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

УТВЕРЖДАЮ

Декан
факультета компьютерных технологий
(наименование факультета)
Я.Ю. Григорьев
(подпись, ФИО)
«16» 05 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Анализ защищенности распределенных информационных систем

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.
4	*7*	*5*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зач_с_оц, КР	*Кафедра ИБАС - Информационная безопасность автоматизированных систем*

Комсомольск-на-Амуре 2021

Разработчик рабочей программы:

доцент, к. т. н. _____ _____ Ураев М.А.

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

СОГЛАСОВАНО:

Заведующий кафедрой

ИБАС _____ Лошманов А.Ю.

(наименование кафедры) (подпись) (ФИО)

1 Общие положения

Рабочая программа дисциплины «Анализ защищенности распределенных информационных систем» 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. Обобщенные трудовые функции: **B/01.6** Диагностика систем защиты информации автоматизированных систем, **B/04.6** Обеспечение работоспособности систем защиты информации при возникновении нештатных ситуаций, **B/06.6** Аудит защищенности информации в автоматизированных системах, **C/03.6** Анализ уязвимостей внедряемой системы защиты информации

Задачи дисциплины	Ознакомить студентов с зарубежной и отечественной нормативной и методической базой по проведению анализа защищенности распределенных информационных систем. Рассмотреть наиболее часто встречающиеся уязвимости в соответствии с OWASP Top 10.
Основные разделы / темы дисциплины	Нормативные и методические документы. Экспертиза документов и анализ защищенности информационной системы.. Анализ защищенности по OWASP Top 10

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

Процесс изучения дисциплины «Анализ защищенности распределенных информационных систем» направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 1):

Таблица 1 – Компетенции и планируемые результаты обучения по дисциплине

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	Знает основные подходы к проведению анализа защищенности и тестирования систем защиты информации автоматизированных систем
	ОПК-13.2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности и тестирования систем защиты информации; проводить анализ уязвимостей систем защиты информации ав-	Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности и тестирования систем защиты информации; проводить анализ уязвимостей систем защиты информа-

	томатизированных систем	ции автоматизированных систем
	ОПК-13.3 Владеет навыками проведения анализа защищенности автоматизированных систем, тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем	Владеет навыками проведения анализа защищенности автоматизированных систем, тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем	**ОПК-7.3..1** Знает виды и порядок проведения анализа защищенности автоматизированных систем	Знает виды и порядок проведения анализа защищенности автоматизированных систем
	ОПК-7.3..2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищённости автоматизированных систем	Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищённости автоматизированных систем
	ОПК-7.3..3 Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем	Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина(модуль) «Анализ защищенности распределенных информационных систем» изучается на 4 курсе в 7 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: информационная безопасность объектов критической информационной инфраструктуры, безопасность операционных систем.

Знания, умения и навыки, сформированные при изучении дисциплины «Анализ защищенности распределенных информационных систем», будут востребованы при изучении последующих дисциплин Анализ и защита веб приложений, анализ и защита мобильных приложений, тестирование на проникновение и анализ безопасности, низкоуровневый анализ машинного кода, форензика, подготовка к сдаче и сдача государственного экзамена, подготовка к процедуре защиты и защита выпускной квалификационной работы.

Дисциплина «Анализ защищенности распределенных информационных систем»» в рамках воспитательной работы направлена на развитие творчества, профессиональных умений, 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 ака-

демических 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	64
В том числе:	
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	32
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	32
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	114
Иная контактная работа	2
Промежуточная аттестация обучающихся – Зач_с_оц, КР	

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	
Нормативные и методические документы. Определение понятия защищенности АС. РД Гостехкомиссии России Методика построения плана анализа защищенности ISO 15408: Common Criteria for Information Technology Security. EvaluationISO	4		4	4

