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
Защита от хакерских угроз

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*	*4*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*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 «Защита от хакерских угроз» 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: **A/03.5** Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем, **D/04.7** Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем

.

Задачи дисциплины	Изучение основных механизмов защиты информации от потенциальных действий злоумышленников направленных на нарушение конфиденциальности, целостности и доступности информации в автоматизированных системах.
Основные разделы дисциплины	Защита предприятия от хакерских угроз

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

Процесс изучения дисциплины ««Наименование_дисциплины»» 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-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем	**ОПК-11.1** Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности автоматизированных систем	Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности автоматизированных систем
	ОПК-11.2 Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем	Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем

	ОПК-11.3 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы	Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина(модуль) «Защита от хакерских угроз» 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: Программно-аппаратные средства защиты инфомации, Разработка и эксплуатация автоматизированных систем в защищенном исполнении.

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

Дисциплина «Защита от хакерских угроз» частично реализуется в форме практической подготовки. Практическая подготовка организуется путем выполнения лабораторных работ.

Дисциплина «Защита от хакерских угроз» 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 3 зачетные единицы, 108 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	108
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
ИКР	1
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	44
Промежуточная аттестация обучающихся – Экзамен	35

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	
Защита предприятия от хакерских угроз Сетевые атаки и методы защиты Терминология в сфере атак на сетевую безопасность. Примеры атак сетевого уровня.	32		32	44

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	
Примеры атак уровня приложений Примеры атак социальной инженерии. Примеры атак на почтовые сообщения.Примеры специфических атак на мобильные устройства. Примеры атак на облачные сервисы. Примеры атак на беспроводные сети. Методология взлома и фреймворки Цели, результаты и преграды при построении сетевой защиты. Стратегия непрерывной/адаптивной безопасности Стратегия защиты в глубину Управление сетевой безопасностью Соответствия требованиям регуляторов. Правовое поле, международные законы и акты. Проектирование и построение политик безопасности Организация обучающего тренинга по основам безопасности. Административные меры обеспечения безопасности. Техническое обеспечение безопасности сети Контроль доступа: терминология, принципы, модели. Контроль доступа в современном мире распределенных вычислений и мобильных устройств. Управление идентификацией и доступом (IAM): идентификация, аутентификация, авторизация и учет. Криптографические инструменты. Криптографические алгоритмы. Сегментирование сетей. Решения по обеспечению безопасности сети. Протоколы безопасного сетевого взаимодействия Обеспечение безопасности периметра сети Межсетевые экраны: преимущества и недостатки. Типы межсетевых экранов и их использование. Топологии сети и размещение межсетевого экрана. Сравнение аппаратного/программного, хостового/сетевого, внутреннего/внешнего межсетевых экранов. Выбор межсетевого экрана в зависимости от трафика. Процесс внедрения и развертывание межсетевых экранов. Рекомендации по внедрению межсетевых экранов Администрирование межсетевого экрана.				

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	
Системы предупреждения вторжений (IDS): роль, возможности, ограничения и рекомендации по развертыванию. Классификация IDS/IPS. Компоненты IDS. Развертывание локальных и сетевых IDS. Работа с ложноположительными срабатываниями и отсутствием оповещений об атаке. Выбор решений IDS. Возможности обнаружения вторжений сетевых и хостовых IDS Рекомендации по безопасности для коммутаторов и маршрутизаторов. Модель нулевого доверия в программно-определяемом периметре (SDP) Обеспечение безопасности ОС Windows Вопросы безопасности ОС Windows Компоненты безопасности Windows Инструменты управления безопасностью Windows Настройка параметров безопасности Windows Управление аккаунтами и паролями в Windows Управление патчами Windows Управление доступом пользователей Техники «заморозки» Windows Рекомендации мирового сообщества по вопросам безопасности Безопасность сетевых сервисов и протоколов Обеспечение безопасности ОС Linux Вопросы безопасности ОС Linux Установка и управление патчами Linux Техники «заморозки» Linux Управление аккаунтами и паролями в Linux Сетевая безопасность и удаленных доступ в Linux Инструменты управления безопасностью и фреймвороки Linux Обеспечение безопасности мобильных устройств Политики работы с мобильными устройствами в организации Риски и рекомендации по использованию мобильных устройств в организации Управление безопасностью мобильных устройств на корпоративном уровне Рекомендации мирового сообщества и руководства по обеспечению безопасности мобильных устройств Инструменты обеспечения				

