МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Проректор по учебной работе

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

_____ Василенко В.Н.

«25» мая 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность открытых систем
(наименование в соответствии с РУП)

Специальность

10.05.03 Информационная безопасность автоматизированных систем
(шифр и наименование направления подготовки/специальности)

Специализация

Безопасность открытых информационных систем
(наименование профиля/специализации)

Квалификация выпускника
специалист по защите информации
(в соответствии с Приказом Министерства образования и науки РФ от 12 сентября 2013 г. N 1061 "Об утверждении перечней специальностей и направлений подготовки высшего образования" (с изменениями и дополнениями)

1. Цели и задачи дисциплины

Целью освоения дисциплины «Информационная безопасность открытых систем» является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

- 06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах).

Дисциплина направлена на решение задач профессиональной деятельности научно-исследовательского, проектного, контрольно-аналитического, эксплуатационного типов.

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИД1$_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования
			ИД2$_{опк-10}$ – владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности
2	ОПК-13	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИД1$_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем
			ИД2$_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах
3	ОПК-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ИД1$_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности
			ИД2$_{ОПК-5.3}$. способен проводить верификацию данных в открытых информационных системах с учетом обеспечения их безопасности

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1$_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования	Знает: Основные методы и средства реализации удаленных сетевых атак на открытые информационные системы
	Умеет: работать с стандартными сетевыми утилитами
	Владеет: навыками анализа угроз и уязвимостей в открытых информационных системах

ИД2$_{опк-10}$ – владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности	Знает: основные классы шифров, способы их реализации;программно-аппаратные средства реализации криптографических систем защиты информации; типовые поточные и блочные шифры, а также асимметричные криптосистемы; основные криптографические протоколы системы шифрования с открытыми ключами
	Умеет: применять методы описания и исследования криптосистем; кодировать алгоритмы с соблюдением требований к качественному стилю программирования; определять струк- туру оптимальных устройств обработки сигналов информационных радиотехнических систем
	Владеет: навыками использования основных типов шифровки криптографических алгоритмов при решении задач обеспечения информационной безопасности; методами оценки криптографической стойкости алгоритмов шифрования; криптографической терминологией
ИД1$_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем	Знает: Политики безопасности и меры защиты в открытых информационных системах
	Умеет: работать с файловой системы LUKS и протокола удалённого управления ОС SSH
	Владеет: навыками построения политик безопасности для открытых информационных систем
ИД2$_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах	Знает: Принципы работы сетевых протоколов
	Умеет: применять на практике стандарты, относящиеся к открытым информационным системам
	Владеет: Терминологией и системным подходом построения защищенных открытых информационных систем
ИД1$_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности	Знает: технологий передачи данных в открытых информационных системах
	Умеет: Работать в UNIX-подобных системах
	Владеет: Терминологией и системным подходом построения защищенных открытых информационных систем
ИД2$_{ОПК-5.3}$. способен проводить верификацию данных в открытых информационных системах с учетом обеспечения их безопасности	Знает: процесс контроля обеспечения информационной безопасности
	Умеет: проводить верификацию данных открытых информационных системах
	Владеет: способностью проводить верификацию данных

3. Место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность открытых систем» относится к базовой части ОП ВО.

Приступая к изучению дисциплины, студент предварительно осваивает следующие дисциплины программы подготовки специалистов по специальности «Информационная безопасность автоматизированных систем»: «Информационная безопасность», «Открытые информационные системы». Дисциплина является предшествующей для следующих дисциплин: «Аудит информационных технологий и систем обеспечения информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем», «Защита конфиденциальной информации». Знания, полученные в ходе изучения дисциплины, используются при подготовке к ГИА.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Виды учебной работы	Всего ак. ч	Распределение трудоемкости по семестрам, ак. ч
		6 семестр
Общая трудоемкость дисциплины (модуля)	**144**	**144**
Контактная работа в т. ч. аудиторные занятия:	**90,9**	**90,9**
Лекции	18	18
в том числе в форме практической подготовки	-	-
Практические занятия	36	36
в том числе в форме практической подготовки	-	-
Консультации текущие	3,1	3,1
Вид аттестации (экзамен)	**33,8**	**33,8**
Самостоятельная работа:	**53,1**	**53,1**
Проработка материалов по лекциям, учебникам, учебным пособиям к собеседованию, коллоквиуму	18	18
Подготовка доклада	24	24
Расчетно-практическая работа	11,1	11,1

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	Часов по разделу
1	Стандартизация и модельное представление открытых информационных систем	Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость. Способность к взаимодействию. Основные модели открытых систем	11
2	Уязвимость открытых систем на примере интранета	Основные понятия. Угрозы ресурсам интранета и причины их реализации. Уязвимость архитектуры клиент-сервер. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, World Wide Web, Команды удаленного выполнения, Sendmail и электронная почта. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы	17
3	Атаки на открытые информационные системы	Удаленные атаки на открытые системы. Типичные сценарии и уровни атак. Классические и современные методы, используемые нападающими для проникновения в открытые системы	13
4	Обеспечение информационной безопасности в открытых системах	Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям. Принципы создания защищенных средств связи объектов в открытых системах. Политика безопасности для открытых сис-	19

		тем. Сервисы безопасности. Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем	
5	Аутентификация субъектов и объектов взаимодействия в открытых системах	Сетевая аутентификация – «первый рубеж» защиты открытой системы. Подсистема аутентификации. Российский рынок средств аутентификации	19
6	Межсетевые экраны	Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов	21
7	Системы анализа защищенности	Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые сканеры. Сканеры безопасности для приложений. Критерии выбора сканеров безопасности	22
8	Системы обнаружения и предотвращения вторжений	Методы отражения вторжений. Основы построения систем обнаружения вторжений. Системное обнаружение вторжений. Сетевое обнаружение вторжений. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений	24
	Консультации текущие		3,1
	экзамен		33,8

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СР, час
1	Стандартизация и модельное представление открытых информационных систем	2	4	5
2	Уязвимость открытых систем на примере интранета	2	4	5
3	Атаки на открытые информационные системы	2	4	5
4	Обеспечение информационной безопасности в открытых системах	2	4	5
5	Аутентификация субъектов и объектов взаимодействия в открытых системах	2	6	7
6	Межсетевые экраны	2	6	8

