ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом ректора
от «31» мая 2024 г. № 425-1

Б1.О.48 Безопасность вычислительных сетей

рабочая программа дисциплины

Специальность/направление подготовки – 10.03.01 Информационная безопасность
Специализация/профиль – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника – Бакалавр
Форма и срок обучения – очная форма 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 3
Часов по учебному плану (УП) – 108

Формы промежуточной аттестации
очная форма обучения:
экзамен 7 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	7	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	28	**28**
– лекции	14	**14**
– практические (семинарские)		
– лабораторные	14	**14**
Самостоятельная работа	44	**44**
Экзамен	36	**36**
Итого	108	**108**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Программу составил(и):
к.п.н., доцент, доцент, В.В.Михаэлис

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «21» мая 2024 г. № 11

Зав. кафедрой, к. э. н, доцент Т.К. Кириллова

1 ЦЕЛЬ И ЗАДАЧА ДИСЦИПЛИНЫ

1.1 Цель дисциплины

1	сформировать у обучающихся основы комплексного подхода к вопросам построения защищенных телекоммуникационных сетей, межсетевого экранирования

1.2 Задача дисциплины

1	освоение методов повышения безопасности, надежности, отказоустойчивости сетей

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.
Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Дисциплина изучается на начальном этапе формирования компетенции

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
2	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-4.2 Способен администрировать операционные системы, системы управления базами данных, вычислительные сети;	ОПК-4.2.1 Знает основы построения локальной компьютерной сети, уровни антивирусной защиты, базы данных, защиты рабочих станций и сетевых серверов	Знать: основы построения локальной компьютерной сети, уровни антивирусной защиты, базы данных, защиты рабочих станций и сетевых серверов
		Уметь: построить локальную компьютерную сеть, создать антивирусную защиту, защитить рабочую станцию и сервер
		Владеть: навыками построения локальной компьютерной сети, уровней защиты
	ОПК-4.2.2 Умеет администрировать операционные системы, системы управления базами данных, вычислительные сети	Знать: эффективные способы защиты информации в различных системах
		Уметь: анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития
		Владеть: анализом эффективности систем организационной защиты информации и разрабатывать направления ее развития
	ОПК-4.2.3 Имеет навыки администрирования операционных систем, систем управления баз данных, вычислительных сетей	Знать: как администрировать операционные системы, системы управления баз данных, вычислительные сети
		Уметь: администрировать операционные системы, системы управления баз данных, вычислительные сети
		Владеть: навыками администрирования операционных систем, систем управления баз данных, вычислительных сетей

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма		*Код индикатора
		Семестр	Часы	

			Лек	Пр	Лаб	СР	достижения компетенции
1.0	**Раздел 1. Политика и модели безопасности в защищенных компьютерных телекоммуникационных сетях. Базовые элементы и устройства обеспечения сетевой безопасности информационных систем**						
1.1	Тема 1. Основные понятия и анализ угроз информационной безопасности, проблемы информационной безопасности сетей	7	2		2	10	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3
1.2	Тема 2.Стандарты информационной безопасности	7	2		2	10	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3
2.0	**Раздел 2. Принципы построения узлов защищенных компьютерных и телекоммуникационных сетей.**						
2.1	Тема 3. Принципы криптографической защиты информации	7	4		4	10	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3
2.2	Тема 4. Технологии межсетевых экранов	7	4		2	10	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3
2.3	Тема 5. Основы технологии виртуальных защищенных сетей	7	2		4	4	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3
	Форма промежуточной аттестации – экзамен	7	36				ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3
	Итого часов (без учёта часов на промежуточную аттестацию)		14		14	44	

