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

«Программное обеспечение анализа защищенности информационных систем и сетей»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ К.А. Разинкин

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ А.Г. Остапенко

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины формирование у студентов основ знаний и приёмов работы с современным программным обеспечением для практического освоения принципов и методов обеспечения информационной безопасности, а также принципов, методологий и паттернов разработки современного безопасного программного обеспечения различных уровней интеграции.

1.2. Задачи освоения дисциплины

- формирование знаний и умений использования программных и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;
- способствование развитию навыков анализа защищенности и верификации программного обеспечения информационных систем;
- изучение процесса проверки инфраструктуры организации на наличие возможных уязвимостей сетевого периметра, виртуальной инфраструктуры, вызванных в том числе ошибками конфигурации, а также программного обеспечения и исходного кода приложений. Другими словами, при анализе защищенности проверяется безопасность различных информационных систем, как внутренних, так и внешних.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Программное обеспечение анализа защищенности информационных систем и сетей» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Программное обеспечение анализа защищенности информационных систем и сетей» направлен на формирование следующих компетенций:

ОПК-7.1. - Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем;

ОПК-7.3. - Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-7.1.	знать принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем
	уметь проводить технико-экономическое обосно-

	вание проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности
ОПК-7.3.	знать программные средства обеспечения защиты информации в программном обеспечении автоматизированных систем
	уметь использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем
	владеть владеет методами выявления уязвимости информационно-технологических ресурсов автоматизированных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Программное обеспечение анализа защищенности информационных 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)	144	72	72
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	72	36	36
Самостоятельная работа	144	72	72
Курсовой проект	+	+	
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет с оценкой	+	+	+
Общая трудоемкость: академические часы зач.ед.	 324 9	 144 4	 180 5

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	Лаб. зан.	СРС	Всего, час
1	Безопасность в DevOps	Методология DevOps и непрерывная интеграция. Непрерывная поставка Инфраструктура как сервис. Непрерывная безопасность. Безопасность на основе тестирования. Мониторинг и реагирование на атаки. Оценка рисков	12	12	24	48

		и усиление безопасности				
2	Уровень безопасности 1: защита веб-приложений	Защита и тестирование веб-приложений: атаки на сайты и безопасность контента; межсайтовые сценарии и политика безопасности контента; подделка межсайтовых запросов; кликджекинг и защита плавающих фреймов; Методы аутентификации пользователей: базовая HTTP-аутентификация; обслуживание паролей; поставщики идентификации; безопасность сессий и cookie-файлов; тестирование аутентификации. Управление зависимостями: golang-вендоринг; система управления пакетами Node.js	12	12	24	48
3	Уровень безопасности 2: защита облачной инфраструктуры	Уровень безопасности 2: защита облачной инфраструктуры. Защита и тестирование облачной инфраструктуры: deployer: Настройка deployer; Настройка уведомлений между Docker Hub и deployer; Тестирование инфраструктуры; Обновление среды invoicer Ограничение сетевого доступа: тестирование групп безопасности; налаживание доступа между группами безопасности. Создание безопасной точки доступа: Генерирование SSH-ключей; создание хоста-бастиона в EC2; Внедрение двухфакторной аутентификации с помощью SSH; Отправка уведомлений о доступе; Рассуждения о группах безопасности; Открытие доступа для групп безопасности. Управление доступом к базе данных: Анализ структуры базы данных; Роли и права доступа в PostgreSQL; Определение минимальных прав доступа для приложения invoicer Определение прав доступа в deployer	12	12	24	48
4	Уровень безопасности 3: защита каналов взаимодействия	Каналы взаимодействия: ранняя симметричная криптография; алгоритм Диффи - Хеллмана и RSA"; инфраструктуры открытых ключей; SSL и TLS. Обзор SSL/TLS: цепочка доверия; установление TLS-соединения; совершенная прямая секретность. Настройка приложений на использование HTTPS: получение сертификата AWS; получение сертификата Let's Encrypt; применение HTTP на AWS ELB. HTTPS: тестирование TLS; HSTS: строгая защита транспорта; HPKP: закрепление открытых ключей	12	12	24	48
5	Уровень безопасности 4: защита конвейера поставки	Распределение доступа к инфраструктуре управления кодом: управление	12	12	24	48