7	Системы анализа защищенности	4	8	10
8	Системы обнаружения и предотвращения вторжений	2	6	8,1
	ИТОГО	18	36	53,1

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, Час
1	Стандартизация и модельное представление открытых информационных систем	Основные элементы технологии открытых информационных систем. Совместимость открытых систем. Переносимость. Способность к взаимодействию. Основные модели открытых систем	2
2	Уязвимость открытых систем на примере интранета	Основные понятия. Угрозы ресурсам интранета и причины их реализации. Уязвимость архитектуры клиент-сервер. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, World Wide Web, Команды удаленного выполнения, Sendmail и электронная почта. Слабости современных технологий программирования. Ошибки в программном обеспечении. Сетевые вирусы	2
3	Атаки на открытые информационные системы	Удаленные атаки на открытые системы. Типичные сценарии и уровни атак. Классические и современные методы, используемые нападающими для проникновения в открытые системы	2
4	Обеспечение информационной безопасности в открытых системах	Четырехуровневая модель открытой системы. Специфика защиты ресурсов открытых систем на примере интранета. Выбор сетевой топологии интранета при подключении к другим внешним сетям. Принципы создания защищенных средств связи объектов в открытых системах. Политика безопасности для открытых систем. Сервисы безопасности. Средства обеспечения информационной безопасности в открытых системах. Создание комплексной системы обеспечения безопасности открытых систем	2
5	Аутентификация субъектов и объектов взаимодействия в открытых системах	Сетевая аутентификация – «первый рубеж» защиты открытой системы. Подсистема аутентификации. Российский рынок средств аутентификации	2

6	Межсетевые экраны	Функции межсетевых экранов. Руководящий документ Гостехкомиссии России по межсетевым экранам. Профили защиты для межсетевых экранов. Типы межсетевых экранов. Основные компоненты межсетевого экрана. Схемы подключения межсетевых экранов. Слабости межсетевых экранов. Выбор реализаций межсетевых экранов	2
7	Системы анализа защищенности	Аудит и мониторинг информационной безопасности в открытых системах. Место и задачи систем анализа защищенности в защите открытых систем. Классификации систем анализа защищенности. Сетевые сканеры. Сканеры безопасности для приложений. Критерии выбора сканеров безопасности	4
8	Системы обнаружения и предотвращения вторжений	Методы отражения вторжений. Основы построения систем обнаружения вторжений. Системное обнаружение вторжений. Сетевое обнаружение вторжений. Поведенческое обнаружение вторжений. Интеллектуальное обнаружение вторжений. Комплексное обнаружение вторжений. Выбор системы обнаружения вторжений	2

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Стандартизация и модельное представление открытых информационных систем	Работа со стандартными сетевыми утилитами. Работа с сетевым сканером и анализатором трафика Модель OSI и POSIX.	4
2	Уязвимость открытых систем на примере интранета	Разработка и управление Политикой использования ресурсов интранета	4
3	Атаки на открытые информационные системы	Атаки на открытые системы: анализ сетевого трафика, подмена доверенного объекта или субъекта, ложный объект, «отказ в обслуживании», удаленный контроль над станцией в сети	4

4	Обеспечение информационной безопасности в открытых системах	Создания защищенных средств связи объектов в открытых системах на основе стандартов ISO 7498-2, 17799, 15408 . Изучение и практическое применение шифрованной файловой системы LUKS и протокола удалённого управления ОС SSH. Слабости системных утилит, команд и сетевых сервисов: Telnet, FTP, NFS, DNS, NIS, World Wide Web, Команды удаленного выполнения, Sendmail и электронная почта	4
5	Аутентификация субъектов и объектов взаимодействия в открытых системах	Построение единых систем аутентификации, авторизации, персонализации, делегированного управления данными о субъектах и объектах и аудита доступа Анализ типовой модели аутентификации	6
6	Межсетевые экраны	Типы межсетевых экранов: экранирующие концентраторы, пакетные фильтры, шлюзы сеансового уровня, шлюзы прикладного уровня, межсетевые экраны экспертного уровня, персональные межсетевые экраны. Сетевой сканер XSpider. Система обнаружения вторжений Cisco IPS.	6
7	Системы анализа защищенности	Анализ угроз ИБ ресурсам интранета и причины их реализации. Уязвимости операционных систем, серверов, рабочих станций, каналов связи. Изучение и практическое применение межсетевого экрана ОС Linux Netfiler/iptables	8
8	Системы обнаружения и предотвращения вторжений	Сервисы безопасности: идентификация/аутентификация, разграничение доступа, протоколирование и аудит, экранирование, туннелирование, шифрование, контроль целостности, контроль защищенности, обнаружение отказов и оперативное восстановление, управление	6

5.2.3 Лабораторный практикум
Не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Стандартизация и модельное	Подготовка доклада с визуаль-	5

	представление открытых информационных систем	ным представлением	
2	Уязвимость открытых систем на примере интранета		5
3	Атаки на открытые информационные системы		5
4	Обеспечение информационной безопасности в открытых системах		5
5	Аутентификация субъектов и объектов взаимодействия в открытых системах	Подготовка к коллоквиуму	7
6	Межсетевые экраны		8
7	Системы анализа защищенности	Расчетно-практическая работа	10
8	Системы обнаружения и предотвращения вторжений		8,1

6Учебно-методическое и информационное обеспечение дисциплины

Для освоения дисциплины обучающийся может использовать:

6.1. Основная литература

1. Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс] : учебник. — Электрон. дан. — М. : ФЛИНТА, 2018. — 448 с.

6.2. Дополнительная литература

1. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие. — Электрон. дан. — СПб. : Лань, 2016. — 324 с.

2. Инструменты безопасности с открытым исходным кодом. Хаулет Т. Национальный Открытый Университет «ИНТУИТ» 2016 г. – 566 с.

3. Безопасность информационных систем. Кияев В., Граничин О. Национальный Открытый Университет «ИНТУИТ» - 2016 - 192 с.

4. Межсетевые экраны. Лапонина О. Р. Национальный Открытый Университет «ИНТУИТ» - 2016 - 466 с.