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. Кемерово : КузГТУ имени Т.Ф. Горбачева, 2022. - 120с. - Текст: электронный. - URL: https://e.lanbook.com/book/257564 (дата обращения: 29.04.2024)	Онлайн
6.1.1.2	Мэйволд, Э. Безопасность сетей : учебное пособие - 2-е изд., испр. / Э. Мэйволд. Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 572с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 29.04.2024)	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Борисова, С. Н. Криптографические методы защиты информации: классическая криптография : учебное пособие / С. Н. Борисова. Пенза : ПГУ, 2018. - 186с. - Текст: электронный. - URL: https://e.lanbook.com/book/162235 (дата обращения: 29.04.2024)	Онлайн
6.1.2.2	Стеганографические и криптографические методы защиты информации : учебное пособие / . Уфа : БГПУ имени М. Акмуллы, 2016. - 112с. - Текст: электронный. - URL: https://e.lanbook.com/book/90963 (дата обращения:	Онлайн

	29.04.2024)	
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Михаэлис, В.В. Методические указания по изучению дисциплины Б1.О.48 Безопасность вычислительных сетей, по направлению подготовки 10.03.01 Информационная безопасность, профиль Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) / В.В. Михаэлис; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 11 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47554_1480_2024_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.2.2	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Packet Tracer УЧ. ПРОЦ. Универсальная общественная лицензия GNU, http://www.packettracernetwork.com/	
6.3.2.2	PuTTY свободно распространяемый клиент для различных протоколов удалённого доступа УЧ. ПРОЦ. http://www.putty.org/	
6.3.3 Информационные справочные системы		
6.3.3.1	Не предусмотрены	
6.4 Правовые и нормативные документы		
6.4.1	Не предусмотрены	

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-415 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Лаборатория Д-508 «Информационные системы и сетевые технологии», «Сети и системы передачи информации» для проведения лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, компьютеры с подключением к сети Интернет, обеспечивающие доступ в электронную информационно-образовательную среду ИрГУПС, учебно-наглядные пособия (презентации, плакаты). коммутационная стойка, сервер cisco 2600, switch catalyst 2900, модем ZyXEL, Router cisco 1600, Hub token ring, тел. адаптер D-link DVG-7111S, управляемый коммутатор 2 уровня D-link DES-1210-10/ME, управляемый коммутатор 3 уровня D-link DGS-1500-28, межсетевой экран D-link DFL-260E, маршрутизатор D-Link DIR-100, беспроводная точка доступа D-Link DWL-3200AP, голосовой шлюз D-Link DVG-7022S Gateway Router с поддержкой SIP, IP-камера D-Link DCS-2130, коммутатор D-link DES-1100-16, коммутатор D-link DES-3028
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы;

	– учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	
Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе

	формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Безопасность вычислительных сетей» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Безопасность вычислительных сетей» участвует в формировании компетенций:

ОПК-4.2. Способен администрировать операционные системы, системы управления базами данных, вычислительные сети;

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр				
1.0	**Раздел 1. Политика и модели безопасности в защищенных компьютерных телекоммуникационных сетях. Базовые элементы и устройства обеспечения сетевой безопасности информационных систем**			
1.1	Текущий контроль	Тема 1. Основные понятия и анализ угроз информационной безопасности, проблемы информационной безопасности сетей	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Лабораторная работа (письменно/устно)
1.2	Текущий контроль	Тема 2.Стандарты информационной безопасности	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Принципы построения узлов защищенных компьютерных и телекоммуникационных сетей**			
2.1	Текущий контроль	Тема 3. Принципы криптографической защиты информации	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Лабораторная работа (письменно/устно)
2.2	Текущий контроль	Тема 4. Технологии межсетевых экранов	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Лабораторная работа (письменно/устно)
2.3	Текущий контроль	Тема 5. Основы технологии виртуальных защищенных сетей	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Лабораторная работа (письменно/устно)
	Промежуточная аттестация	Тема 1. Основные понятия и анализ угроз информационной безопасности, проблемы информационной безопасности сетей Тема 2.Стандарты информационной безопасности Тема 3. Принципы криптографической защиты информации Тема 4. Технологии межсетевых экранов Тема 5. Основы технологии виртуальных защищенных сетей	ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

Описание показателей и критериев оценивания компетенций.
Описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Образец задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (образец экзаменационного билета) к экзамену
2	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме экзамена. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения	Высокий

	полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	
«хорошо»	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме экзамена

Критерии оценивания	Шкала оценивания
Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования	«отлично»
Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования	«хорошо»
Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования	«удовлетворительно»
Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования	«неудовлетворительно»

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Лабораторная работа

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»		Лабораторная работа выполнена с задержкой, письменный отчет с недочетами.

		Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	«не зачтено»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Типовые задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Тема 1. Основные понятия и анализ угроз информационной безопасности, проблемы информационной безопасности сетей»

ЛАБОРАТОРНАЯ РАБОТА

Классификация и анализ угроз информационной безопасности

Цель работы

Научиться конфигурировать и администрировать вычислительные сети, формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе серверных технологий.

Общие сведения

Угроза безопасности информационной системы (ИС) – это возможность воздействия на ИС, которое прямо или косвенно может нанести ущерб ее безопасности. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты ИС. Кроме выявления возможных угроз, целесообразно проведение анализа угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование. ИС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие важные свойства информации и систем обработки: доступность, целостность и конфиденциальность информации.

Уровни информационной безопасности ИС:

− доступность (возможность за разумное время получить требуемую информацию);

− целостность (невозможность несанкционированной или случайной модификации информации);

− конфиденциальность (невозможность несанкционированного получения информации).

Для автоматизированных информационных систем угрозы следует классифицировать по аспекту информационной безопасности (доступность, целостность, конфиденциальность):

− угрозы нарушения доступности (отказ в обслуживании), направленные на создание таких ситуаций, когда определенные действия либо блокируют доступ к некоторым ресурсам ИС, либо снижают ее работоспособность, например, если один пользователь системы запрашивает доступ к некоторой службе, а другой пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным;

− угрозы нарушения целостности информации, хранящейся в компьютерной системе или передаваемой по каналу связи, которые направлены на ее изменение либо искажение, приводящее к нарушению ее качества или полному уничтожению, например, если целостность информации может быть нарушена преднамеренно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему;

− угрозы нарушения конфиденциальности, направленные на разглашение конфиденциальной или секретной информации, например, если при реализации угроз информация становится известной лицам, которые не должны иметь к ней доступ. Данные виды угроз можно считать первичными, или непосредственными, поскольку их реализация ведет к непосредственному воздействию на защищаемую информацию. Угрозы следует классифицировать по природе их возникновения. Например, естественные угрозы возникают при воздействии на ИС объективных физических процессов или стихийных природных явлений; искусственные угрозы безопасности (ИС) возникают под влиянием деятельности человека. По степени преднамеренности проявления угрозы могут быть вызваны ошибками или халатностью персонала, а также преднамеренно вызваны действиями злоумышленников. Источниками угроз безопасности информационной системы могут быть природная среда, человек, санкционированные программно-аппаратные средства, несанкционированные программно-аппаратные средства. Источники угроз могут располагаться на различных расстояниях от цели. Например, вне контролируемой зоны ИС, в пределах контролируемой зоны ИС, непосредственно в ИС. Угрозы, воздействующие на информационные системы, могут поражать ИС независимо от ее активности, например, вскрытие шрифтов криптозащиты информации или только в процессе обработки данных. Существуют пассивные угрозы, реализация которых ничего не меняет в структуре и содержании ИС, и активные. На этапе получения доступа в ИС угрозы могут быть реализованы как вовремя, так и после разрешения доступа к ресурсам. Угрозы бывают скрытого доступа, путем использования «дыр» в ИС и стандартного доступа, например, незаконное получение паролей и других реквизитов разграничения доступа с последующей маскировкой под зарегистрированного пользователя. Кроме этого, можно классифицировать угрозы ИС по текущему месту расположения информации, хранимой и обрабатываемой в ИС угрозы доступа к информации, могут находиться на внешних запоминающих устройствах, в оперативной памяти, в линиях связи, отображаться на терминале или печатаемом на принтере текстовой информации.