		правами доступа в GitHuЬ-организации; управление правами доступа в GitHub и Circle; подпись коммитов и меток с помощью Git; Управление доступом к хранилищу контейнеров: управление правами доступа в пределах Docker Hub и CircleCI; подписание контейнеров с помощью Docker Content Trust; Распределение прав доступа для управления инфраструктурой: Управление правами доступа с помощью ролей и политик AWS; распределение закрытых данных в системах среды эксплуатации				
6	Выявление аномалий и защита сервисов от атак	Выявление аномалий и защита сервисов от атак: сбор и хранение журналов; сбор данных журналов из систем и приложений; сбор журналов от систем; сбор журналов приложения; журналирование инфраструктуры; сбор журналов от GitHub. Потоковая передача событий журналов с помощью брокеров сообщений. Обработка событий потребителями журналов. Хранение и архивация журналов. Анализ журналов.	12	12	24	48
Итого			**72**	**72**	**144**	**288**

5.2 Перечень лабораторных работ

1. DevSecOps – методология использования инструментов безопасности в жизненном цикле DevOps.
2. Запуск и отладка контейнеров с использованием Dev Spaces.
3. Программное обеспечение тестирования защищенности веб-приложений транспортного уровня.
4. Программное обеспечение сканирования уязвимостей веб-приложений.
5. Выявление аномалий и защита сервисов от атак
6. Механизмы защиты фреймворков больших данных

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

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 9 семестре для очной формы обучения.

Примерная тематика курсового проекта: «Администрирование программное обеспечения защищённости корпоративной сети предприятия »

Задачи, решаемые при выполнении курсового проекта:

• Анализ информационных ресурсов и аудит информационных рисков предприятия

• Использование конкретных инструментов анализа защищённости (разработка, настройка, конфигурирование)

• формирование предложений по повышению эффективности систем защиты по результатам анализа и управления защищённости корпоративной сети предприятия.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

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
ОПК-7.1.	знать принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем	знает принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности	умеет проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-7.3.	знать программные средства обеспечения защиты информации в программном обеспечении автоматизированных систем	знает программные средства обеспечения защиты информации в программном обеспечении автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	умеет использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть владеет методами выявления уязвимости информационно-технологических ресурсов автоматизированных	владеет методами выявления уязвимости информационно-технологических ресурсов автоматизиро-	Выполнение работ в срок, предусмотренный в ра-	Невыполнение работ в срок, предусмотренный в

	систем	ванных систем	бочих программах	рабочих программах

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.**
ОПК-7.1.	знать принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь проводить технико-экономическое обоснование проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-7.3.	знать программные средства обеспечения защиты информации в программном обеспечении автоматизированных систем	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть владеет методами выявления уязвимости информационно-технологических ресурсов автоматизированных систем	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован 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) Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием

средств вычислительной техники, - это…

информационная система

информационная технология

автоматизированная система

информационно - телекоммуникационная сеть

2) Что из нижеперечисленного предназначено для борьбы с вирусным ПО?

межсетевые экраны

антивирусные системы

текстовые редакторы

маршрутизаторы

3) Что такое резидентный сторож?

программа, которая следит за изменениями файлов и дисковых секторов на компьютере

программа, осуществляющая несанкционированные действия в системе

программа в оперативной памяти компьютера, которая отслеживает действия остальных программ

программа, которая просматривает файлы с поисках сигнатур

4) Что такое программа-ревизор?

программа, которая следит за изменениями файлов и дисковых секторов на компьютере

программа, осуществляющая несанкционированные действия в системе

программа в оперативной памяти компьютера, которая отслеживает действия остальных программ

программа, которая просматривает файлы с поисках сигнатур

5) На применении каких программ основан метод обнаружения изменений?

сканеров

ревизоров

резидентных сторожей

межсетевых экранов

6) Недостатком какого метода обнаружения вирусов является большое количество ложных срабатываний антивирусных средств?

сканирование

эвристический анализ

обнаружение изменений

использование резидентных сторожей

7) Недостатком какого метода является невозможность обнаружения вируса в файлах, которые поступают в систему уже зараженными?

сканирование

эвристический анализ

обнаружение изменений

использование резидентных сторожей

8) Какой метод криптографического преобразования информации позволяет не только сохранять смысл хранящейся или передаваемой информа-

ции, но и сам факт хранения или передачи закрытой информации?

шифрование

стеганография

кодирование

сжатие

9) Что такое хэш?

результат преобразования входных данных произвольной длины в данныk фиксированной длины

результат преобразования входных данных произвольной длины в данные произвольной длины

результат преобразования входных данных фиксированной длины в данные произвольной длины

секретный ключ при ассиметричном шифровании

10) Как называется протокол управления групповой передачей данных в сетях, основанных на протоколе IP?