5. Информационная безопасность открытых систем: методические указания для самостоятельной работы студентов, обучающихся по специальности 10.05.03– «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников**,** Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2021. - 20 с.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Данылив, М. М. Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс]: методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж: ВГУИТ, 2016. – 32 с. Режим доступа в электронной среде:
http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813.

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

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp?*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ»	*https://education.vsuet.ru/*

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение и информационные справочные системы: информационная среда для дистанционного обучения «Moodle», локальная сеть университета и глобальная сеть Internet.

При освоении дисциплины используется лицензионное и открытое программное обеспечение – ОС Windows; Microsoft Office.

7 Материально-техническое обеспечение дисциплины (модуля)

Необходимый для реализации образовательной программы перечень материально-технического обеспечения включает:

- лекционные аудитории (оборудованные видеопроекционным оборудованием для презентаций; средствами звуковоспроизведения; экраном; имеющие выход в Интернет);
- помещения для проведения лабораторных и практических занятий (оборудованные учебной мебелью);
- библиотеку (имеющую рабочие места для студентов, оснащенные компьютерами с доступом к базам данных и Интернет);
- компьютерные классы.

Обеспеченность процесса обучения техническими средствами полностью соответствует требованиям ФГОС по специальности 10.05.03. Материально-техническая база приведена в лицензионных формах и расположена во внутренней сети по адресу http://education.vsuet.ru.

Аудитории для проведения лекционных, практических и лабораторных занятий, текущего контроля и промежуточной аттестации:

Учебная аудитория № 401 для проведения лекционных занятий, текущего контроля и промежуточной аттестации	Комплект мебели для учебного процесса – 80 шт. Переносной проектор Acer. Аудио-визуальная система лекционных аудиторий (мультимедийный проектор EpsonEB-X18, настенный экран ScreenMedia)	Microsoft Windows 8.1, Microsoft Office 2007 Standart, Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com

Учебная аудитория. № 332а для проведения для проведения	Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570), стенды – 5 шт.	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.

Аудитория для самостоятельной работы обучающихся, курсового и дипломного проектирования

Учебная аудитория № 424 для самостоятельной работы обучающихся, курсового и дипломного проектирования	Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая станция Регард РДЦБ.; стенды – 3	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.

Дополнительно самостоятельная работа обучающихся может осуществляться при использовании:

Читальные залы библиотеки.	Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами.	Microsoft Office Professional Plus 2010 Microsoft Open License Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 License No Level #48516271 от17.05.2011 г. http://eooen.microsoft.com Microsoft Office 2007 Standart, Microsoft Open License Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com Microsoft Windows XP, Microsoft Open License Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com. Adobe Reader XI, (бесплатное ПО) httos://acrobat.adobe.com/ru/ru/acrobat/odfreader/volume-distribution.html

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

Оценочные материалы (ОМ) для дисциплины включают в себя:

- перечень компетенций с указанием индикаторов достижения компетенций, этапов их формирования в процессе освоения образовательной программы;
- описание шкал оценивания;

- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков;

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины**.

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

ОЦЕНОЧНЫЕМАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Информационная безопасность открытых систем

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИД1$_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования
			ИД2$_{опк-10}$ – владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности
2	ОПК-13	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	ИД1$_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем
			ИД2$_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах
3	ОПК-5.3	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ИД1$_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности
			ИД2$_{ОПК-5.3}$. способен проводить верификацию данных в открытых информационных системах с учетом обеспечения их безопасности

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1$_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования	Знает: Основные методы и средства реализации удаленных сетевых атак на открытые информационные системы
	Умеет: работать с стандартными сетевыми утилитами
	Владеет: навыками анализа угроз и уязвимостей в открытых информационных системах
ИД2$_{опк-10}$ – владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности	Знает: основные классы шифров, способы их реализации;программно-аппаратные средства реализации криптографических систем защиты информации; типовые поточные и блочные шифры, а также асимметричные криптосистемы; основные криптографические протоколы системы шифрования с открытыми ключами
	Умеет: применять методы описания и исследования криптосистем; кодировать алгоритмы с соблюдением требований к качественному стилю программирования; определять струк- туру оптимальных устройств обработки сигналов информационных радиотехнических систем
	Владеет: навыками использования основных типов шифровки криптографических алгоритмов при решении задач обеспечения информационной безопасности; методами оценки криптографической стойкости алгоритмов шифрования; криптографической терминологией
ИД1$_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование	Знает: Политики безопасности и меры защиты в открытых информационных системах
	Умеет: работать с файловой системы LUKS и протокола удалённого управления ОС SSH
	Владеет: навыками построения политик безопасности для открытых информационных

систем защиты информации автоматизированных систем	систем
ИД2$_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах	Знает: Принципы работы сетевых протоколов
	Умеет: применять на практике стандарты, относящиеся к открытым информационным системам
	Владеет: Терминологией и системным подходом построения защищенных открытых информационных систем
ИД1$_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности	Знает: технологий передачи данных в открытых информационных системах
	Умеет: Работать в UNIX-подобных системах
	Владеет: Терминологией и системным подходом построения защищенных открытых информационных систем
ИД2$_{ОПК-5.3}$. способен проводить верификацию данных в открытых информационных системах с учетом обеспечения их безопасности	Знает: процесс контроля обеспечения информационной безопасности
	Умеет: проводить верификацию данных открытых информационных системах
	Владеет: способностью проводить верификацию данных

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Код и наименование индикатора достижения компетенции	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Стандартизация и модельное представление открытых информационных систем	ИД1$_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования	Вопросы к экзамену	1-15	Проверка преподавателем (уровневая шкала)
2	Уязвимость открытых систем на примере интранета		Банк тестовых заданий	46-60	Бланочное тестирование (процентная шкала)
			Задания для практических работ	101-110	Проверка преподавателем (уровневая шкала)
			Домашнее задание	131-140	Проверка преподавателем (уровневая шкала)
3	Атаки на открытые информационные системы	ИД1$_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем	Вопросы к экзамену	16-30	Проверка преподавателем (уровневая шкала)
4	Обеспечение информационной безопасности в открытых системах		Банк тестовых заданий	61-80	Бланочное тестирование (процентная шкала)
			Задания для практических работ	111-120	Проверка преподавателем (уровневая шкала)