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	
безопасности для Android Инструменты обеспечения безопасности для iOS Обеспечение безопасности устройств IoT IoT устройства: области применения, потребности и приложения Экосистема и модели коммуникаций IoT устройств Вызовы и риски безопасности при использовании IoT устройств Безопасность для IoT устройств Меры по обеспечению безопасности в средах с IoT устройствами Рекомендации мирового сообщества и средства обеспечения безопасности для IoT устройств Стандарты, инициативы и организационные усилия при обеспечении безопасности IoT устройств Управление безопасностью приложений Белые и черные списки для приложений Внедрение песочниц для приложений Управление патчами приложений Фаерволы для веб-приложений Безопасность данных Почему важно обеспечить безопасность данных Внедрение управления доступом к данным Шифрование данных на носителе Шифрование данных при передаче Концепции маскировки данных Резервное копирование и восстановление Концепции повреждения данных Обеспечение безопасности корпоративных виртуальных сетей Управление безопасностью в среде виртуализации Базовые концепции виртуализации Безопасность виртуальных сетей Безопасность программно-определяемых сетей (SDN) Безопасность виртуализации сетевых функций (NFV) Безопасность виртуальных машин Рекомендации мирового сообщества и руководства по безопасности при использовании контейнеров Рекомендации мирового сообщества и руководства по безопасности при работе с Docker Обеспечение безопасности облачных сетей Основы облачных вычислений Безопасность				

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	
облаков Выбор решения для обеспечения безопасности перед подключением облачного сервиса Безопасность облаков Amazon Безопасность в облаке Google Рекомендации мирового сообщества и инструменты обеспечения безопасности облака Мониторинг и анализ сетевых журналов Краткий обзор современных технологий беспроводных сетей Угрозы безопасности беспроводных сетей и основные виды атак на них Методы и средства защиты беспроводных сетей Аудит безопасности беспроводных сетей Системы обнаружения и предупреждения вторжений в беспроводные сети (WIDS/WIPS) Настройки безопасности точек доступа и беспроводных маршрутизаторов Реакция на инцидент и расследование инцидента Организация процесса управления инцидентами информационной безопасности Роли и задачи участников процесса обработки инцидента информационной безопасности Что делать и не делать при обнаружении инцидента информационной безопасности Последовательность действий при обработке инцидента информационной безопасности Процесс расследования инцидента информационной безопасности Непрерывность бизнеса и восстановление после сбоя Концепции непрерывности бизнеса и восстановления после сбоя Действия для обеспечения непрерывности бизнеса и восстановления после сбоя План обеспечения непрерывности бизнеса и план восстановления после сбоя Стандарты обеспечения непрерывности бизнеса и восстановления после сбоя Оценка риска и управление рисками Концепции управления рисками Программы управления рисками Фреймворки для управления рисками Программы управления уязвимостями Сканирование и оценка уязвимо-				

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	
стей Оценка угроз и анализ поверхности атаки Анализ поверхности атаки Определение и визуализация поверхности атаки Обнаружения индикаторов воздействия (IoE) Проведение симуляции атаки Уменьшение поверхности атаки Анализ поверхности атаки для облаков и IoT Противодействие угрозам с помощью разведки кибер-угроз (Threat Intelligence) Роль разведки кибер-угроз в организации защиты сети Различные типы разведки кибер-угроз Индикаторы разведки кибер-угроз: IoC и AoC Уровни разведки кибер-угроз Использование разведки кибер-угроз для организации проактивной защиты				
ИТОГО по дисциплине	**32**		**32**	**44**

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 РГР	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 CND v2 от EC-Consil.

