Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

УТВЕРЖДАЮ
Декан факультета
факультета компьютерных технологий
(наименование факультета)
_____ Я.Ю. Григорьев
(подпись, ФИО)
«12» 03 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Тестирование на проникновение и анализ безопасности

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
5	*10*	*5*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой, КР	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

доцент, к.т.н. _____ _____

(должность, степень, ученое звание) (подпись) (ФИО)

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС _____ _____

(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа дисциплины «Тестирование на проникновение и анализ безопасности» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства науки и высшего образования Российской Федерации № 1457 от 26.11.2020, и основной профессиональной образовательной программы подготовки «Анализ безопасности информационных систем» по специальности 10.05.03 "Информационная безопасность автоматизированных систем".

Практическая подготовка реализуется на основе:
Профессиональный стандарт утвержденного приказом Министерства труда и социальной защиты от 15 сентября 2016 года N 522н №843 "Специалист по защите информации в автоматизированных системах" зарегистрированного в Министерстве юстиции Российской Федерации 28 сентября 2016 года, регистрационный N 43857. Обобщенная трудовая функция: B/01.6 Диагностика систем защиты информации автоматизированных систем
B/04.6 Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуацийB/06.6 Аудит защищенности информации в автоматизированных системах.

Изучаемые вопросы в рамках данной дисциплины носят исключительно образовательный характер.

Задачи дисциплины	Изучение основных механизмов проведения атак со стороны злоумышленников для более детальной диагностики систем защиты, обеспечения работоспособности в нештатных ситуациях и проведения аудита защищенности автоматизированных систем
Основные разделы дисциплины	Тестирование на проникновение Анализ безопасности

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины «Тестирование на проникновение и анализ безопасности»» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и индикаторы их достижения

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Общепрофессиональные		
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	**ОПК-13.1** Знает основные подходы к проведению анализа защищенности и тестирования систем защиты информации автоматизированных систем	Понимать взаимосвязь компонентов безопасности сети, сферу ответственности и влияния каждого из узлов; Знать и управлять уязвимыми местами сети; Самостоятельно обнаруживать уязвимости; Работать с инструментами взлома сетей и систем; Знать хакерские уловки для проникновения в системы и сети;
	ОПК-13.2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности и тестирования систем защиты информации;	Проводить тестирование любых компонентов сети на предмет взлома; Классифицировать рабочие станции по степени риска проведения

	проводить анализ уязвимостей систем защиты информации автоматизированных систем	атаки; Понимать ход мыслей злоумышленника; Оценить масштаб потенциально возможных атак; Противодействовать несанкционированному сбору информации о сети организации; Понимать стратегию злоумышленника; Оценивать защищенность платформ виртуализации и облачных вычислений;
	ОПК-13.3 Владеет навыками проведения анализа защищенности автоматизированных систем, тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем	Определять атаку на основе социальной инженерии; Изучить методы взлома беспроводной сети; Определить наиболее уязвимые места мобильных платформ; Противодействовать криптографическим атакам; Понимать процесс вторжения в систему; Проводить аудит систем безопасности; Противодействовать вторжению.

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина(модуль) «Тестирование на проникновение и анализ безопасности» изучается на 5 курсе в 10 семестре.

Дисциплина является базовой дисциплиной, входит в состав блока 1 «Дисциплины (модули)» и относится к обязательным дисциплинам.

Для освоения дисциплины необходимы знания, умения, навыки и (или) опыт практической деятельности, сформированные в процессе изучения дисциплин / практик: Анализ и защита веб-приложений, Анализ защищенности распределенных информационных систем.

Знания, умения и навыки, сформированные при подготовке к процедуре защиты и защите выпускной квалификационной работы.

Дисциплина «Тестирование на проникновение и анализ безопасности» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем выполнения лабораторных работ.

Дисциплина «Тестирование на проникновение и анализ безопасности» в рамках воспитательной работы направлена на формирование у обучающихся умения аргументировать, самостоятельно мыслить, развивает профессиональные умения, ответственности за выполнение учебно-производственных заданий.