			Домашнее задание	131-140	Проверка преподавателем (уровневая шкала)
5	Аутентификация субъектов и объектов взаимодействия в открытых системах	$ИД2_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах	Вопросы к экзамену	16-30	Проверка преподавателем (уровневая шкала)
6	Межсетевые экраны		Банк тестовых заданий	61-80	Бланочное тестирование (процентная шкала)
			Задания для практических работ	111-120	Проверка преподавателем (уровневая шкала)
			Домашнее задание	131-140	Проверка преподавателем (уровневая шкала)
7	Системы анализа защищенности Системы обнаружения и предотвращения вторжений	$ИД1_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности	Вопросы к экзамену	21-45	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	81-95	Бланочное тестирование (процентная шкала)
			Задания для практических работ	121-130	Проверка преподавателем (уровневая шкала)
			Домашнее задание	131-140	Проверка преподавателем (уровневая шкала)

3 Оценочные материалы для промежуточной аттестации

Аттестация обучающегося по дисциплине проводится в форме письменного ответа и предусматривает возможность последующего собеседования (зачета).

Каждый вариант теста включает 2 контрольных вопроса и 1 задачу, из них:

- 5 контрольных заданий на проверку знаний;
- 5 контрольных заданий на проверку умений;
- 5 контрольныхзаданий на проверку навыков.

Каждый билет включает 3 контрольных вопроса, из них:

- 1 контрольный вопрос на проверку знаний;
- 1 контрольный вопрос на проверку умений;
- 1 контрольный вопрос на проверку навыков.

3.1 Вопросы к экзамену.

ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ИД1ОПКв-10 – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования).

№ задания	Формулировка вопроса
1	Шифры замены. Математическая модель. Примеры.
2	Шифры перестановки. Математическая модель. Примеры.

3	Шифры гаммирования. Математическая модель. Примеры.
4	Принципы построения блочных шифров. Схема Фейстеля.
5	Алгоритм симметричного шифрования DES.
6	Алгоритм симметричного шифрования ГОСТ 28147-99.
7	Алгоритм симметричного шифрования Rijndael.
8	Алгоритмы симметричного шифрования IDEA и Blowfish.
9	Режимы выполнения алгоритмов симметричного шифрования.
10	Поточные криптосистемы. Принципы построения. Классификация. Проблема синхронизации.
11	Линейные конгруэнтные генераторы. Линейные регистры сдвига.
12	Основные принципы построения асимметричных криптосистем. Стойкость.
13	Шифросистема RSA. Стойкость.
14	Шифросистема Эль-Гамаля. Стойкость.
15	Шифросистема на основе принципа «рюкзака».

ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем ($ИД1_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем, $ИД2_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах).

№ задания	Формулировка вопроса
16	Технология Ethernet. Четыре основных разновидности кадров Ethernet. Общий формат кадра Ehternet.
17	Стандарты IEEE на 10 Мбит/с: стандарт l0BaseT, стандарт 10Base2, стандарт l0Base5, стандарт l0BaseFL.
18	Стандарты IEEE на 100 Мбит/с. Технология Fast Ethernet: 100BASE-T4, 100 BASE-TX, 100BASE-FX.
19	Технология Ethernet. Четыре основных разновидности кадров Ethernet. Общий формат кадра Ehternet.
20	Сетевые адаптеры передача и прием кадра. Распределение обязанностей между сетевым адаптером и его драйвером. Классификация сетевых адаптеров.
21	Концентраторы, функция ретрансляции кадров. Конструктивное исполнение концентраторов: концентратор с фиксированным количеством портов, модульный концентратор и стековый концентратор.
22	Ограничения сети, построенной на общей разделяемой среде: порог количества узлов и интенсивность загрузки сети. Преимущества логической структуризации сети.
23	Понятия мост и коммутатор. Два типа алгоритмов, используемых мостами и коммутаторами.
24	Мосты с маршрутизацией от источника: их суть и назначение. Пример работы моста с маршрутизацией от источника.
25	Ограничения топологии сети, построенной на мостах. Влияние замкнутых маршрутов на работу моста.
26	Алгоритм покрывающего дерева: определение активной конфигурации, пример построения конфигурации покрывающего дерева для сети.
27	Коммутаторы локальных сетей. Понятие коммутационная матрица, принцип её работы. Способы передачи кадра: «коммутация на лету» и параллельная обработка нескольких кадров.
28	Понятия глобальной сети, абонента глобальной компьютерной сети, оператор сети, поставщик услуг сети. Управление обменом информации в глобальных сетях. Способы коммутации абонентов: коммутация пакетов, коммутация каналов, сети с динамической коммутацией и сети с постоянной коммутацией.
29	Список низкоуровневых и высокоуровневых услуг, который предоставляет Internet. Понятие intranet. Пример структуры глобальной компьютерной сети: коммутаторы, компьютеры, маршрутизаторы, мультиплексор, интерфейс пользователь - сеть и интерфейс сеть – сеть, аппаратура передачи данных.
30	Виды глобальных сетей с коммутацией пакетов. Принцип коммутации пакетов с использованием техники виртуальных каналов. Два типа виртуальных соединений — коммутируемый виртуальный канал и постоянный виртуальный канал. Принцип маршрутизации пакетов на основе виртуальных каналов.

ОПК-5.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах ($ИД1_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности).

№ задания	Формулировка вопроса

31	Базовые принципы обеспечения безопасности телекоммуникационных связей в сетях ЭВМ
32	Административный контроль в сетях ЭВМ
33	Основные проблемы секретности в сетях ЭВМ
34	Физическая структуризация сетей ЭВМ
35	Логическая структуризация сетей ЭВМ
36	Модель OSI. Понятие «открытая система»
37	Уровни, протоколы, интерфейсы
38	Сетезависимые и сетенезависимые уровни модели взаимодействия открытых систем
39	Стандартные стеки коммуникационных протоколов
40	Управление доступом к передающей среде
41	Методы кодирования и передачи данных
42	Методы обнаружения и коррекции ошибок передачи данных
43	Типы соединительных кабелей
44	Сетевые операционные системы
45	Технические средства и оборудование локальных сетей ЭВМ

3.2Тесты (тестовые задания)

ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности ($ИД1_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования).