Порядок выполнения работы

1. По рекомендуемой литературе изучить классификацию угроз информационной безопасности.
2. Составить классификационную таблицу угроз безопасности сети.
3. Привести примеры угроз для каждой из рассматриваемых категорий угроз.

Контрольные вопросы

1. Дать определение понятию «угроза безопасности информационной системы».
2. На какие основные категории подразделяются угрозы безопасности?
3. Для чего необходимо составление классификации основных угроз?
4. Приведите примеры угроз нарушения целостности информации, передаваемой по каналу связи.
5. Приведите примеры угроз, вызывающих отказ в обслуживании ИС.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты
«Тема 3. Принципы криптографической защиты информации»

Введение

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

1. Цель работы

Исследование и разработка классических методов симметричных криптосистем

2. Краткие сведения из теории

Шифры простой замены. Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на K букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены. Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143143

Шифровка ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ

Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i=Г(ш)_i+Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i=Г(ш)_i+Т(ш)_i$.

3. Порядок выполнения работы

Основные шаги шифрования текстового файла методом гаммирования.

1. Получить от пользователя ключ, имя входного и выходного файла.
2. Инициализировать генератор случайных чисел с помощью ключа. Открыть указанные файлы.
3. Прочитать строку из файла.
4. Получить случайное число.
5. Получить ASCII-код очередного символа строки и увеличить его на случайное число, полученное на шаге 4.
6. Проверить правильность (допустимый диапазон) нового ASCII-кода.
7. В выходную строку записать очередной символ, соответствующий ASCII-коду, полученному на шаге 6.
8. Если не достигли конца входной строки, то перейти к шагу 4.
9. Записать полученную строку в выходной файл.
10. Если не достигнут конец файла, то перейти к шагу 3.
11. Закрыть файлы.

4. Вопросы для самопроверки

1.Шифр Гронсфельда.

2.Шифры двойной перестановки. Шифрование с помощью магического квадрата.

3.Шифр многоалфавитной замены и алгоритм его реализации.

3.2 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД/РПП	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Тема 1. Основные понятия и анализ угроз информационной безопасности, проблемы информационной безопасности сетей	Знать	5 – ОТЗ 5 – ЗТЗ
ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Тема 2.Стандарты информационной безопасности	Знать	5 – ОТЗ 5 – ЗТЗ
ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Тема 3. Принципы криптографической защиты информации	Знать	5 – ОТЗ 5 – ЗТЗ
		Уметь	5 – ОТЗ 5 – ЗТЗ
ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Тема 4. Технологии межсетевых экранов	Уметь	5 – ОТЗ 5 – ЗТЗ
		Навык	5 – ОТЗ 5 – ЗТЗ
ОПК-4.2.1 ОПК-4.2.2 ОПК-4.2.3	Тема 5. Основы технологии виртуальных защищенных сетей	Знать	5 – ОТЗ 5 – ЗТЗ
		Уметь	6 – ОТЗ 5 – ЗТЗ
		Итого	41 – ОТЗ 40 – ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

Номер 1
Информация - это:

Ответ:

(1) сведения, полученные при исследовании, изучении или обучении

(2) известия, новости, факты, данные

(3) команды или символы представления данных (в системах связи или в компьютере)

(4) знания (сообщения, экспериментальные данные, изображения), меняющие концепцию, полученную в результате физического или умственного опыта

Номер 2
Безопасность - это:

Ответ:

(1) свобода от угроз

(2) возможность выполнения любых действий

(3) состояние защищенности от внешних и внутренних угроз

Номер 3
Информационная безопасность – это:

Ответ:

(1) меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним

(2) это система управления доступом, защищающее внутренние сети от внешних атак

(3) механизм аутентификации, предполагающий использование определенного устройства для идентификации человеческих характеристик

Номер 4
Аутентификация личности в компьютерных системах может быть реализована при помощи:

Ответ:

(1) пароля

(2) смарт-карты

(3) биометрической системы

(4) паспорта

Номер 5
Самое слабое звено в системе безопасности?