DNS

DHCP

OSPF

IGMP

7.2.2 Примерный перечень заданий для решения стандартных задач по сигнатурам вирусов и атак

по адресу отправителя трафика

на основе статистического анализа

с помощью поля ESP в составе передаваемых данных

1) Как называется определенные образцы вирусов и атак, с использованием которых IDP обнаруживает вторжения?

сертификаты

профили

сигнатуры

аутентификаторы

2) На каком принципе основано обнаружение неизвестных угроз в NetDefendOS IDP?

она не способна обнаруживать неизвестные угрозы

на основе статистического анализа

на использовании сертификатов открытых ключей

при создании вторжений за основу часто берется использовавшийся ранее код

3) Какие сигнатуры обладают самой высокой точностью?

сигнатуры предотвращения вторжений

сигнатуры обнаружения вторжения

политики сигнатур

4) Какие сигнатуры обнаруживают различные типы приложений трафика и могут применяться для блокировки определенных приложений?

сигнатуры предотвращения вторжений

сигнатуры обнаружения вторжения

политики сигнатур

5) Какие сигнатуры способны обнаруживать события, которые могут оказаться вторжениями, но не обязательно ими являются?

сигнатуры предотвращения вторжений

сигнатуры обнаружения вторжения

политики сигнатур

6) Какие сигнатуры могут обнаружить попытки перехвата управления и сканеры сети с максимальной точностью?

сигнатуры предотвращения вторжений

сигнатуры обнаружения вторжения

политики сигнатур

7) Какой механизм фильтрации интернет-трафика в межсетевых экранах NetDefend помогает защитить пользователей от потенциально опасного контента веб-страниц – объектов ActiveX, Java-скриптов и т.п.?

работа с активным содержимым

статическая фильтрация

динамическая фильтрация

8) Какой механизм фильтрации интернет-трафика в межсетевых экранах NetDefend предполагает то, что администратор вручную создает «черные» и «белые» списки сайтов?

работа с активным содержимым

статическая фильтрация

динамическая фильтрация

9) Как называется функция в межсетевых экранах D-Link, которая автоматически изолирует инфицированные компьютеры локальной сети и предотвращает распространение ими вредоносного трафика?

Port Forwarding

Virtual Servers

ZoneDefense

Host Monitoring

7.2.3 Примерный перечень заданий для решения прикладных задач

1) Чем системы IPS отличаются от систем IDS?

они способны обнаруживать атаки на сеть

они способны создавать оповещения в случае обнаружения сетевой атаки

они способны блокировать сетевую атаку

они способны осуществлять преобразование IP-адресов

2) Какие системы предназначены для обеспечения сетевого монито-

ринга, анализа, оповещения в случае обнаружения сетевой атаки, а также способны ее блокировать?

IDP
AV
WCF
IPS

3) В чем заключается отличие вторжений от вирусных атак?

вторжения обычно содержатся в отдельном загрузочном файле, который закачивается в систему пользователя

вторжения по характеру воздействия на атакуемую сеть могут быть как негативные, так и нейтральные

вторжения проявляются как образцы вируса, нацеленные на поиск путей преодоления механизмов обеспечения безопасности

вторжения могут осуществляться посредством сети

4) Система IDP предназначена для обнаружения…

дефектов в программном обеспечении
спама
вторжений
нарушения целостности передаваемых данных

5) Какая настройка в NetDefendOS IDP определяет действие, которое следует предпринять при обнаружении вторжения во входящем трафике?

Pipe Rules
Threshold Rules
IDP Rules
IP Rules

6) Какое действие рекомендуется выбрать для сигнатур обнаружения вторжений?

ignore
audit
protect

7) Какое действие рекомендуется выбрать для сигнатур предотвращения вторжений?

ignore
audit
protect

8) Какова длительность триального периода подписки для опциональных сервисов IPS, AV и WCF?

30 дней
30 дней
90 дней
12 месяцев

9) Какие системы предназначены для проверки сетевого трафика на вирусы, троянские и другие вредоносные программы?

IDP

AV
WCF
IPS

10) Какая система помогает администраторам осуществлять мониторинг, управление и контроль использования доступа пользователей локальной сети к интернет-ресурсам, разрешая/блокируя доступ к тем или иным Web-сайтам?