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 зачетных единиц, 180 академических часов.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
Общая трудоемкость дисциплины	180
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	82
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	32
ИКР	2
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	48
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	98
Промежуточная аттестация обучающихся – Зачет с оценкой	-

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебной работы

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Тестирование на проникновение Ведение в этичный хакинг Обзор концепций информационной безопасности Угрозы информационной безопасности и векторы атак	16		24	49

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
Концепции хакинга Этапы хакинга Концепции этичного хаккинга Управление обеспечением информационной безопасности (ИБ) предприятия Модель угроз ИБ Законодательство и стандарты в области ИБ Предварительный сбор информации о цели Концепции изучения целевой системы Методологии сбора информации из открытых источников Средства сбора информации Меры противодействия утечкам информации Сканирование сети Обзор возможностей сканирования сети Средства сканирования Техники обнаружения узлов Техники обнаружения открытых портов и сервисов Анализ баннеров Техники уклонения от систем обнаружения вторжений Построение диаграмм топологии сети Подготовка прокси Инвентаризация ресурсов Концепции инвентаризации Инвентаризация NetBIOS Инвентаризация SNMP Инвентаризация LDAP Инвентаризация NTP и NFS Инвентаризация SMTP и DNS Другие техники инвентаризации Меры противодействия инвентаризации Анализ уязвимостей Концепции исследования уязвимостей Классификация уязвимостей Средства оценки уязвимостей Построение отчета о найденных уязвимостях Хакинг системыТемы Методология взлома системы Получение доступа Повышение привилегий Обеспечение доступа Сокрытие следов Вредоносный код Концепции работы вредоносного кода Концепции ATP Концепция работы троянов Концепция работы вирусов и червей Концепции работы вредоносного кода без использования файлов Анализ вредоносного кода Меры противодействия Антишпионский софт Снифферы Концепции сниффинга Техники сниффинга Инструменты сниффинга Меры противодействия сниффингу Техники обнаружения сниффинга Социальная инженерия Концепции социаль-				

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
ной инженерии Методы и техники социальной инженерии Угрозы инсайдеров Подмена личности в социальных сетях Кража персональных данных Меры противодействия социальной инженерии Отказ в обслуживании Концепции атак на доступность системы (отказ в обслуживании, Denial-of-Service) Распределенный отказ в обслуживании (DDoS атака)Методы и средства организации DoS/DDoS атак Бот-сети Изучение примера реализация DDoS атаки Инструменты проведения DoS атак Меры противодействия DoS атакам инструменты защиты от DoS Перехват сесии Концепции перехвата сессии Перехват на прикладном уровне Перехват на сетевом уровне Инструменты для перехвата сессий Меры противодействия перехвату сессий Обход IDS, брандмауэров и ханипотов Концепции IDS, брандмауэра и Honey Pot Системы IDS, брандмауэра и Honey Pot Уклонение от IDS Обход брандмауэра Инструменты обхода брандмауэра Обнаружение Honey Pot Противодействие обходу систем обнаружения Хакинг веб-серверов Концепции веб-серверов Типы атак на веб-серверы Методология атак Инструменты взлома веб-серверов Меры противодействия взлому веб-серверов Управление исправлениями Повышение безопасности веб-серверов Управление патчами Инструменты повышения безопасности веб-сервера Хакинг веб-приложений Концепции веб-приложений Угрозы веб-приложениям Методология атаки на веб-приложения Инструменты взлома веб-приложений Меры противодействия взлому веб-приложений Инструменты защиты веб-приложений				
Анализ безопасности SQL инъекции Концепции SQL инъекции Типы SQL инъекций Методология SQL инъекции Средства для выполнения SQL инъекции Сокрытие SQL инъекции от IDS Меры	16		24	49