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	
17799: Code of Practice for Information Security Management Методика проведения анализа защищенности				
Экспертиза документов и анализ защищенности информационной системы. Экспертиза документов политики информационной безопасности на соответствие требованиям федерального законодательства и полномочных органов исполнительной власти РФ Эксперизa документов политики информационной безопасности, регламентирующих требования, порядок и правила применения мер и средств защиты информации, обеспечивающих защиту от актуальных угроз безопасности (в соответствии с моделью угроз и нарушителя). Эксперизу документов политики информационной безопасности, регламентирующих требования, порядок и правила применения мер и средств защиты информации, обеспечивающих защиту от актуальных угроз безопасности (в соответствии с моделью угроз и нарушителя). Анализ защищенности информационной системы	4		4	4
Анализ защищенности по OWASP Top 10 Концепции веб-сайтов, Инъекции, Взлом аутентификации и сеанса, Утечка важных данных, Внешние XML объекты, Нарушение контроля доступа Небезопасная конфигурация, Межсайтовый скриптинг (XSS), Небезопасная десериализация, Использование компонентов с известными уязвимостями, Отсут-	**24**		**24**	**106**

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	
ствие журналирования и мониторинга. Безопасность приложений за пределами OWASP Top 10. Использование реверс прокси на примере owasp ZAP. Анализ защищенности web приложений (XSS от Google, программы bug bounty, google dorks. Закрепление в сети, honeypots. Виды атак на мобильные устройства и облачные технологии. Атаки на блокчейн.				
ИТОГО по дисциплине	**32**		**32**	**114**

6 Внеаудиторная самостоятельная работа обучающихся по дисциплине (модулю)

При планировании самостоятельной работы студенту рекомендуется руководствоваться 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	106
Всего	114

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. В седьмом семестре проведение текущего и промежуточного контроля осуществляется с использованием элементов дистанционного обучения – курс «Анализ защищенности распределенных информационных систем» на портале ДО КнАГУ.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

8.1 Основная литература

1. Компьютерные сети: Учебное пособие [Электронный ресурс]/ Кузин А.В., Кузин Д.А. - 3-е изд., перераб. и доп. - 2015. - 192 с.: // ZNANIUM.COM: электронно-библиотечная система. - Режим доступа: http://znanium.com/catalog/product/536468, ограниченный, Загл. с экрана.

2. Сети связи и системы коммутации: Учебное пособие [Электронный ресурс]/ Паринов А.В., Ролдугин С.В., Мельник В.А. 2015. - 178 с.// ZNANIUM.COM: электронно-библиотечная система - Режим доступа: http://znanium.com/catalog/product/923309, ограниченный, Загл. с экрана.

3. Компьютерные сети: Учебное пособие [Электронный ресурс]/ Н.В. Максимов, И.И. Попов. - 3-е изд., испр. и доп. 2008. - 448 с.: ил.; // ZNANIUM.COM: электронно-библиотечная система - Режим доступа: http://znanium.com/catalog/product/163728, ограниченный, Загл. с экрана.

Дополнительная литература

1. Трещев И.А., Кожин И.А. Эмуляторы и симуляторы сетей ЭВМ : Для студентов технических специальностей / Издательские решения, 2020. — 166 с. ISBN 978-5-4493-9748-5

2. Трещев И.А., Вильдяйкин Г.Ф., Ватолина А.С. Технология сканирования на наличие уязвимостей / Издательские решения, 2020. — 136 с. ISBN 978-5-4498-9961-3

3. Трещев И.А. Сети и телекоммуникации : Для студентов / Издательские решения, 2020. — 140 с.ISBN 978-5-4493-9742-3

4. Трещев И.А., Григорьев Я.Ю. Проектирование и защита информационных систем / Издательские решения, 2020. — 86 с. ISBN 978-5-4498-9392-5

5. Трещев И.А., Кожин И.А., Вильдяйкин Г.Ф. Безопасность операционных систем : Часть 1. RAID, восстановление файлов, metasploit / Издательские решения, 2020. — 160 с. ISBN 978-5-4498-9599-8 (т. 1) ISBN 978-5-4498-9600-1

