ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом и.о. ректора
от «17» июня 2022 г. № 77

Б1.О.36 Основы управления информационной безопасностью

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. – 6
Часов по учебному плану (УП) – 216

Формы промежуточной аттестации
очная форма обучения:
зачет 7 семестр, экзамен 8 семестр, курсовая работа 8 семестр

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

Семестр	7	8	**Итого**
Вид занятий	Часов по УП	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	42	36	**78**
– лекции	14	12	**26**
– практические (семинарские)	28	24	**52**
– лабораторные			
Самостоятельная работа	30	72	**102**
Экзамен		36	**36**
Итого	72	144	**216**

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.э.н., доцент, Н.И. Глухов

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «17» июня 2022 г. № 12

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

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цель дисциплины

1	изучение основных понятий, методологии и применения практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии

1.2 Задачи дисциплины

1	приобретение обучающимися необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;
2	формирование у обучающихся целостного представления об организации и сущности процессов управления информационной безопасностью (ИБ) на предприятии как результата внедрения системного подхода по решению задач обеспечения ИБ

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового – 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 воспитания 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	Б1.О.27 Основы информационной безопасности
2	Б1.О.40 Информационные технологии
3	Б1.О.47 Теоретические основы компьютерной безопасности
4	Б2.О.01(У) Учебная - ознакомительная практика
5	Б2.О.02(У) Учебная - учебно-лабораторная практика

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

1	Б1.О.53 Методология построения защищенных автоматизированных систем
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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и	ОПК-1.1 Знает сущность и значение информации, информационных технологий и информационной безопасности в развитии современного общества	Знать: сущность и значение информации, информационных технологий и информационной безопасности в развитии современного общества
		Уметь: реализовывать сущность и значение информации, информационных технологий и информационной безопасности в развитии современного общества
		Владеть: навыками работ по реализации знаний по сущности и значению информации, информационных технологий и информационной безопасности в развитии сов-ременного общества
	ОПК-1.2 Умеет пользоваться нормативными документами, современным программным обеспечением в области информационной	Знать: нормативные документы с современным программным обеспечением в области информационной безопасности
		Уметь: пользоваться нормативными документами с современным программным обеспечением в области

государства;	безопасности	информационной безопасности
		Владеть: навыками работ по реализации знаний нормативных документов с современным программным обеспечением в области информационной безопасности
	ОПК-1.3 Имеет навыки применения методов и средств защиты информации для обеспечения объективных потребностей личности, общества и государства	Знать: методы и средства защиты информации для обеспечения объективных потребностей личности, общества и государства
		Уметь: использовать навыки применения методов и средств защиты информации для обеспечения объективных потребностей личности, общества и государства
		Владеть: навыками применения методов и средств защиты информации для обеспечения объективных потребностей личности, общества и государства

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1 Система управления информационной безопасностью.**						
1.1	Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии	7	4			8	ОПК-1.1 ОПК-1.2
1.2	Политика безопасности	7		4		6	ОПК-1.2 ОПК-1.3
1.3	Аудит информационной безопасности	7	2	2		8	ОПК-1.1 ОПК-1.3
1.4	Организация обеспечения информационной безопасности автоматизированных систем	7		4		6	ОПК-1.1
1.5	Средства поддержки процессов управления информационной безопасностью /	7		4			ОПК-1.2 ОПК-1.3
2.0	**Раздел 2 Комплексная система защиты информации.**						
2.1	Сущность и задачи комплексной системы защиты информации	7	2			8	ОПК-1.1 ОПК-1.2
2.2	Факторы, влияющие на организацию комплексной системы защиты информации	7		6		8	ОПК-1.1 ОПК-1.2
2.3	Определение компонентов комплексной системы защиты информации	7		4		6	ОПК-1.3
2.4	Определение условий функционирования комплексной системы защиты информации	7	3	4		6	ОПК-1.1 ОПК-1.2
2.5	Технологическое и организационное построение комплексной системы защиты	7	3	4		8	ОПК-1.1 ОПК-1.3
	Форма промежуточной аттестации – зачет	7					
3.0	**Раздел 3 Управление комплексной системой защиты информации.**						
3.1	Назначение, структура и содержание управления комплексной системой защиты информации	8	2	4		8	ОПК-1.1 ОПК-1.2
3.2	Принципы и методы планирования комплексной системы защиты информации	8	4	4		6	ОПК-1.2 ОПК-1.3
3.3	Сущность и содержание контроля функционирования комплексной системы защиты информации	8	2	4		8	ОПК-1.1
3.4	Общая характеристика подходов к оценке эффективности систем защиты информации	8	2	4		8	ОПК-1.2
3.5	Методы и модели оценки эффективности комплексной системы защиты информации	8	2	4		8	ОПК-1.3
	Форма промежуточной аттестации – экзамен	8	36				ОПК-1.1 ОПК-1.2 ОПК-1.3
	Курсовая работа	8				26	ОПК-1.1
	Итого часов (без учёта часов на промежуточную аттестацию)		26	52		102	