Наименование разделов, тем и содержание материала	Виды учебной работы, включая самостоятельную работу обучающихся и трудоемкость (в часах)			
	Контактная работа преподавателя с обучающимися			СРС
	Лекции	Семинарские (практические занятия)	Лабораторные занятия	
противодействия SQL инъекции Хакинг беспроводных сетей Концепции построения беспроводных сетей Шифрование в беспроводных сетях Угрозы беспроводным сетям Методология взлома беспроводных сетей Инструменты хакинга беспроводных сетей Взлом Bluetooth Меры противодействия атакам на беспроводные сети Инструменты защиты беспроводных сетей Хакинг мобильных платформ Векторы атаки на мобильные платформы Взлом Android OS Взлом iOS Техники и инструменты джейлбрейка Управление мобильными устройствами и современные MDM-решения Инструменты и рекомендации по защите мобильных устройств Взлом IoT и OT Концепция “Интернета вещей” (IoT) Основные угрозы и векторы атак на IoT Методология взлома IoT Средства взлома IoT Методы и средства защиты IoT Концепция “Операционных технологий” (OT) Основные угрозы и векторы атак на OT Методология взлома OT Средства взлома OT Методы и средства защиты OT Облачные вычисления Концепции облачных вычислений Технологии контейнеров Бессерверные вычисления Основные угрозы ИБ при использовании облачных вычислений Атаки на среду виртуализации и облачные платформы Методы и средства защиты облачной инфраструктуры Криптография Концепции криптографии Алгоритмы шифрования Криптографические средства Инфраструктура публичных ключей Шифрование почты Шифрование диска Средства криптоанализа Меры противодействия крипто-атакам				
ИТОГО по дисциплине	**32**		**48**	**98**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руковод-

ствоваться следующим распределением часов на самостоятельную работу (таблица 4):

Таблица 4 – Рекомендуемое распределение часов на самостоятельную работу

Компоненты самостоятельной работы	Количество часов
Изучение теоретических разделов дисциплины	4
Подготовка к занятиям семинарского типа	4
Подготовка и оформление КР	36
	44

7 Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации представлен в Приложении 1.

Полный комплект контрольных заданий или иных материалов, необходимых для оценивания результатов обучения по дисциплине (модулю), практике хранится на кафедре-разработчике в бумажном и электронном виде.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1 1 Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. – М. : ФОРУМ : ИНФРА-М, 2014. – 416 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: **http://www.znanium.com/catalog.php**, ограниченный. – Загл. с экрана.

2 2 Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. – М. : ФОРУМ : ИНФРА-М, 2013. – 592 с. // ZNANIUM.COM : электронно-библиотечная система. – Режим доступа: **http://www.znanium.com/catalog.php**, ограниченный. – Загл. с экрана.

9.2 Дополнительная литература

1 Касперски, К. Техника сетевых атак. Т.1 / К. Касперски. – М.: Солон-Р, 2001. – 396с.

2 Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592с.

3 Курс CEHv11 от EC-Consil.

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Тестирование на проникновение и анализ безопасности» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и практических занятий.

Таблица 7 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Лабораторные занятие	Работа с автоматизированными рабочими местами.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к практическим занятиям, изучение теоретических разделов дисциплины, подготовка РГР.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Тестирование на проникновение и анализ безопасности» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление РГР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения и защиты РГР;

8.4 Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

1. Электронно-библиотечная система ZNANIUM.COM – **Ошибка! Недопустимый объект гиперссылки.**.
2. Консультант+

8.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. 1. Об информации, информационных технологиях и о защите информации: [Электронный ресурс] : федер. закон от 27 июля 2007 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
2. 2. О персональных данных : [Электронный ресурс] : федер. закон от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
3. 3. Сайт университета www.knastu.ru[Электронный ресурс]:. Раздел сотрудникам, документы СМК, режим доступа – свободный. Загл. с экрана
4. Научная электронная библиотека Elibrary http://elibrary.ru.

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразу-

мевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» по адресу https://student.knastu.ru. Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий.

8.6 Лицензионное программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Таблица 5 – Перечень используемого программного обеспечения

Наименование ПО	Реквизиты
Microsoft® Windows Professional 7 Russian	Лицензионный сертификат № 46243844 от 09.12.2009

9 Организационно-педагогические условия

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Язык обучения (преподавания) — русский. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на перезачет соответствующих дисциплин и профессиональных модулей, освоенных в процессе предшествующего обучения, который освобождает обучающегося от необходимости их повторного освоения.

9.1 Образовательные технологии

Учебный процесс при преподавании курса основывается на использовании традиционных, инновационных и информационных образовательных технологий. Традиционные образовательные технологии представлены лекциями и семинарскими (практическими) занятиями. Инновационные образовательные технологии используются в виде широкого применения активных и интерактивных форм проведения занятий. Информационные образовательные технологии реализуются путем активизации самостоятельной работы студентов в информационной образовательной среде.

9.2 Занятия лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов учебного плана.