6. Трещев И.А., Кожин И. Безопасность вычислительных сетей : Практические аспекты / Издательские решения, 2020. — 126 с. ISBN 978-5-4498-9454-0

7. Трещев И.А. Анализ защищенности распределенных информационных систем : Для студентов технических специальностей / Издательские решения, 2020. — 102 с. ISBN 978-5-4493-9419-4

8. Трещев И.А., Кожин И.А., Вильдяйкин Г.Ф. Администрирование распределенных информационных систем : Часть 1. Администрирование информационных систем / Издательские решения, 2020. — 170 с. ISBN 978-5-4498-9912-5 (т. 1) ISBN 978-5-4498-9913-2

9. Трещев И.А., Ватолина А.С., Сериков В.А. Техника и технология атак злоумышленников в распределенных информационных системах. Часть 1 Рекогнасцировка, начала атак. / Издательские решения, 2021. — 160 с. ISBN 978-5-0055-1061-7 (т. 1) ISBN 978-5-0055-1062-4

10. Трещев И.А., Прокофьев С.В. Администрирование распределенных информационных систем. Часть 2 технологии информационных систем. / Издательские решения, 2021. — 228 с. ISBN 978-5-0055-0683-2 (т. 2) ISBN 978-5-4498-9913-2

11. Трещев И.А., Прокофьев С.В. Безопасность операционных систем. Часть 2 Операционные системы, уязвимости. / Издательские решения, 2021. — 262 с. ISBN 978-5-0055-0940-6 (т. 2) ISBN 978-5-4498-9600-1

8.2 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Анализ защищенности распределенных информационных

систем» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и лабораторных занятий. Так же используются элементы смешанного обучения – привлекаются дистанционные технологии (портал ДО КнАГУ).

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 лабораторным занятиям, изучение теоретических разделов дисциплины, подготовка КР.

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 «Анализ защищенности распределенных информационных систем» 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 КР.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

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

– выполнения и защиты КР;

Курсовая работа и отчеты по лабораторным работам должны быть оформлены в соответствии с требованиями внутренних нормативных документов ФГБОУ ВО КнАГУ.

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

1. Электронно-библиотечная система ZNANIUM.COM – http://www. znanium.com.
2. Консультант+

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

1. 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. Материалы данного курса (7 семестр) выложены на портал ДО КнАГУ и организация взаимодействия в рамках данной дисциплины проводится с привлечением дистанционных технологий.

8.5 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
Open Office или аналог	Свободно-распространяемое
Операционная система Kali Linux или аналог содержащая необходимые модули для анализа защищенности	Свободно-распространяемое
Операционная система Ubuntu или аналог	Свободно-распространяемое
Гипервизор Virtual Box или аналог	Свободно-распространяемое
Обозреватель Google Chrome или аналог	Свободно-распространяемое
Виртуальные машины согласно перечню из фондов оценочных средств для дисциплины	Свободно-распространяемое
Parrot OS или аналог	Свободно-распространяемое
Alien Vault OS или аналог	Свободно-распространяемое

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.

В данной дисциплине в рамках самостоятельной работы студенты выполняют одну курсовую работу состоящую из двух частей.

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.

1. 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.

2. Методические указания по самостоятельной работе над изучаемым материалом и при подготовке к лабораторным 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. Оформлять отчеты следует руководствуясь внутренними нормативными документами КнАГУ.

3. Методические указания по выполнению курсовой работы

Теоретическая часть курсовой работы выполняется по установленным темам с использованием практических материалов. К каждой теме курсовой работы рекомендуется примерный перечень узловых вопросов, список необходимой литературы. Излагая вопросы темы, следует строго придерживаться плана. Работа не должна представлять пересказ отдельных глав учебника или учебного пособия. Необходимо изложить собственные соображения по существу излагаемых вопросов, внести свои предложения. Общие положения должны быть подкреплены и пояснены кон-

кретными примерами. Излагаемый материал при необходимости следует проиллюстрировать таблицами, схемами, диаграммами.