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	Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. Москва, Берлин : Директ-Медиа, 2015. - 255с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 14.09.2022)	Онлайн
6.1.1.2	Краковский, Ю. М. Информационная безопасность и защита информации : учеб. пособие / Ю. М. Краковский. Иркутск : ИрГУПС, 2016. - 224с.	93
6.1.1.3	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 14.09.2022)	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Минин, И. В. Защита конфиденциальной информации при электронном документообороте : учебное пособие / И. В. Минин, О. В. Минин. Новосибирск : Новосибирский государственный технический университет, 2011. - 20с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=228779 (дата обращения: 14.09.2022)	Онлайн
6.1.2.2	Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. Санкт-Петербург : Издательство Политехнического университета, 2014. - 322с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 14.09.2022)	Онлайн

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	Глухов Н.И. Методические указания по изучению дисциплины Б1.0.36 Основы управление информационной безопасностью по направлению подготовки – 10.03.01 Информационная безопасность, профиль Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности / Н.И. Глухов; ИрГУПС. – Иркутск: ИрГУПС, 2023. – 15 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_2646_1480_2022_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	Не предусмотрено
6.3.3 Информационные справочные системы	
6.3.3.1	«Консультант +» http://www.consultant.ru/
6.3.3.2	«Техэксперт» http://www.cntd.ru/
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-518 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). Для проведения занятий имеются учебно-наглядные пособия (презентации, плакаты).
3	Учебная аудитория Д-413 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). Для проведения занятий имеются учебно-наглядные пособия (презентации).
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

Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Самостоятельная работа	Обучение по дисциплине «Основы управления информационной безопасностью» 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 «Основы управления информационной безопасностью» участвует в формировании компетенций:

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

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. Система управления информационной безопасностью**			
1.1	Текущий контроль	Тема 1. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии	ОПК-1.1	Собеседование (устно)
1.2	Текущий контроль	Тема 2. Политика безопасности	ОПК-1.1 ОПК-1.2 ОПК-1.3	Собеседование (устно)
1.3	Текущий контроль	Тема 3. Аудит информационной безопасности	ОПК-1.1	Собеседование (устно)
1.4	Текущий контроль	Тема 4. Организация обеспечения информационной безопасности автоматизированных систем	ОПК-1.1 ОПК-1.2 ОПК-1.3	Собеседование (устно)
1.5	Текущий контроль	Тема 5. Средства поддержки процессов управления информационной безопасностью	ОПК-1.1	Собеседование (устно)
2.0	**Раздел 2. Комплексная система защиты информации**			
2.1	Текущий контроль	Тема 6. Сущность и задачи комплексной системы защиты информации. Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ	ОПК-1.1	Собеседование (устно)
2.2	Текущий контроль	Тема 7. Факторы, влияющие на организацию комплексной системы защиты информации	ОПК-1.1 ОПК-1.2 ОПК-1.3	Собеседование (устно)
2.3	Текущий контроль	Тема 8. Определение компонентов комплексной системы защиты информации	ОПК-1.1	Собеседование (устно)
2.4	Текущий контроль	Тема 9. Определение условий функционирования комплексной системы защиты информации	ОПК-1.1 ОПК-1.2 ОПК-1.3	Собеседование (устно)
2.5	Текущий контроль	Тема 10. Разработка модели комплексной системы защиты информации	ОПК-1.1	Собеседование (устно)
2.6	Текущий контроль	Тема 11. Технологическое и организационное построение комплексной системы защиты	ОПК-1.1 ОПК-1.2 ОПК-1.3	Собеседование (устно)
	Промежуточная аттестация	Темы 1-8		Зачет (собеседование) Зачет - тестирование (компьютерные технологии)
8 семестр				
3.0	**Раздел 3. Управление комплексной системой защиты информации**			
3.1	Текущий	Тема 12. Назначение, структура	ОПК-1.1	Собеседование (устно)

	контроль	и содержание управления комплексной системой защиты информации		
3.2	Текущий контроль	Тема 13. Принципы и методы планирования комплексной системы защиты информации	ОПК-1.1	Собеседование (устно)
3.3	Текущий контроль	Тема 14. Сущность и содержание контроля функционирования комплексной системы	ОПК-1.1 ОПК-1.2 ОПК-1.3	Тестирование (компьютерные технологии)
3.4	Текущий контроль	Тема 15. Общая характеристика подходов к оценке эффективности систем защиты информации	ОПК-1.1	Собеседование (устно)
3.5	Текущий контроль	Тема 16. Методы и модели оценки эффективности комплексной системы защиты информации	ОПК-1.1	Собеседование (устно)
	Промежуточная аттестация	Все разделы	ОПК-1.1	Курсовая работа (письменно) Курсовая работа (устно)
	Промежуточная аттестация	Все разделы	ОПК-1.1 ОПК-1.2 ОПК-1.3	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	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Тестирование (компьютерные	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и	Фонд тестовых заданий

	технологии)	умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Зачет	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 к зачету
2	Тест – промежуточная аттестация в форме зачета	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
3	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
4	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
5	Курсовая работа	Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты

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

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями	Базовый

		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	
«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»	«не зачтено»	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 зачета и экзамена

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

Курсовая работа

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть

	нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсовой работы в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала. Курсовая работа не представлена преподавателю. Обучающийся не явился на защиту курсовой работы

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Тестирование

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

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

3.1 Типовые контрольные задания для проведения собеседования

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

Ниже приведен образец типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования
«Политика безопасности»

1. Организационно-правовой статус сотрудников информационной безопасности?
2. Порядок доступа пользователей к информационным системам, в которых обрабатывается информация конфиденциального характер?
3. Средства и системы защиты ИС?
4. Локальная безопасность. Антивирусная защита?
5. Защищенные каналы с использованием криптозащиты, на базе решений VipNet, VPN, Банк-клиент или других, сертифицированных ФСТЭК?
6. Разграничение прав доступа к информационным системам и системам хранения данных?
7. Организация физической безопасности
8. Как осуществляется хранение информации конфиденциального характера локально на компьютере?
9. Ответственность за соблюдение положений Политики ИБ?
10. Дублирование, резервное копирование и хранение информации

Образец типового варианта вопросов для проведения собеседования
«Назначение, структура и содержание управления комплексной системой защиты информации»

1. Понятие «принятие решений» в широком и узком смысле.
2. Понятие «управленческое решение».
3. Что такое технология разработки решения?
4. Цель, объект и предмет разработки управленческих решений
5. Классификация видов решений.
6. Программируемые и непрограммируемые управленческие решения.
7. Основанные на суждениях, интуитивные и творческие решения.
8. Решения, типичные для общих функций управления
9. Составляющие задачи принятия управленческого решений.
10. Понятие проблемной ситуации.
11. Ограничения и критерии при принятии решения.
12. Схема процесса принятия управленческого решения.
13. Механизм предпочтений лица, принимающего решение.
14. Варианты алгоритмов разработки и принятия решений с учетом проблем и задач, стоящих перед лицами, принимающими решения.
15. Содержание и особенности этапов полного процесса разработки управленческого решения.
16. Линейное уравнение: характеристика, построение, решение примеров задач.

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	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-1.1	Тема 1. Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии	Знание	1 – ОТЗ 1 – ЗТЗ

		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-1.1 ОПК-1.2 ОПК-1.3	Тема 2. Политика безопасности	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-1.1	Тема 3. Аудит информационной безопасности	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-1.1 ОПК-1.2 ОПК-1.3	Тема 4. Организация обеспечения информационной безопасности автоматизированных систем	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-1.1	Тема 5. Средства поддержки процессов управления информационной безопасностью	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-1.1	Тема 6. Сущность и задачи комплексной системы защиты информации. Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-1.1 ОПК-1.2 ОПК-1.3	Тема 7. Факторы, влияющие на организацию комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-1.1	Тема 8. Определение компонентов комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-1.1 ОПК-1.2 ОПК-1.3	Тема 9. Определение условий функционирования комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-1.1	Тема 10. Разработка модели комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-1.1 ОПК-1.2 ОПК-1.3	Тема 11. Технологическое и организационное построение комплексной системы защиты	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-1.1	Тема 12. Назначение, структура и содержание управления комплексной системой защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-1.1	Тема 13. Принципы и методы планирования комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ

ОПК-1.1 ОПК-1.2 ОПК-1.3	Тема 14. Сущность и содержание контроля функционирования комплексной системы	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ЗТЗ
ОПК-1.1	Тема 15. Общая характеристика подходов к оценке эффективности систем защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ
ОПК-1.1	Тема 16. Методы и модели оценки эффективности комплексной системы защиты информации	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
		Итого	41 – ОТЗ 41 – 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.

Образец типового варианта итогового теста,
предусмотренного рабочей программой дисциплины

1. Выберите правильное определение термина «информация»:
   а) совокупность содержащихся в базах данных сведений;
   б) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;
   в) сведения (сообщения, данные) воспроизводимые различными системами;
   г) сведения (сообщения, данные) независимо от формы их представления.

2. Выберите правильное определение термина «обладатель информации»:
   а) лицо, самостоятельно создавшее информацию;
   б) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;
   в) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
   г) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

3. Предоставление информации – это

Ответ: действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

4. Защищаемые помещения – это

Ответ: помещения, специально предназначенные для проведения конфиденциальных мероприятий.

5. Выберите правильное определение термина «контролируемая зона»:
   а) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств;
в) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации;
г) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.

6. К рекомендуемым методам и способам защиты информации в информационных системах относятся (выберите все верные варианты ответов):

а) методы и способы защиты информации от несанкционированного доступа;
б) методы и способы сокрытия информации от внутренних нарушителей;
в) методы и способы устранения конкурентов;
г) методы и способы защиты информации от утечки по техническим каналам.

7. Технические способы защиты информации в зависимости от используемых средств классифицируются как (выберите все верные варианты ответов):

а) полуактивные;
б) пассивные;
в) разноплановые;
г) удостоверяющие;
д) активные.

8. Технический канал утечки информации – это

Ответ: совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

9. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно ____

Ответ: 16.

10. Техническими каналами утечки информации являются (выберите все верные варианты ответов):

а) кражи технических средств информационной системы;
б) утечки акустической (речевой) информации;
в) утечки информации, реализуемые через общедоступные информационные сети;
г) утечки видовой информации;
д) утечки информации по каналам побочных электромагнитных излучений;
е) утечки информации, реализуемые через интернет.

11. Несанкционированный доступ к информации – это

Ответ: **доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств.**

12. Механизм контроля целостности СЗИ Secret Net предназначен для

а) формирония цифровых отпечатков данных;
б) контроля информационных потоков;
в) слежения за неизменностью содержимого ресурсов компьютера.

13. Механизм замкнутой программной среды СЗИ Secret Net и Dallas Lock предназначен для

а) ограничения использования программного обеспечения на компьютере;
б) установки ограниченного количества программ;
в) сбора сведений об используемых приложениях.

14. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями

а) «конфиденциально»;
б) «секретно»;
в) «строго конфиденциально»,
г) «неконфиденциально».

15. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного_____

Ответ: логарифма.

16. Хэш-функции предназначены, главным образом, для _____

Ответ: контроля целостности данных.

17. Длина хэш-кода алгоритма MD5 составляет _____

Ответ: 128 бит.

18. Каким образом в СЗИ Secret Net реализуется настройка дискреционного разграничения доступа к файлам и папкам?

Ответ: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы.

3.3 Перечень тем курсовых работ

1. Основные положения теории управления в системах организационно-технологического типа.
2. Основы методологии принятия управленческого решения в системах организационно-технологического типа.
3. Требования, предъявляемые к комплексной системе защиты информации.
4. Основные этапы разработки комплексной системы защиты информации.
5. Факторы, влияющие на организацию комплексной системы защиты информации.
6. Порядок нормативного закрепления состава защищаемой информации.
7. Определение объектов защиты.
8. Источники и способы дестабилизирующего воздействия на информацию.
9. Каналы и методы несанкционированного доступа к информации.
10. Определение компонентов комплексной системы защиты информации.
11. Условия функционирования комплексной системы защиты информации.
12. Функциональная модель комплексной системы защиты информации.
13. Организационная модель комплексной системы защиты информации.
14. Информационная модель комплексной системы защиты информации.
15. Стадии создания комплексной системы защиты информации.
16. Структура и содержание документационного обеспечения стадий создания комплексной системы защиты информации.
17. Кадровое обеспечение функционирования комплексной системы защиты информации.
18. Нормативно-методическое и материально-техническое обеспечение комплексной системы защиты информации.
19. Общая технология управления комплексной системы защиты информации.
20. Принципы и методы планирования деятельности комплексной системы защиты информации.
21. Принципы и методы контроля функционирования комплексной системы защиты информации.
22. Управление комплексной системы защиты информации в условиях чрезвычайных

ситуаций.

23. Общая характеристика подходов к оценке эффективности комплексной системы защиты информации.

24. Вероятностный подход к оценке эффективности комплексной системы защиты информации.

25. Статистические и экспертные методы оценки эффективности системы защиты информации.

26. Показатели защищенности комплексной системы защиты информации.

27. Место и роль системы защиты информационных активов в системе управления деятельностью предприятия.

28. Сущность комплексной системы защиты информационных активов предприятий.

29. Особенности система защиты информационных активов хозяйствующего субъекта.

30. Особенности организационного направления в деятельности по защите информационных активов предприятия.

31. Сущность направления в организационной защите – работе с персоналом, определении его надежности

32. Методика оценки надежности персонала, как основного источника угроз информационным активам предприятия.

33. Суть методики оценки возможного ущерба при реализации угроз безопасности.

34. Сущность направления в организационной защите - информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.

35. Обоснование позиции защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.

3.4 Перечень теоретических вопросов к зачету

1. Основные понятия, термины и определения; предмет и объект защиты;
2. Уязвимости и угрозы безопасности информации в АИС; риски информационной безопасности (ИБ) и методы их оценки;
3. Правовые и организационные методы защиты информации в АИС; аудит ИБ;
4. Базовые принципы организации ЗИ;
5. Защита информации в АИС от несанкционированного доступа (НСД): подсистема идентификации и аутентификации (методы и средства);
6. Модели разграничения доступа к объектам: избирательное управление; мандатное управление; замкнутая программная среда;
7. Архитектура системы защиты информации (СЗИ) от НСД SecretNet;
8. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа;
9. СЗИ от НСД Dallas Lock: основные функциональные возможности;
10. Электронный замок Соболь-PCI: настройка и эксплуатация; управление пользователями; диагностика устройства; настройка контроля целостности; регистрация событий;
11. Классификация методов криптографического преобразования информации; методы стеганографии и кодирования;
12. Требования к симметричным и асимметричным криптосистемам;
13. Алгоритм DES; свойства стандарта AES;
14. Стандарт ГОСТ 28145-89;
15. Функции хэширования, алгоритм MD5;
16. Электронная подпись; инфраструктура открытых ключей.

3.7 Перечень теоретических вопросов к экзамену

1. Основные понятия, термины и определения; предмет и объект защиты;
2. Уязвимости и угрозы безопасности информации в АИС; риски информационной безопасности (ИБ) и методы их оценки;
3. Правовые и организационные методы защиты информации в АИС; аудит ИБ;
4. Базовые принципы организации ЗИ;
5. Защита информации в АИС от несанкционированного доступа (НСД): подсистема идентификации и аутентификации (методы и средства);
6. Модели разграничения доступа к объектам: избирательное управление; мандатное управление; замкнутая программная среда;
7. Архитектура системы защиты информации (СЗИ) от НСД SecretNet;
8. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа;
9. СЗИ от НСД Dallas Lock: основные функциональные возможности;
10. Электронный замок Соболь-PCI: настройка и эксплуатация; управление пользователями; диагностика устройства; настройка контроля целостности; регистрация событий;
11. Классификация методов криптографического преобразования информации; методы стеганографии и кодирования;
12. Требования к симметричным и асимметричным криптосистемам;
13. Алгоритм DES; свойства стандарта AES;
14. Стандарт ГОСТ 28145-89;
15. Функции хэширования, алгоритм MD5;
16. Электронная подпись; инфраструктура открытых ключей.

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
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста
Курсовая работа	Ход выполнения разделов курсовой работы в рамках текущего контроля оценивается преподавателем исходя из объемов выполненных работ в соответствие со шкалами оценивания. Преподаватель информирует обучающихся о результатах оценивания выполнения курсового проекта сразу после контрольно-оценочного мероприятия. В ходе защиты курсовой работы обучающийся делает доклад протяженностью 5 – 7 минут. Преподаватель ставит окончательную оценку за курсовую работу после завершения защиты, учитывая уровень ее защиты

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 зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

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.

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 «Основы управления информационной безопасностью»**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1. Основные понятия, термины и определения; предмет и объект защиты 2. Уязвимости и угрозы безопасности информации в АИС; риски информационной безопасности (ИБ) и методы их оценки 3. Стандарт ГОСТ 28145-89 4. Требования к симметричным и асимметричным криптосистемам		