https://bdu.fstec.ru/vul(База данных уязвимостей ФСТЭК)

https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-117a

Агентство кибербезопасности и безопасности инфраструктуры (CISA, США)

https://www.ptsecurity.com/ru-ru/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Анализ уязвимостей компьютерных систем и сетей» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков анализа уязвимостей.

1. Базы данных угроз безопасности информации (ФСТЭК, MITRE)
2.Поиск уязвимостей к атакам CSRF.
3.Поиск уязвимостей к атакам XSS.
4. Поиск уязвимостей к атакам SQL-injection.
5. Поиск уязвимостей к атакам RCE.
6. Сканирование уязвимостей веб-приложений.
7. Программные средства инструментального анализа защищенности

8. Сканеры уязвимостей веб-приложений

Занятия проводятся путем решения конкретных задач в аудитории.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед экзаменом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4