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

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.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ[1]
по дисциплине

Анализ защищенности распределенных информационных систем

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.
4	*7*	*5*

Вид промежуточной аттестации	Обеспечивающее подразделение
Зач_с_оц, 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 планируемые результаты обучения по дисциплине

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	Знает основные подходы к проведению анализа защищенности и тестирования систем защиты информации автоматизированных систем
	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	Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищенности и тестирования систем защиты информации; проводить анализ уязвимостей систем защиты информации автоматизированных систем
	ОПК-13.3 Владеет навыками проведения анализа защищенности автоматизированных систем, тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем	Владеет навыками проведения анализа защищенности автоматизированных систем, тестирования систем защиты информации автоматизированных систем, проведения анализа уязвимостей систем защиты информации автоматизированных систем
ОПК-7.3. Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем	**ОПК-7.3..1** Знает виды и порядок проведения анализа защищенности автоматизированных систем	Знает виды и порядок проведения анализа защищенности автоматизированных систем
	ОПК-7.3..2 Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищённости автоматизированных систем	Умеет выбирать программное и аппаратное обеспечение для проведения анализа защищённости автоматизированных систем
	ОПК-7.3..3 Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем	Владеет навыками проведения анализа защищенности и верификации программного обеспечения автоматизированных систем

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	Формируемая компетенция	Наименование оценочного средства	Показатели оценки
Анализ защищенности АРМ без системы защиты, Анализ защищенности АРМ с системой защиты	ПК-3-2	Лабораторная работа 1	Умение составлять план тестирования Умение осуществлять анализ защищенности изолированных АРМ
Анализ защищенности распределенной информационной системы построенной на сервере безопасности Secret Net Studio. Анализ защищенности распределенной информационной системы построенной на сервере безопасности Dallas Lock	ПК-3-2	Лабораторная работа 2	Умение составлять план анализа защищенности распределенных информационных систем Умение проводить анализ защищенности доменов безопасности
Уязвимости по OWASP Top 10	ПК-27-4	Курсовая работа	Умение осуществлять поиск уязвимостей в распределенных информационных системах

Промежуточная аттестация в седьмом семестре проводится в форме зачета с оценкой.

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 3 – Технологическая карта

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
_____ 7 семестр Промежуточная аттестация в форме зачета с оценкой				
1	Лабораторная работа 1 № 1	В течение семестра	25 баллов	25 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения в рамках освоенного учебного материала. 20 балла - студент выполнил задание, с небольшими неточностями. Показал хорошие знания, навыки и умения в рамках освоенного учебного материала. 15 балла - студент выполнил задание с существенными неточно-

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				стями. Показал удовлетворительные знания, навыки и умения в рамках освоенного учебного материала. 8 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Лабораторная работа № 2	В течение семестра	25 баллов	25 баллов - студент правильно выполнил задание. Показал отличные знания, навыки и умения в рамках освоенного учебного материала. 20 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания, навыки и умения в рамках освоенного учебного материала. 15 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания, навыки и умения в рамках освоенного учебного материала. 8 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
ИТОГО:		-	50 баллов	-

Критерии оценки результатов обучения по дисциплине:
0 – 64 % от максимально возможной суммы баллов – «неудовлетворительно» (недостаточный уровень для промежуточной аттестации по дисциплине);
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)
Дополнительно студент должен освоить курс «Анализ защищенности распределенных информационных систем» на портале ДО ФГБОУ ВО КнАГУ

«7» 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

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
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 для дисциплины представлены на портале ДО КнАГУ.

Лабораторная работа №1

Необходимо выбрать АРМ и согласовать его с преподавателем. Для каждого задания смоделировать инцидент безопасности и проверить его с помощью сканера.

Задание 1.

Необходимо для произвольного АРМ из состава лабораторий, на котором отсутствует установленная и настроенная система защиты информации, составить план анализа и провести анализ защищенности с использованием сканера СКАНЕР-ВС, OpenVAS, сканер от Microsoft, AlienVault. При этом допустимо провести нарушение периметра сети (подключить ноутбук с запущенным сканером в одну подсеть с исследуемым хостом и присвоить себе IP адрес из диапазона 192.168.1.0/24). Отчет анализатора вставить в отчет по лабораторной.