№ задания	Тестовое задание с вариантами ответов
46	Как называется распределенный алгоритм, определяющий последовательность действий каждой из сторон? Ответ: (1) процесс шифрования (2) электронная цифровая подпись **(3) протокол** (4) хэш-функция
47	Как называется способ реализации криптографического метода, при котором все процедуры шифрования и расшифрования выполняются специальными электронными схемами по определенным логическим правилам? Ответ: **(1) аппаратный** (2) программный (3) ручной (4) электромеханический
48	Какой способ реализации криптографических методов обладает максимальной скоростью обработки данных? Ответ: **(1) аппаратный** (2) программный

	(3) ручной (4) электромеханический
49	Что является целью криптографического преобразования информации? Ответ: **(1) защита информации от несанкционированного доступа, аутентификация и защита от преднамеренных изменений** (2) защита информации от случайных помех при передаче и хранении (3) защита информации от всех случайных или преднамеренных изменений (4) сжатие информации
50	Что является целью помехоустойчивого кодирования информации? Ответ: (1) защита информации от несанкционированного доступа, аутентификация и защита от преднамеренных изменений **(2) защита информации от случайных помех при передаче и хранении** (3) защита информации от всех случайных или преднамеренных изменений (4) сжатие информации
51	Что является целью эффективного кодирования информации? Ответ: (1) защита информации от несанкционированного доступа, аутентификация и защита от преднамеренных изменений (2) защиты информации от случайных помех при передаче и хранении (3) защита информации от всех случайных или преднамеренных изменений **(4) уменьшение избыточности в сообщениях**
52	Как называется преобразование информации с целью обнаружения и коррекции ошибок при воздействии помех при передаче данных? Ответ: (1) компрессия (2) эффективное кодирование (3) шифрование **(4) помехоустойчивое кодирование**
53	Как называется преобразование сообщения из одной кодовой системы в другую, в результате которого уменьшается размер сообщения? Ответ: (1) имитозащита **(2) эффективное кодирование** (3) шифрование (4) помехоустойчивое кодирование

54	Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений? Ответ: (1) компрессия (2) эффективное кодирование **(3) криптографическое шифрование** (4) помехоустойчивое кодирование
55	В чем заключается общая идея помехоустойчивого кодирования? Ответ: **(1) из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые** (2) из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые (3) производится преобразование информации с целью сокрытия ее смысла (4) уменьшается избыточность передаваемых сообщений
56	В чем заключается общая идея эффективного кодирования методом Хаффмана? Ответ: **(1) символам с большей вероятностью присваиваются более короткие коды, тогда как реже встречающимся символам – более длинные** (2) символам с меньшей вероятностью присваиваются более короткие коды, тогда как чаще встречающимся символам – более длинные (3) производится замена цепочек или серий повторяющихся байтов на один кодирующий байт-заполнитель и счетчик числа их повторений (4) из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
57	В чем заключается общая идея сжатия информации методом кодирования серий последовательностей (методом RLE)? Ответ: (1) символам с большей вероятностью присваиваются более короткие коды, тогда как реже встречающимся символам – более длинные (2) символам с меньшей вероятностью присваиваются более короткие коды, тогда как чаще встречающимся символам – более длинные **(3) производится замена цепочек или серий повторяющихся байтов на один кодирующий байт-заполнитель и счетчик числа их повторений** (4) из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
58	Что такое «расстояние по Хэммингу»? Ответ: **(1) число разрядов двух кодовых слов, в которых они различны** (2) наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код (3) характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом

	(4) число контрольных разрядов в кодовом слове
59	Что такое «минимальное кодовое расстояние»? Ответ: (1) число разрядов двух кодовых слов, в которых они различны **(2) наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код** (3) характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом (4) число контрольных разрядов в кодовом слове
60	Что такое «избыточность» помехоустойчивого кода? Ответ: (1) число разрядов двух кодовых слов, в которых они различны (2) наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код **(3) характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом** (4) число информационных разрядов в кодовом слове

ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем ($ИД1_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем, $ИД2_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах).

№ задания	Формулировка вопроса
61	Какая служба безопасности является наиболее критичной для электронной коммерции? Ответ: (1) целостность **(2) доступность** (3) идентифицируемость
62	В каком файле должны быть определены файлы .cgi и .pl, чтобы программы выполнялись без отображения исходного кода на веб-странице? Ответ: **(1) httpd.conf** (2) x-httpd-cgi.cgi (3) x-httpd-cgi.pl
63	В каком файле должны быть определены файлы .cgi и .pl, чтобы программы выполнялись без отображения исходного кода на веб-странице? Ответ: (1) httpd.pl

	(2) httpd.conf (3) httpd.cgi
64	В каком файле должны быть определены файлы .cgi и .pl, чтобы программы выполнялись без отображения исходного кода на веб-странице? Ответ: (1) x-httpd-cgi.cgi (2) httpd.cgi **(3) httpd.conf**
65	Какая учетная запись должна использоваться для работы с веб-сервером? Ответ: (1) корневая учетная запись **(2) учетная запись владельца веб-сервера** (3) гостевая учетная запись
66	Какие основные меры необходимо предпринять для защиты сервера от атак злоумышленника через интернет? Ответ: **(1) расположение сервера** **(2) конфигурация веб-сервера** (3) шифрование информации
67	Какие основные меры необходимо предпринять для защиты сервера от атак злоумышленника через интернет? Ответ: **(1) конфигурация операционной системы** (2) шифрование информации (3) ограничение доступа
68	Какие порты следует разрешить для доступа к серверу электронной коммерции? Ответ: **(1) 80 (HTTP)** (2) 21 (FTP) (3) 23 (Telnet)
69	Какие порты следует разрешить для доступа к серверу электронной коммерции? Ответ: **(1) 80 (HTTP)** **(2) 443 (HTTPS)** (3) 21 (FTP)
70	Какие порты следует разрешить для доступа к серверу электронной коммерции?