8.3 Методические указания для студентов по освоению дисциплины

Обучение дисциплине «Защита от хакерских угроз» 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 «Защита от хакерских угроз» 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 подразумевает 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

OllyDbg (свободнораспространяемый) http://www.ollydbg.de/

MASM (свободнораспространяемый) https://www.microsoft.com/en-us/download/details.aspx?id=12654

Для разработки программ рекомендуется использовать текстовый процессор

Notepad++(свободнораспространяемый) (**https://notepad-plus-plus.org**). Для отладки программ, написанных для 32-х или 64-х битных архитектур рекомендуется использовать GDB(свободнораспространяемый) (**https://www.gnu.org/software/gdb/**). Для эмулирования операционной системы MS-DOS рекомендуется использовать эмулятор DosBox(свободнораспространяемый) (**https://www.dosbox.com**).

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.

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

Защита от хакерских угроз

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*	*4*

Вид промежуточной аттестации	Обеспечивающее подразделение
Экзамен	*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-11 Способен разрабатывать компоненты систем защиты информации автоматизированных систем	**ОПК-11.1** Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности автоматизированных систем	Знает программно-аппаратные средства, используемые в качестве компонентов систем защиты информации в программном обеспечении автоматизированных систем; методы проектирования решений по обеспечению безопасности автоматизированных систем
	ОПК-11.2 Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем	Умеет проектировать защищенные распределенные информационные системы и компоненты систем защиты информации автоматизированных систем
	ОПК-11.3 Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы	Владеет навыками разработки компонентов систем защиты информации автоматизированных систем и защищенных распределенные информационные системы

Таблица 2 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Код контролируемой компетенции**	**Наименование оценочного средства**	**Показатели оценки**
1. Защита предприятия от хакерских угроз	ОПК-11	Лабораторная работа 1-15	Знания и умения а так же навыки владения современными средствами обеспечения информационной безопасности
Разработка игровых приложений	ОПК-11	Расчетно-	Знания в области оценки

на языке низкого уровня		графическая работа	рисков и анализа инцидентов

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 1-15	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.
3	Расчетно-графическая работа	В течение семестра	30 баллов	15 баллов - студент правильно выполнил задания. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы на защите. 10 баллов - студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов на защите. 5 баллов - студент выполнил задания с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополни-

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
				тельные вопросы на защите было допущено много неточностей. 0 баллов - при выполнении задания студент продемонстрировал недостаточный уровень владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы на защите было допущено множество неточностей.
Текущий контроль:			180 баллов	
ИТОГО:			180 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)				

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

Работа SQL-инъекций;Работа XSS-атак;Атака сканирования сети;Атака на пароли методом грубой силы;

Лабораторная работа 2

Внедрение политики паролей через Групповые политики Windows;Политика паролей в ОС Linux;Мониторинг активности удаленных систем.

Лабораторная работа 3

Контроль доступа на базе ролей с помощью JEA;Контроль доступа на базе ролей с помощью Windows Admin Center;Подключение прокси-сервера Squid; Подключение VPN с помощью OpenVPN; Подключение VPN с помощью SoftEther VPN;

Лабораторная работа 4

Блокировка нежелательных веб-сайтов с помощью pfSense;Блокировка небезопасный портов с помощью pfSense;Блокировка внутреннего FTP-сервера с помощью Smoothwall Firewall;Создание правил блокировки доступа на основе IP-адреса;Настройка Windows Firewall;Настройка iptables;Настройка IDS Snort;Настройка IDS Suricata;Настройка IDA Bro (Zeek);Настройка Wazuh HIDS.