Задание 2

Необходимо для произвольного АРМ из состава лабораторий, на котором присутствует установленная и настроенная система защиты информации, составить план анализа и провести анализ защищенности с использованием сканера СКАНЕР-ВС, OpenVAS, сканер от Microsoft, AlienVault. При этом допустимо провести нарушение периметра сети (подключить ноутбук с запущенным сканером в одну подсеть с исследуемым хостом и присвоить себе IP адрес из диапазона 192.168.1.0/24). Отчет анализатора вставить в отчет по лабораторной.

Лабораторная работа 2

Необходимо выбрать АРМ и согласовать его с преподавателем. Для каждого задания смоделировать инцидент безопасности и проверить его с помощью сканера.

Задание 1

В распределенной информационной системе используется домен безопасности и несклько компьютеров входящих в домен на основе DL (настройку проводит студент). Необходимо в соответствии с вариантом составить план тестирования и провести анализ с использованием сканера СКАНЕР-ВС, OpenVAS, сканер от Microsoft, AlienVault.

Задание 2

В распределенной информационной системе используется домен безопасности и несколько компьютеров входящих в домен на основе SNS (настройку проводит студент). Необходимо в соответствии с вариантом составить план тестирования и провести анализ с использованием сканера СКАНЕР-ВС, OpenVAS, сканер от Microsoft, AlienVault.

Варианты.

	МЭ	СОВ	Хосты
1	+	+	1
2	+	+	2
3	+	+	3
4	+	+	4
5	+	+	5
6	+	-	1
7	+	-	2
8	+	-	3
9	+	-	4
10	+	-	5
11	-	+	1
12	-	+	2
13	-	+	3
14	-	+	4
15	-	+	5

Обобщенная тематика и варианты КР.

Студенты разбиваются на пары в соответствии со своим вариантом и используют в работе соответствующую виртуальную машину. Допускается работать с виртуальной машиной расположенной не в ФГБОУ ВО КнАГУ. При необходимости установления вариантов для большего количества студентов данные варианты устанавливаются преподавателем.

№	Пара	Машина
1	1	Web For Pentester II
2	2	DVWA
3	3	Metasploitable
4	3	Metasploitable
5	5	Beebox
6	4	Web For Pentester I
7	5	Beebox
8	4	Web For Pentester I
9	2	DVWA
10	1	Web For Pentester II
11	6	bWAPP
12	6	bWAPP
13	7	Webgoat
14	7	Webgoat

Адреса в сети факультета компьютерных технологий представлены ниже для соответствующих виртуальных машин. В виртуальной лаборатории анализа защищенности

распределенных информационных систем по необходимости могут быть развернуты дополнительные площадки для работы.
Web For Pentester I
http://192.168.249.76/
Web For Pentester II
http://192.168.249.77/
DVWA
http://192.168.249.103/dvwa
Metasploitable
http://192.168.249.104/
Beebox
http://192.168.249.106/

Курсовая работа
Раздел 1

Задания для выполнения КР представлены в соответствующем модуле на портале ДО курс «Анализ защищенности распределенных информационных систем» в разделе «Итоговая работа». Необходимо для данных виртуальных машин реализовать соответствующие уязвимости на всех уровнях сложности.
Web For Pentester I

Номер пары(студент в паре)	Directory traversal	File include	Code injection	Command injection	LDAP attacks	File upload	XML related attacks	SQL-инъекции	XSS атаки
1(1)					+	+	+	+	+
1(2)	+	+	+	+					

Web For Pentester II

Номер пары(студент в паре)	Authorization	Mass Assignment	Randomness Issues	Authentication	MongoDB injection	SQL injections	Captcha
2(1)	+	+	+				
2(2)				+	+	+	+