	Ответ: **(1) 443 (HTTPS)** (2) 21 (FTP) (3) 23 (Telnet)
71	Во время этапа разработки проекта разработчики должны предотвращать переполнение буфера посредством: Ответ: **(1) запрета на прямую передачу введенных данных командам оболочки** **(2) ограничением размера вводимых пользователем данных** (3) использования 128 битного ключа шифрования
72	В каких зонах необходимо проводить ежемесячное сканирование уязвимостей на коммерческих сайтах? Ответ: **(1) вне зоны, охраняемой межсетевым экраном** **(2) во внутренней сети организации** (3) внутри зоны, охраняемой межсетевым экраном
80	В каких зонах необходимо проводить ежемесячное сканирование уязвимостей на коммерческих сайтах? Ответ: **(1) в сети веб-сервера** (2) в клиентской сети **(3) в сети сервера приложения**
81	В каких зонах необходимо проводить ежемесячное сканирование уязвимостей на коммерческих сайтах? Ответ: (1) внутри зоны, охраняемой межсетевым экраном (2) в клиентской сети **(3) во внутренней сети организации**
82	Когда необходимо производить сканирование уязвимостей на коммерческих сайтах? Ответ: **(1) перед вводом системы в эксплуатацию** (2) ежедневно (3) при выходе обновлений
83	Когда необходимо производить сканирование уязвимостей на коммерческих сайтах? Ответ: **(1) ежемесячно**

	(2) ежедневно (3) при обнаружении вторжения
84	Когда необходимо производить сканирование уязвимостей на коммерческих сайтах? Ответ: **(1) перед вводом системы в эксплуатацию** (2) при обнаружении вторжения **(3) ежемесячно**
85	Какие вопросы необходимо решить для реализации безопасности клиентской стороны? Ответ: (1) защита информации, хранимой на сервере **(2) защита информации при передаче между компьютером клиента и сервером** (3) защита сервера от вторжения злоумышленников

ОПК-5.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах ($ИД1_{ОПКв\text{-}5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности).

№ задания	Формулировка вопроса
86	Какие вопросы необходимо решить для реализации безопасности серверной части? Ответ: (1) защита информации при передаче между компьютером клиента и сервером **(2) защита информации, хранимой на сервере** **(3) защита сервера от вторжения злоумышленников**
87	В управление конфигурацией входят следующие составляющие: Ответ: (1) контроль за несанкционированными изменениями (2) запрет изменений конфигурации **(3) контроль за санкционированными изменениями**
88	В управление конфигурацией входят следующие составляющие: Ответ: **(1) обнаружение несанкционированных изменений** (2) запрет изменений конфигурации (3) обнаружение санкционированных изменений
89	Порт 80 позволяет: Ответ: **(1) осуществлять доступ к веб** (2) передавать файлы

	(3) получать и отсылать почту (4) подключаться к серверам новостей
90	Порты 110 и 143 позволяют: Ответ: (1) осуществлять доступ к веб (2) передавать файлы **(3) получать почту** (4) подключаться к серверам новостей
91	Порт 119 позволяет: Ответ: (1) осуществлять доступ к веб (2) передавать файлы (3) получать и отсылать почту **(4) подключаться к серверам новостей**
82	Для чего используются службы NetBIOS? Ответ: (1) для удаленных сеансов X Window System (2) системами Unix для удаленного вызова процедур (3) для управления сетью организации **(4) для предоставления общего доступа к файлам**
93	Для чего используются службы NFS? Ответ: (1) для удаленных сеансов X Window System (2) системами Unix для удаленного вызова процедур **(3) для работы Network File Services** (4) для управления сетью организации
94	Какие службы следует предоставлять сотрудникам? Ответ: **(1) почта** **(2) шифрованная почта** (3) FTP (4) Telnet
95	Какой способ внешнего доступа к внутренним системам наиболее распространен? Ответ: **(1) VPN**

	(2) коммутируемое соединение (3) Telnet (4) арендуемый канал
96	Какие службы следует предоставлять сотрудникам? Ответ: **(1) почта, шифрованная почта, интернет** (2) любые (3) Telnet, FTP, NFS, NetBIOS
97	Какое назначение службы DNS? Ответ: **(1) разрешения системных имен и их преобразования в IP адреса** (2) синхронизация времени (3) поддержка функционирования сети
98	Какое назначение службы ICMP? Ответ: (1) разрешения системных имен и их преобразования в IP адреса (2) синхронизация времени **(3) поддержка функционирования сети**
99	Какое назначение службы NTP? Ответ: (1) разрешения системных имен и их преобразования в IP адреса **(2) синхронизация времени** (3) поддержка функционирования сети
100	Какое подключение к провайдеру является наиболее надежным? Ответ: (1) через один канал (2) многоканальный доступ (3) с одной точкой присутствия **(4) с несколькими точками присутствия**

3.3Задания для практических работ (типовые задачи)

ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности ($ИД1_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования).

№ задания	Условие задачи (формулировка задания)
101	Изучение методов физического и кодирования, используемых в цифровых сетях передачи данных.
102	Потенциальный код без возврата к нулю (NRZ)
103	Биполярный импульсный код (RZ)
104	Биполярное кодирование с чередующейся инверсией (AMI)
105	Манчестерский код
106	Дифференциальный манчестерский код
107	Код трехуровневой передачи MLT-3
108	Пятиуровневый код PAM-5
109	Избыточное кодирование
110	Скремблирование

ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем ($ИД1_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем, $ИД2_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах).

№ задания	Условие задачи (формулировка задания)
111	Анализ трафика утилиты ping
112	Анализ трафика утилиты tracert (traceroute)
113	Анализ HTTP-трафика
114	Анализ DNS-трафика
115	Анализ ARP-трафика
116	Анализ трафика утилиты nslookup
117	Анализ FTP-трафика
118	Анализ DHCP-трафика
119	Анализ Skype-трафика
120	Просмотр базы данных Shodan.io

ОПК-5.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах ($ИД1_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности).