Ответ:

люди, человек

Номер 6
Какие уровни существуют в правительственной классификации уровней секретности информации?

Ответ:

(1) общедоступная

(2) несекретная

(3) конфиденциальная

(4) секретная

(5) совершенно секретная

Номер 7
Какой уровень безопасности соответствует уровню D шкалы "Оранжевой книги"?

Ответ:

(1) минимальная защита (ненормируемая)

(2) защита по усмотрению

(3) контролируемая защита доступа

(4) защита с метками безопасности

(5) структурированная защита

Номер 8
Какой уровень безопасности соответствует уровню B2 шкалы "Оранжевой книги"?

Ответ:

(1) минимальная защита (ненормируемая)

(2) защита по усмотрению

(3) контролируемая защита доступа

(4) защита с метками безопасности

(5) структурированная защита

Номер 9
Какая система получила сертификат уровня A1 "Оранжевой книги"?

Ответ:

Honeywell SCOMP

Номер 10
Какой стандарт рассматривает вопросы сетевой безопасности?

Ответ:

красная книга

Номер 11
Для каких сетей сертификат "Красной книги" считается устаревшим?

Ответ:

беспроводных сетей

Номер 11
Антивирусное программное обеспечение обеспечивает защиту от:

Ответ:

(1) самовоспроизводящихся компьютерных программ, которые распространяются, внедряя себя в исполняемый код других программ или в документы специального формата

(2) от незаконного вторжения в компьютерную сеть

(3) перехвата трафика

Номер 12
Межсетевой экран - это:

Ответ:

(1) устройство управления доступом, защищающее внутренние сети от внешних атак

(2) устройство маршрутизации трафика

(3) устройство кэширования сетевого трафика

Номер 13
Биометрия - механизм аутентификации, предполагающий использование:

Ответ:

(1) определенного устройства для идентификации человеческих характеристик

(2) пароля

(3) смарт-карты

(4) паспорта

Номер 14
Какие параметры могут использоваться в биометрических системах?

Ответ:

(1) отпечатки пальцев

(2) отпечатки сетчатки/радужной оболочки

(3) паспорт

Номер 15
Какие параметры могут использоваться в биометрических системах?

Ответ:

(1) конфигурации руки

(2) конфигурации лица

(3) голоса

Номер 17
Шифрование - это:

Ответ:

(1) способ преобразования информации, применяемый для хранения важной информации в ненадежных источниках или передачи её по незащищённым каналам связи

(2) меры, принятые для предотвращения несанкционированного использования, злоупотребления, изменения сведений, фактов, данных или аппаратных средств либо отказа в доступе к ним

(3) механизм аутентификации, предполагающий использование определенного устройства для идентификации человеческих характеристик

Номер 18
Защита информации включает

Ответ:

(1) физическую защиту

(2) защиту коммуникаций

(3) защиту излучения

Номер 19
INFOSEC - это:

Ответ:

(1) совокупность всех видов защиты информации

(2) защита компьютеров

(3) физическая защита информации

Номер 20
Межсетевой экран

Ответ:

защищает от внешних атак

Номер 21
Система управления доступом

Ответ:

(1) ограничивает доступ к файлам, идентифицируя пользователя, который входит в систему

(2) предотвращает атаку через разрешенный канал связи.