Лабораторная работа 5
Базовое администрирование сети с помощью утилит командной строки;Настройки безопасности для общих папок в AD DS;Анализ настроек безопасности с помощью Microsoft Security Compliance Toolkit;Удаленное управление патчами с помощью BatchPatch;Удаленное управление патчами с помощью ManageEngine Patch Manager Plus; Делегирование административных привилегий с помощью Delegation of Control Wizard;Повышение безопасности паролей локальных администраторов с помощью LAPS.

Лабораторная работа 6
Рекомендации мирового сообщества по обеспечению безопасности Linux;Мандатный контроль доступа с помощью AppArmor;Аудит безопасности и «заморозка» системы с помощью Lynis.По окончании этого модуля слушатели смогут:Устанавливать и управлять патчами Linux;Управлять аккаунтами и паролями в Linux; Выполнять аудит безопасности Linux.

Лабораторная работа 7
Безопасность корпоративных мобильных устройств с помощью Miradore MDM Solution; Безопасность корпоративных мобильных устройств с помощью Comodo MDM Solution.

Лабораторная работа 8
Обеспечение безопасности коммуникаций IoT с помощью TLS/SSL.

Лабораторная работа 9
Настройка белого списка приложений с помощью AppLocker; Настройка белого списка приложений с помощью Software Restriction Policy; Обеспечение безопасности приложений с помощью Firejail Sandbox; Противодействие атакам на уровне приложений с помощью Microsoft URL Scan Web Application Firewall.

Лабораторная работа 10
Шифрование данных с помощью VeraCript; Шифрование базы на SQL сервере с помощью метода прозрачного шифрования базы;Настройка непрерывного шифрования в SQL сервере;Шифрование данных при передаче по SSL;Шифрование почтовых сообщений при помощи PGP; Внедрение резервного копирования с помощью AIMEI Backupper Standard;
Лабораторная работа 11
Восстановление файлов с помощью EaseUS Data Recovery Wizard; Восстановлении файлов с помощью Kernal for Windows Data Recovery Tool; Восстановление разделов с помощью MiniTool Power Data Recovery Tool.

Лабораторная работа 12
Аудит безопасности хоста Docker с помощью Docker Bench Security Tool; Обеспечение безопасной передачи между свичем и контроллером SDN с помощью SSL.

Лабораторная работа 13
Проверка подлинности и контроль доступа в AWS;Службы управления ключами;Безопасность хранилища AWS.

Лабораторная работа 14
VНастройка, просмотр и анализ логов Windows Event Viewer; Настройка, просмотр и анализ логов IIS; Настройка, просмотр и анализ логов с помощью Splunk; Обнаружение подозрительной активности с помощью SIEM.

Лабораторная работа 15

Обработка тикетов с помощью OSSIM.

Примерная тематика расчетно-графической работы

Организация непрерывности бизнеса и восстановления после сбоя с помощью NLB. Управление уязвимостями с помощью OSSIM; Управление уязвимостями с помощью Nessus; Использование GFI LanGuard; Аудит сетевой безопасности с помощью NSAuditor; Сканирование уязвимостей с помощью OWASP ZAP.

Перечень вопросов на экзамен

1. Сетевые атаки и стратегии защиты
2. Административные меры безопасности
3. Технические меры безопасности
4. Безопасность сетевого периметра
5. Безопасность хостов Windows
6. Безопасность хостов Linux
7. Безопасность мобильных устройств
8. Безопасность IoT устройств
9. Безопасность приложений
10. Безопасность данных
11. Защита виртуальных сетей
12. Безопасность облачных вычислений
13. Wi-Fi. Защита беспроводных сетей
14. Мониторинг и анализ сетевого трафика
15. Мониторинг и анализ сетевых журналов
16. Управление реагированием на инциденты
17. Непрерывность бизнеса и восстановление после сбоев
18. Управление рисками
19. Определение угроз и анализ поверхности атаки
20. Анализ киберугроз

Лист регистрации изменений к РПД

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