№ задания	Условие задачи (формулировка задания)
121	На рисунке изображена топология сети и требуемый путь прохождения сетевых пакетов. Необходимо так настроить хосты сети, чтобы ping-запрос (request) от компьютера 4 к компьютеру 2 шёл по пути, указанному сплошной стрелкой. При этом ping-ответ (reply) должен возвращаться другим путём: по пунктирной стрелке.
122	На рисунке изображена топология сети и один путь прохождения сетевых пакетов от nc client 1 до nc server. На компьютере 4 должно быть запущено два nc-клиента, которые подключаются к различным nc-серверам. Nc-серверы запущены на компьютерах 1 и 2, они должны принимать подключения на адреса интерфейсов, обозначенных на рисунке nc server и nc server 2
123	На рисунке изображена топология сети и требуемый путь прохождения сетевых пакетов. Сплошными линиями показаны сообщения от клиента к серверам, штриховыми – сообщения от серверов к клиенту. На компьютерах 1 и 2 запущены два nc-сервера. На компьютере 4 запущен один nc-клиент, который осуществляет подключение к IP-адресу, который не представлен ни на одном из интерфейсов в сети. На компьютере 3 должен быть настроен DNAT и дублирование трафика таким образом, чтобы оба nc-сервера получали запросы от nc-клиента. Ответные сообщения от обоих nc-серверов должны приходить к nc-клиенту. Клиент и серверы должны работать по протоколу UDP.

124	На рисунке изображена топология сети и требуемый путь прохождения сетевых пакетов. В компьютере 2 имеется два сетевых адаптера, на которых должны быть настроены различные IP адреса: IP1 и IP2. IP1 — адрес интерфейса, подключенного к компьютеру 1, IP2 — адрес интерфейса, подключенного к компьютеру 3 Необходимо настроить сеть таким образом, чтобы при отправлении ICMP Echo Request с компьютера 4 на IP1 пакет проходил через компьютер 3 и компьютер 1, а ICMP Echo Reply шел с компьютера 2 сразу через компьютер 3 (штрихпунктирная линия на рисунке 4.8). При отправлении ICMP Echo Request с компьютера 4 на IP2 пакет должен пройти через компьютер 3 сразу на компьютер 2, а ICMP Echo Reply должен пройти с компьютера 2 на компьютер 1 и далее на компьютер 3
125	На рисунке изображена топология сети и требуемый путь прохождения сетевых пакетов. С компьютера 4 посылается ICMP Echo Request на адрес, который не существует в данной сети.
126	На рисунке изображена топология сети. В каждом компьютере для интерфейса lo должен быть задан уникальный IP-адрес. Нужно настроить таблицы маршрутизации на компьютерах сети таким образом, чтобы связь каждого компьютера с каждым другим осуществлялась через 3 канала компьютерной сети.
127	На рисунке изображена топология сети и один из путей прохождения сетевых пакетов. Между компьютерами 1 и 2 проведено 2 изолированных друг от друга канала. IP1 – адрес интерфейса в компьютере 1, подключенный к каналу 1 IP2 – адрес интерфейса в компьютере 2, подключенный к каналу 1
128	На рисунке изображена топология сети и требуемый путь прохождения сетевых пакетов. В каждом компьютере для интерфейса lo должен быть задан уникальный IP-адрес.
129	На сетевом интерфейсе компьютера 4 должен быть задан MTU = 1000 С компьютера 4 отправить ICMP Echo request в компьютер 1, размер которого больше заданного MTU, но меньше 2*MTU, т.о. пакет будет разделен на 2 фрагмента. На всех компьютерах настроить таблицы маршрутизации таким образом, чтобы второй фрагмент дошел до компьютера 1 раньше, чем первый фрагмент.
130	На рисунке 4.14 изображена топология сети. С компьютера 5 посылается ICMP Echo Request на компьютер 3 Размер пакета и MTU сетевого интерфейса должны быть выбраны таким образом, чтобы пакет был фрагментирован на 3 фрагмента.

3.4 Домашнее задание (типовые задачи)

ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности ($ИД1_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования).

ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем ($ИД1_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем, $ИД2_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах).

ОПК-5.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах ($ИД1_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности).

№ задания	Формулировка задания
130	Реферат на тему Основные понятия программно-технического уровня информационной безопасности
131	Реферат на тему Требования к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к защите информации от НСД.
132	Реферат на тему Общие подходы к построению систем защиты компьютерной информации. Различия требований и основополагающих механизмов защиты от НСД.
133	Реферат на тему Требования к защите ОС. Понятие защищенной системы. Подходы к организации защиты ОС и их недостатки.
134	Реферат на тему Этапы построения защиты. Административные меры защиты. Стандарты безопасности ОС.
135	Реферат на тему Разграничение доступа в ОС. Субъекты, объекты, методы и права доступа.

136	Реферат на тему Межсетевые экраны
137	Реферат на тему Системы обнаружения компьютерных атак
138	Реферат на тему Доверенная загрузка
139	Реферат на тему Цифровая подпись
140	Реферат на тему система сертификации ключей

4. Методические материалы,определяющие процедуры оценивания знаний, умений, навыкови (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03-2017 Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.02-2018 Положение о рейтинговой оценке текущей успеваемости.

Для оценки знаний, умений, навыков обучающихся по дисциплине применяется рейтинговая система. Итоговая оценка по дисциплине определяется на основании определения среднеарифметического значения баллов по каждому заданию.

5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания для каждого результата обучения по дисциплине

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ОПК-10 - Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности					
ИД1$_{ОПКв-10}$ – осуществляет защиту данных открытых информационных систем от утечки по техническим каналам с использованием современных средств шифрования					
Знает: Основные методы и средства реализации удаленных сетевых атак на открытые информационные системы	Результаты текущего тестирования	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	Отлично	Освоена / повышенный
			Обучающийся ответил на 70-84 % вопросов	Хорошо	Освоена / повышенный
			Обучающийсяответил на 50-69 % вопросов	Удовлетворительно	Освоена / базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетворительно	Не освоена / недостаточный
	Вопросы к экзамену	Правильность ответов	Обучающийсядал исчерпывающий ответ на вопрос, не допустил ошибок. Студент владеет знаниями и умениями по дисциплине в полном объеме	Отлично	Освоена / повышенный
			Обучающийсядал подробный и полный ответ, допустил не более 1 ошибки. Студент владеет знаниями и умениями по дисциплине в полном объеме	Хорошо	Освоена / повышенный
			Обучающийсядал поверхностный ответ на вопрос, допустил более 2 ошибок	Удовлетворительно	Освоена / базовый
			Обучающийсяне смог правильно ответить на вопрос, допустил ошибку в анализе задания	неудовлетворительно	Не освоена / недостаточный
Умеет: работать с стандартными сетевыми утилитами	Задания для практических работ	Правильность и полнота выполнения задания	Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал развернутые выводы	Отлично	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал краткие выводы	Хорошо	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, но не смог грамотно их применить, выводы отсутствуют	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно выбрать инструменты для решения задачи	неудовлетворительно	Не освоена / недостаточный
Владеет: навыками анали-	Домашнее за-	Правиль-	Обучающийся разносторонне проанализировал ситуа-	Отлично	Освоена / повы-