На первой лекции лектор обязан предупредить студентов, применительно к какому базовому учебнику (учебникам, учебным пособиям) будет прочитан курс.

Лекционный курс должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньшей затрате времени, чем это требуется большинству студентов на самостоятельное изучение материала.

9.3 Занятия семинарского типа

Семинарские занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

Активность на семинарских занятиях оценивается по следующим критериям:

· ответы на вопросы, предлагаемые преподавателем;

· участие в дискуссиях;

· выполнение проектных и иных заданий;

· ассистирование преподавателю в проведении занятий.

Ответ должен быть аргументированным, развернутым, не односложным, содержать ссылки на источники.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

Оценивание заданий, выполненных на семинарском занятии, входит в накопленную оценку.

9.4 Самостоятельная работа обучающихся по дисциплине (модулю)

Самостоятельная работа студентов – это процесс активного, целенаправленного приобретения студентом новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности обучающегося.

Цели самостоятельной работы:

· систематизация и закрепление полученных теоретических знаний и практических умений студентов;

· углубление и расширение теоретических знаний;

· формирование умений использовать нормативную и справочную документацию, специальную литературу;

· развитие познавательных способностей, активности студентов, ответственности и организованности;

· формирование самостоятельности мышления, творческой инициативы, способностей к саморазвитию, самосовершенствованию и самореализации;

· развитие исследовательских умений и академических навыков.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, уровня сложности, конкретной тематики.

Технология организации самостоятельной работы студентов включает использование информационных и материально-технических ресурсов университета.

Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.

Студенты должны подходить к самостоятельной работе как к наиважнейшему средству закрепления и развития теоретических знаний, выработке единства взглядов на отдельные вопросы курса, приобретения определенных навыков и использования профессиональной литературы.

9.5 Методические указания для обучающихся по освоению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

При самостоятельной проработке курса обучающиеся должны:

· просматривать основные определения и факты;

· повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

· изучить рекомендованную литературу, составлять тезисы, аннотации и конспекты наиболее важных моментов;

· самостоятельно выполнять задания, аналогичные предлагаемым на занятиях;

· использовать для самопроверки материалы фонда оценочных средств.

Методические указания при работе над конспектом лекции

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций….и т.д.

Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к практическим занятиям

Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы необходимо стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале… и т.д.

Все лабораторные работы выполняются исключительно на виртуальных машинах или же в локальной вычислительной сети с обязательным информированием руководства факультета о проведении лабораторных работ.

10 Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю)

10.1 Учебно-лабораторное оборудование

Таблица 6 – Перечень оборудования лаборатории

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование
202/5	Лаборатория программно-аппаратных средств защиты информации	СЗИ НСД Secret Net, СЗИ НСД Dallas Lock, СЗИ НСД Страж NT, СЗИ НСД Щит РЖД, СЗИ НСД Аура ,СЗИ НСД Криптон ,СЗИ НСД Аккорд, ФИКС, Ревизор 1,2 как для операционных систем семейства Windows так и для Linux, Ревизор Сети 2.0, Анализатор сетевого траффика Астра,Агент инвентаризации сети,Сканер сетевой безопасности XSpider, Терьер, Secret Net Touch Memory Card, Криптон АМДЗ, Аккорд АМДЗ, КриптоПРО АРМ, ,CryptoPro CSP 3.6, VipNet firewall, Etoken PKI Client, Etoken, Ноутбук с Windows 7+проектор. 16 ПЭВМ на базе процессоров не ниже Intel Pentium IV

201/5	Лаборатория технических средств защиты информации	Модельное помещение для проведения измерений параметров различных полей

10.2 Технические и электронные средства обучения

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Лабораторные занятия

Для лабораторных занятий используется аудитория №_202_, оснащенная оборудованием, указанным в табл. 8:

Самостоятельная работа.

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде КнАГУ:

- читальный зал НТБ КнАГУ;
- компьютерные классы (ауд. 311 корпус № 5, ауд. 205 корпус № 5, ауд. 313 корпус № 5).

11 Иные сведения

Методические рекомендации по обучению лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины обучающимися с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Предполагаются специальные условия для получения образования обучающимися с ограниченными возможностями здоровья.