IDP
AV
WCF
IPS

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

Методология DevOps и непрерывная интеграция. Непрерывная поставка

Инфраструктура как сервис. Непрерывная безопасность. Безопасность на основе тестирования. Мониторинг и реагирование на атаки. Оценка рисков и усиление безопасности

Защита и тестирование веб-приложений: атаки на сайты и безопасность контента;

межсайтовые сценарии и политика безопасности контента; подделка межсайтовых запросов; кликджекинг и защита плавающих фреймов; Методы аутентификации пользователей: базовая HTTP-аутентификация; обслуживание паролей; поставщики идентификации; безопасность сессий и cookie-файлов; тестирование аутентификации. Управление зависимостями: golang-вендоринг; система управления пакетами Node.js

Уровень безопасности 2: защита облачной инфраструктуры. Защита и тестирование облачной инфраструктуры: deployer: Настройка deployer; Настройка уведомлений между Docker Hub и deployer; Тестирование инфраструктуры;

Обновление среды invoicer

Ограничение сетевого доступа: тестирование групп безопасности; налаживание доступа между группами безопасности. Создание безопасной точки доступа: Генерирование SSH-ключей; создание хоста-бастиона в EC2; Внедрение двухфакторной аутентификации с помощью SSH; Отправка уведомлений о доступе; Рассуждения о группах безопасности; Открытие доступа для групп безопасности. Управление доступом к базе данных: Анализ структуры базы данных; Роли и права доступа в PostgreSQL; Определение минимальных прав доступа для приложения invoicer

Определение прав доступа в deployer

Каналы взаимодействия: ранняя симметричная криптография; алгоритм Диффи - Хеллмана и RSA"; инфраструктуры открытых ключей; SSL и TLS.

Обзор SSL/TLS: цепочка доверия; установление TLS-соединения; совершенная прямая секретность. Настройка приложений на использование HTTPS: получение сертификата AWS; получение сертификата Let's Encrypt; применение HTTP на AWS ELB. HTTPS: тестирование TLS; HSTS: строгая защита транспорта; HPKP: закрепление открытых ключей

Распределение доступа к инфраструктуре управления кодом: управление правами доступа в GitHuЬ-организации; управление правами доступа в GitHub и Circle; подпись коммитов и меток с помощью Git; Управление доступом к хранилищу контейнеров: управление правами доступа в пределах Docker Hub и CircleCI; подписание контейнеров с помощью Docker Content Trust;

Распределение прав доступа для управления инфраструктурой: Управление правами доступа с помощью ролей и политик AWS; распределение закрытых данных в системах среды эксплуатации

Выявление аномалий и защита сервисов от атак: сбор и хранение журналов; сбор данных журналов из систем и приложений; сбор журналов от систем; сбор журналов приложения; журналирование инфраструктуры; сбор журналов от GitHub. Потоковая передача событий журналов с помощью брокеров сообщений. Обработка событий потребителями журналов. Хранение и архивация журналов. Анализ журналов.Укажите вопросы для экзамена

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	Безопасность в DevOps	ОПК-7.1., ОПК-7.3.	Тест, защита лабораторных работ, требования к курсовому проекту
2	Уровень безопасности 1: защита веб-приложений	ОПК-7.1., ОПК-7.3.	Тест, защита лабораторных работ, требования к курсовому проекту

3	Уровень безопасности 2: защита облачной инфраструктуры	ОПК-7.1., ОПК-7.3.	Тест, защита лабораторных работ, требования к курсовому проекту
4	Уровень безопасности 3: защита каналов взаимодействия	ОПК-7.1., ОПК-7.3.	Тест, защита лабораторных работ, требования к курсовому проекту
5	Уровень безопасности 4: защита конвейера поставки	ОПК-7.1., ОПК-7.3.	Тест, защита лабораторных работ, требования к курсовому проекту
6	Выявление аномалий и защита сервисов от атак	ОПК-7.1., ОПК-7.3.	Тест, защита лабораторных работ, требования к курсовому проекту

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.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : элек-

тронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249

Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182491

Дополнительная литература

Сети и телекоммуникации : учебное пособие для бакалавров / составители И. В. Винокуров. — Москва : Ай Пи Ар Медиа, 2022. — 105 с. — ISBN 978-5-4497-1418-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/115699.html

Краковский, Ю. М. Защита информации : учебное пособие / Ю. М. Краковский. — Ростов-на-Дону : Феникс, 2016. — 347 с. — ISBN 978-5-222-26911-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/102279

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://att.nica.ru

http://www.edu.ru/

http://window.edu.ru/window/library

http://www.intuit.ru/catalog/

http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp

https://cchgeu.ru/education/cafedras/kafsib/?docs

http://www.eios.vorstu.ru

http://e.lanbook.com/ (ЭБС Лань)

http://IPRbookshop.ru/ (ЭБСIPRbooks)

https://www.anti-malware.ru/security/security-check

Системы для анализа защищенности информационных систем

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 «Программное обеспечение анализа защищенности информационных систем и сетей» читаются лекции, проводятся лабораторные работы, выполняется курсовой проект.

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

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

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.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
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 зачетом с оценкой, 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