за угроз и уязвимостей в открытых информационных системах	дание	ность и полнота выполнения задания	цию, выбрал верную методику решения, сделал развернутые выводы, не допустил ошибок в расчетах		шенный
			Обучающийся разносторонне проанализировал ситуацию, полностью выполнил задание, сделал вывод, допустил не более 1 ошибки в расчетах	Хорошо	Освоена / повышенный
			Обучающийся поверхностно проанализировал ситуацию, выполнил задание, сделал вывод, допустил не более 2 ошибок в расчетах	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно решить задачу, допустил ошибку в анализе ситуации	неудовлетворительно	Не освоена / недостаточный
ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем					
$ИД1_{ОПКв-13}$ – обладает способностью организовать и провести диагностику и тестирование систем защиты информации автоматизированных систем $ИД2_{ОПКв-13}$ – обладает способностью проводить анализ защищённости информации в автоматизированных системах					
Знает: Политики безопасности и меры защиты в открытых информационных системах Знает: Принципы работы сетевых протоколов	Результаты текущего тестирования	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	Отлично	Освоена / повышенный
			Обучающийся ответил на 70-84 % вопросов	Хорошо	Освоена / повышенный
			Обучающийся ответил на 50-69 % вопросов	Удовлетворительно	Освоена / базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетворительно	Не освоена / недостаточный
	Вопросы к экзамену	Правильность ответов	Обучающийся дал исчерпывающий ответ на вопрос, не допустил ошибок. Студент владеет знаниями и умениями по дисциплине в полном объеме	Отлично	Освоена / повышенный
			Обучающийся дал подробный и полный ответ, допустил не более 1 ошибки. Студент владеет знаниями и умениями по дисциплине в полном объеме	Хорошо	Освоена / повышенный
			Обучающийся дал поверхностный ответ на вопрос, допустил более 2 ошибок	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно ответить на вопрос, допустил ошибку в анализе задания	неудовлетворительно	Не освоена / недостаточный
Умеет: работать с файловой системы LUKS и протокола удалённого управления ОС SSH Умеет: применять на практике стандарты, относящиеся к открытым информационным системам	Задания для практических работ	Правильность и полнота выполнения задания	Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал развернутые выводы	Отлично	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал краткие выводы	Хорошо	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, но не смог грамотно их применить, выводы отсутствуют	Удовлетворительно	Освоена / базовый

			Обучающийся не смог правильно выбрать инструменты для решения задачи	неудовлетворительно	Не освоена / недостаточный
Владеет: навыками построения политик безопасности для открытых информационных систем Владеет: Терминологией и системным подходом построения защищенных открытых информационных систем	Домашнее задание	Правильность и полнота выполнения задания	Обучающийся разносторонне проанализировал ситуацию, выбрал верную методику решения, сделал развернутые выводы, не допустил ошибок в расчетах	Отлично	Освоена / повышенный
			Обучающийся разносторонне проанализировал ситуацию, полностью выполнил задание, сделал вывод, допустил не более 1 ошибки в расчетах	Хорошо	Освоена / повышенный
			Обучающийся поверхностно проанализировал ситуацию, выполнил задание, сделал вывод, допустил не более 2 ошибок в расчетах	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно решить задачу, допустил ошибку в анализе ситуации	неудовлетворительно	Не освоена / недостаточный
ОПК-5.3 Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах					
ИД1$_{ОПКв-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности					
Знает: технологий передачи данных в открытых информационных системах	Результаты текущего тестирования	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	Отлично	Освоена / повышенный
			Обучающийся ответил на 70-84 % вопросов	Хорошо	Освоена / повышенный
			Обучающийся ответил на 50-69 % вопросов	Удовлетворительно	Освоена / базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетворительно	Не освоена / недостаточный
	Вопросы к экзамену	Правильность ответов	Обучающийся дал исчерпывающий ответ на вопрос, не допустил ошибок. Студент владеет знаниями и умениями по дисциплине в полном объеме	Отлично	Освоена / повышенный
			Обучающийся дал подробный и полный ответ, допустил не более 1 ошибки. Студент владеет знаниями и умениями по дисциплине в полном объеме	Хорошо	Освоена / повышенный
			Обучающийся дал поверхностный ответ на вопрос, допустил более 2 ошибок	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно ответить на вопрос, допустил ошибку в анализе задания	неудовлетворительно	Не освоена / недостаточный
Умеет: Работать в UNIX-подобных системах	Задания для практических работ	Правильность и полнота выполнения задания	Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал развернутые выводы	Отлично	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал краткие выводы	Хорошо	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, но не смог грамотно их применить, выво-	Удовлетворительно	Освоена / базовый

			ды отсутствуют		
			Обучающийся не смог правильно выбрать инструменты для решения задачи	неудовлетворительно	Не освоена / недостаточный
Владеет: Терминологией и системным подходом построения защищенных открытых информационных систем	Задания для практических работ	Правильность и полнота выполнения задания	Обучающийся разносторонне проанализировал ситуацию, выбрал верную методику решения, сделал развернутые выводы, не допустил ошибок в расчетах	Отлично	Освоена / повышенный
			Обучающийся разносторонне проанализировал ситуацию, полностью выполнил задание, сделал вывод, допустил не более 1 ошибки в расчетах	Хорошо	Освоена / повышенный
			Обучающийся поверхностно проанализировал ситуацию, выполнил задание, сделал вывод, допустил не более 2 ошибок в расчетах	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно решить задачу, допустил ошибку в анализе ситуации	неудовлетворительно	Не освоена / недостаточный