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

· в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);

· в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);

· методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

· письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);

· выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);

· устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине

Тестирование на проникновение и анализ безопасности

Направление подготовки	*10.05.03 "Информационная безопасность автоматизированных систем"*
Направленность (профиль) образовательной программы	*Анализ безопасности информационных систем*
Квалификация выпускника	*специалист по защите информации*
Год начала подготовки *(по учебному плану)*	*2021*
Форма обучения	*очная*
Технология обучения	*традиционная*

Курс	Семестр	Трудоемкость, з.е.
5	*10*	*5*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зачет с оценкой, КР	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

[1] В данном приложении представлены типовые оценочные средства. Полный комплект оценочных средств, включающий все варианты заданий (тестов, контрольных работ и др.), предлагаемых обучающемуся, хранится на кафедре в бумажном и электронном виде.

1 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и индикаторы их достижения

Код и наименование компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине
Общепрофессиональные		
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;	**ОПК-13.1** Знает основные подходы к проведению анализа защищенности и тестирования систем защиты информации автоматизированных систем	Понимать взаимосвязь компонентов безопасности сети, сферу ответственности и влияния каждого из узлов; Знать и управлять уязвимыми местами сети; Самостоятельно обнаруживать уязвимости; Работать с инструментами взлома сетей и систем; Знать хакерские уловки для проникновения в системы и сети;
	ОПК-13.2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности и тестирования систем защиты информации; проводить анализ уязвимостей систем защиты информации автоматизированных систем	Проводить тестирование любых компонентов сети на предмет взлома; Классифицировать рабочие станции по степени риска проведения атаки; Понимать ход мыслей злоумышленника; Оценить масштаб потенциально возможных атак; Противодействовать несанкционированному сбору информации о сети организации; Понимать стратегию злоумышленника; Оценивать защищенность платформ виртуализации и облачных вычислений;
	ОПК-13.3 Владеет навыками проведения анализа защищенности автоматизированных систем, тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем	Определять атаку на основе социальной инженерии; Изучить методы взлома беспроводной сети; Определить наиболее уязвимые места мобильных платформ; Противодействовать криптографическим атакам; Понимать процесс вторжения в систему; Проводить аудит систем безопасности; Противодействовать вторжению.

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства	Показатели оценки
1. Тестирование на проникновение 2. Анализ Безопасности	ОПК-13	Лабораторная работа 1-15	Знания и умения а так же навыки владения современными средствами обеспечения информационной безопасности
Вектора атак	ОПК-13	Курсовая работа	Знания в области оценки рисков и анализа инцидентов, защита от проникновения

2 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, представлены в виде технологической карты дисциплины (таблица 3).

Таблица 6 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
10 семестр Промежуточная аттестация в форме экзамена				
1	Лабораторная работа 1-19	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
Текущий контроль:			190 баллов	
ИТОГО:			190 баллов	
Критерии оценки результатов обучения по дисциплине: 0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине);				

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
65 – 74 % от максимально возможной суммы баллов – «удовлетворительно» (пороговый (минимальный) уровень); 75 – 84 % от максимально возможной суммы баллов – «хорошо» (средний уровень); 85 – 100 % от максимально возможной суммы баллов – «отлично» (высокий (максимальный) уровень)				

«10» семестр ***Промежуточная аттестация в форме*** «КР»
По результатам защиты курсового проекта (работы) выставляется оценка по 4-балльной шкале оценивания - оценка *«отлично»* выставляется студенту, если в работе содержатся элементы научного творчества и делаются самостоятельные выводы, достигнуты все результаты, указанные в задании, качество оформления отчета соответствует установленным в вузе требованиям и при защите студент проявил отличное владение материалом работы и способность аргументировано отвечать на поставленные вопросы по теме работы; - оценка *«хорошо»* выставляется студенту, если в работе достигнуты все результаты, указанные в задании, качество оформления отчета соответствует установленным в вузе требованиям и при защите студент проявил хорошее владение материалом работы и способность аргументировано отвечать на поставленные вопросы по теме работы; - оценка *«удовлетворительно»* выставляется студенту, если в работе достигнуты основные результаты, указанные в задании, качество оформления отчета в основном соответствует установленным в вузе требованиям и при защите студент проявил удовлетворительное владение материалом работы и способность отвечать на большинство поставленных вопросов по теме работы; - оценка *«неудовлетворительно»* выставляется студенту, если в работе не достигнуты основные результаты, указанные в задании или качество оформления отчета не соответствует установленным в вузе требованиям, или при защите студент проявил неудовлетворительное владение материалом работы и не смог ответить на большинство поставленных вопросов по теме работы.