DVWA

Номер пары(студент в паре)	Command Injection	File Inclusion	SQL Injection	SQL Injection (Blind)	XSS (Stored)	CSP Bypass	JavaScript	Bruteforce	CSRF	File Upload	Insecure CAPTCHA	Weak Session IDs	XSS (DOM)	XSS (Reflected)
3(1)	+	+	+	+	+	+	+							
3(2)								+	+	+	+	+	+	+

Metasploitable

Но-	Inj	Bro-	Inse	Cr	Securit	X	Inse	Fai	Unv	Mutilli	Mutillidae_Insu

мер пары(студент в паре)	ection	ken Authen-tication and Session Man-agement	cure Direct Object Refe-rences	oss Site Request Forgery	y Miscon figuration	SS	cure Direct Object Refe-rences	lure to Re-strict URL Access	alidated Redirects and Forwards	dae_Crypto	fficientTransportLayer
4(1)	+	+	+	+	+						
4(2)						+	+	+	+	+	+

Beebox

Номер пары(студент в паре)	Injection	XSS	Broken Auth	SensitiveData Exposure	Missing Functional Level Access Control	SecurityMisconfiguration	Cross-Site Request Forgery	Using Known Vulnerable Components	Unvalidated Redirects & Forwards
5(1)	+	+	+	+	+				
5(2)						+	+	+	+

Выполнить отчет о проделанной работе. Оформление должно быть выполнено в соответствии с РД ФГБОУ ВО «КнАГУ» «Текстовые студенческие работы. Правила оформления».

Раздел 2

Задания для выполнения КР представлены в соответствующем модуле на портале ДО курс «Анализ защищенности распределенных информационных систем» в разделе «Итоговая работа».

Необходимо для данных виртуальных машин реализовать соответствующие уязвимости на всех уровнях сложности.

Web For Pentester I

Номер пары(студент в паре)	Directory traversal	File include	Code injection	Command injection	LDAP attacks	File upload	XML related attacks	SQL-инъекции	XSS атаки
2(1)	+	+	+	+					
2(2)					+	+	+	+	+

Web For Pentester II

Номер пары(студент в паре)	Authorization	Mass Assignment	Randomness Issues	Authentication	MongoDB injection	SQL injections	Captcha

1(1)				+	+	+	+
1(2)	+	+	+				

DVWA

Номер пары(студент в паре)	Command Injection	File Inclusion	SQL Injection	SQL Injection (Blind)	XSS (Stored)	CSP Bypass	JavaScript	Bruteforce	CSRF	File Upload	Insecure CAPTCHA	Weak Session IDs	XSS (DOM)	XSS (Reflected)
5(1)								+	+	+	+	+	+	+
5(2)	+	+	+	+	+	+	+							

Metasploitable

Номер пары(студент в паре)	Injection	Broken Authentication and Session Management	Insecure Direct Object References	Cross Site Request Forgery	Security Misconfiguration	XSS	Insecure Direct Object References	Failure to Restrict URL Access	Unvalidated Redirects and Forwards	Mutillidae_Crypto	Mutillidae_InsufficientTransportLayer
3(1)						+	+	+	+	+	+
3(2)	+	+	+	+	+						

Beebox

Номер пары(студент в паре)	Injection	XSS	Broken Auth	SensitiveData Exposure	Missing Functional Level Access Control	SecurityMisconfiguration	Cross-Site Request Forgery	Using Known Vulnerable Components	Unvalidated Redirects & Forwards
4(1)						+	+	+	+
4(2)	+	+	+	+	+				

Выполнить отчет о проделанной работе. Оформление должно быть выполнено в соответствии с РД ФГБОУ ВО «КнАГУ» «Текстовые студенческие работы. Правила оформления». Описать механизмы защиты которые можно применить для закрытия данных уязвимостей. Теоретический раздел должен содержать описание по OWASP Top 10.
Дополнительно необходимо установить любой honeypot и осуществить на него атаку.

Лист регистрации изменений к РПД

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