(3) защищает от внутренних пользователей

Номер 22
Основные достоинства парольной аутентификации:

Ответ:

(1) высокая надежность

(2) низкая стоимость внедрения

(3) простота реализации

Номер 24
Основные недостатки аутентификации с использованием смарт-карт:

Ответ:

(1) высокая надежность

(2) высокая цена

(3) простота реализации

Номер 25
Основные достоинства и недостатки биометрической аутентификации:

Ответ:

(1) высокая надежность

(2) низкая стоимость внедрения

(3) высокая стоимость

Номер 26
Обозначение, семейства протоколов охватывающих проблемы безопасности на IP-уровне:

Ipsec

3.3 Перечень теоретических вопросов к экзамену

(для оценки знаний)

1. Правовые принципы использования информационно-телекоммуникационных сетей
2. Организационно-распорядительные документы по обеспечению безопасности ЛВС.
3. Характеристики безопасности сети
4. Обеспечение безопасности сети. Классификация атак и типовые угрозы
5. Средства анализа защищенности сети.
6. Инкапсуляция и деинкапсуляция данных
7. Стек протоколов TCP/IP
8. Справочные модули командной строки коммутатора
9. Характеристики протокола Интернета
10. Скорости передачи данных беспроводных топологий стандартов 802.11b
11. Формат IP-адреса
12. Протокол DNS
13. Причины образования «петель» и протоколы управления путями к сетевым сегментам
14. Протокол DHCP
15. Протоколы безопасного удаленного подключения к устройствам сети
16. Характеристики безопасности UDP и TCP - протоколов
17. Проблемы среды передачи коммутируемой среды
18. Установление соединения. Трехстороннее квитирование и управление потоком
19. Протокол ARP
20. Протоколы безопасности сетей WLAN
21. Стандарты локальных сетей
22. Множественный доступ к разделяемой среде. Алгоритм CSMA/CD
23. Протоколы безопасности сетей WLAN
24. Обзор средств анализа защищенности вычислительных сетей
25. Назначение виртуальных сетей
26. Инструменты хоста: основные команды и их описание.
27. Перечень организационно-распорядительных документов по обеспечению безопасности сетей ЭВМ

3.4 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

1. Выделите из сети 10.1.32.0/22 следующие подсети: а) подсеть общего пользования для абонентов сети Интернет 1000 ПК; б) подсеть управления — 20 устройств; в) подсеть обработки персональных данных — 50 ПК; г) остальной офис — 100 ПК.

2. Выделите из сети 192.168.132.0/24 следующие подсети: а) подсеть общего пользования - 90 ПК; б) подсеть управления — 5 устройств; в) подсеть обработки персональных данных — 20 ПК; г) остальной офис — 50 ПК.

3. Методики применения средств анализа защищенности сетей

4. Создание виртуальных сетей на базе одного коммутатора
5. Настройка исходных параметров безопасности коммутатора
6. Использование «Сканер ВС»
7. Обеспечение безопасности простой сети
8. Организация и настройка VLAN

9. Применение «MaxPatrol» для оценки защищенности вычислительных сетей
10. Применение «XSpider»

3.8 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

1. Безопасность коммутатора ЛВС
2. Домены коллизий
3. Процесс коммутации кадров
4. Характеристики коммутатора ЛВС
5. Передача пакетов данных между хостами (через коммутатор)
6. Дуплексная передача данных
7. Диапазоны IP-адресов
8. Функции маршрутизатора
9. Средства анализа защищенности сетей ЭВМ
10. Методики применения средств анализа защищенности сетей
11. Назначение и основные функции MaxPatrol
12. Назначение и основные функции XSpider
13. Виды аудита безопасности сетей ЭВМ
14. Безопасность маршрутизатора
15. Сканер безопасности сети «Сканер ВС»
16. Создание виртуальных сетей на базе нескольких коммутаторов

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Лабораторная работа	Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено. Преподаватель на лабораторной работе, предшествующей занятию проведения защиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы. Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия

Для организации и проведения промежуточной аттестации составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Перечень теоретических вопросов и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике фондов оценочных средств.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

Образец экзаменационного билета

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «Безопасность вычислительных сетей»**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____

1 Характеристики безопасности сети
2 Создание виртуальных сетей на базе одного коммутатора.
3 Использование «Сканер ВС»