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

Задания согласуются с преподавателем.

Лабораторная работа 1:

Сбор информации через поисковые системы; Сбор информации через веб-сервисы; Сбор информации через сайты социальных сетей; Сбор информации о сайте; Сбор информации через электронную почту; Сбор информации через сервис Whois; Сбор информации через DNS;Сбор информации о сети; Различные инструменты сбора инфорации;

Лабораторная работа 2:

Обнаружение узлов; Обнаружение открытых портов и запущенных сервисов; Определение ОС; Сканирование за IDS и файерволом;

Построение диаграммы сети; Различные инструменты сканирования сети.

Лабораторная работа 3:

Инвентаризация по протоколу NetBIOS Инвентаризация по протоколу SNMP Инвентаризация по протоколу LDAP Инвентаризация по протоколу NFS Инвентаризация по прото-

колу DNS Инвентаризация по протоколам RPC, SMB и FTP Различные инструменты инвентаризации.

Лабораторная работа 4:
Обнаружение уязвимостей с помощью Vulnerability Scoring Systems and Databases; Обнаружение уязвимостей с помощью Various Vulnerability Assessment Tools.

Лабораторная работа 5:
Получение доступа к системе; Повышение привилегий; Удаленный доступ и сокрытие вредоносной активности; Зачистка следов.

Лабораторная работа 6:
Получение доступа к системе с помощью трояна; Инфицирование системы вирусом; Статический анализ вредоносного кода; Динамический анализ вредоносного кода.

Лабораторная работа 7:
Активный сниффинг; Сниффинг сети и различные инструменты сниффинга; Обнаружение сниффинга сети;

Лабораторная работа 8:
Применение различных техник социальной инженерии; Обнаружение фишинговых атак; Аудит безопасности организации против фишинговых атак.

Лабораторная работа 9:
Проведение DDoS атак с использованием различных техник; Обнаружение и противодействие DoS/DDos атакам;

Лабораторная работа 10:
Перехват сессии; Обнаружение перехвата сессии.

Лабораторная работа 11:
Обнаружении вторжений различными средствами; Обход брандмауэра различными техниками;

Лабораторная работа 12:
Изучение веб-сервера; Взлом веб-сервера;

Лабораторная работа 13:
Изучение инфраструктуры веб-приложения Взлом веб-приложений;

Лабораторная работа 14:
SQL инъекция; Обнаружение уязвимостей к SQL инъекциями различными способами;

Лабораторная работа 15:
Анализ трафика беспроводной сети; Взлом беспроводной сети;

Лабораторная работа 16:
Взлом мобильной ОС Android; Средства защиты ОС Android;

Лабораторная работа 17:
Сбор информации различными средствами; Перехват и анализ трафика IoT устройства;

Лабораторная работа 18:
Сбор информации с помощью Various S3 Bucket Enumeration Tools; Эксплоит S3 Buckets; Эскалация привилегий и получение привилегированного доступа;

Лабораторная работа 19:
Шифрование с помощью различных средств; Создание самоподписаного сертификата; Шифрование почты; Шифрование диска; Криптоанализ с помощью различных средств

Примерная тематика курсовой работы

Пояснительная записка обязательно включает как теоретическое описание раздела, так и практическую часть, заключающуюся в демонстрации соответствующей техники.

1. Тестирование на проникновение и анализ безопасности сети ФКТ.
2. Сбор информации
3. Сканирование
4. Перечисление
5. Анализ уязвимостей
6. Хакинг системы
7. Трояны и другое вредоносное ПО
8. Снифферы
9. Социальная инженерия
10. Отказ в обслуживании
11. Перехват сеанса
12. Обход систем обнаружения вторжений, фаерволлов и систем-ловушек
13. Хакинг веб-серверов
14. Хакинг веб-приложений
15. SQL инъекции
16. Хакинг беспроводных сетей
17. Хакинг мобильных платформ
18. Хакинг интернета вещей и операционных технологий
19. Облачные вычисления
20. Криптография

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД