

ИРКУТСК
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказ ректора
от «07» июня 2021 г. № 78

Б1.О.46 Аудит информационных технологий и систем обеспечения информационной безопасности

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – 5 лет 6 месяцев, очная форма
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 4
Часов по учебному плану (УП) – 144

Формы промежуточной аттестации в семестрах
экзамен- А.

Распределение часов дисциплины по семестрам

Семестр	А	Итого
Число недель в семестре	17	
Вид занятий	Часов по УП	Часов по УП
Аудиторная контактная работа по видам учебных занятий/ в форме ПП*	68	68
– лекции	34	34
– практические (семинарские)	34	34
– лабораторные	-	-
Самостоятельная работа	40	40
Экзамен	36	36
Итого	144	144

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Электронный документ выгружен из ЕИС ФГБОУ ВО ИрГУПС и соответствует оригиналу

Подписант ФГБОУ ВО ИрГУПС Трофимов Ю.А.

00a73c5b7b623a969ccad43a81ab346d50 с 08.12.2022 14:32 по 02.03.2024 14:32 GMT+03:00

Подпись соответствует файлу документа



Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки России от 26.11.2020 г. № 1457.

Программу составил:

к.э.н., доцент

_____ С.П. Серёдкин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «04» июня 2021 г. № №11/2.

И.о. заведующий кафедрой, к. э. н, доцент

_____ Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	изучение видов, практических методов и средств проведения аудита информационной безопасности (ИБ) информационных технологий (ИТ) и систем обеспечения ИБ (СОИБ).
1.2 Задачи дисциплины	
1	изучение основных понятий аудита информационной безопасности, процессного подхода к организации информационной безопасности, состав основных требований к содержанию аудита информационной безопасности;
2	изучение процесса комплексного обследования информационной безопасности, методов оценивания информационной безопасности.
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
	<p>Цель воспитания обучающихся – разностороннее развитие личности будущего конкурентоспособного специалиста с высшим образованием, обладающего высокой культурой, интеллигентностью, социальной активностью, качествами гражданина-патриота.</p> <p>Задачи воспитательной работы с обучающимися:</p> <ul style="list-style-type: none"> – развитие мировоззрения и актуализация системы базовых ценностей личности; – приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям; – воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности как важнейшей черты личности, проявляющейся в заботе о своей стране, сохранении человеческой цивилизации; – воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях; – обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности; – выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации. – ориентация обучающихся на дальнейшую работу по решению экономических задач

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
	Б1.О.53 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта
	Б1.О.55 Защита объектов критической информационной инфраструктуры
	Б2 Б1.О.54 Методы и средства криптографической защиты информации
	В.02(П) Производственная - эксплуатационная
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.58 Обработка и анализ больших данных
2	Б1.О.59 Проектирования систем защиты объектов информатизации
3	Б1.О.60 Защита информации от несанкционированного доступа
4	Б1.О.62 Моделирование процессов и систем защиты информации
5	Б2.В.05(Пд) Производственная - преддипломная практика

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование Компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-6 Способен при решении профессиональных задач организовывать защиту информации	ОПК-6.1; Знает основные принципы административно-правовой защиты информации в соответствии с нормативными	Знать: Законодательную базу, нормативно-методические документы ФСБ, ФСТЭК, российские стандарты в области ИБ; Системы обеспечения ИБ объектов

<p>ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;</p>	<p>правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ОПК-6.2 Умеет быстро реагировать на различные угрозы информационной безопасности и организывает защиту информации ограниченного доступа</p>	<p>информатизации в соответствии с требованиями законодательства, ФОИБ в области защита информации и российских стандартов.</p> <p>Уметь: Анализировать направления развития информационных технологий в области ИБ; Анализировать эффективность функционирования ИТ в области ИБ; Анализировать и оценивать риски реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ</p> <p>Владеть: Навыками анализа нормативно-методических документов и российских стандартов в области ИБ. Навыками применения расчетов эффективности функционирования ИТ в области ИБ. Навыками анализа и оценки рисков реализации угроз информационной безопасности объектов и систем в соответствии с требованиями стандартов в области ИБ</p>
<p>ОПК-13Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;</p>	<p>ОПК-13.1Знает основы диагностики и тестирования систем защиты информации автоматизированных систем. ОПК-13.2Умеет проводить анализ защищенности, в том числе выявлять и оценивать опасность уязвимостей систем защиты информации и угроз информационной безопасности автоматизированных систем</p>	<p>Знать; Требования законодательства, руководящих документов ФСТЭК для создания системы ЗИ на объектах информатизации. Методики проведения аудита информационных технологий и систем обеспечения информационной безопасности в АС; Методики разработки политики информационной безопасности организации. Этапы создания системы обеспечения информационной безопасности и способы реализации эффективной системы организационной защиты информации.</p> <p>Уметь: Формировать проект необходимых мер обеспечению ИБ в зависимости от специфики функционирования АС. Провести аудит АС ОИ по требованиям ИБ с формированием соответствующих проектных решений. Анализировать современные методики проведения аудита ИБ с целью повышения эффективности инвестиций в ЗИ.</p> <p>Владеть: Навыками анализа полного набора необходимых мер обеспечения ИБ в зависимости от специфики функционирования ИС для повышения эффективности средств ЗИ. Практическими приемами проведения аудита ИБ, методами сбора данных, оценки рисков, анализа защищенности с целью подготовки предложений по повышению уровня защиты информации. Методиками обоснования инвестиций в защиту информации для обеспечения целей аудита ИБ.</p>

Код	Наименование разделов, тем и видов работы	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	СР	
1.0	Раздел 1. Базовые сведения о проверке и оценке уровня ИБ организации	А	6	6		8	
1.1	Проверки и оценки уровня ИБ организации /Лек/		6				ОПК-13
1.2	Подготовка к практическим занятиям на тему «Проверки и оценки уровня ИБ организации» /Ср/					8	ОПК-6
1.3	Проверки и оценки уровня ИБ организации /Пр/			6			ОПК-6 ОПК-13
2.0	Раздел 2. Аудит ИБ организации: общие понятия и определения	А	8	8		10	
2.1	Базовые определения /Лек/		8				ОПК-13
2.2	Подготовка к практическим занятиям на тему «Базовые определения» /Ср/					6	ОПК-6 ОПК-13
2.3	Базовые определения /Пр/			4			ОПК-13
	Принципы и формы аудита ИБ организации /Лек/		8				ОПК-6
2.4	Подготовка к практическим занятиям на тему «Принципы и формы аудита ИБ организации» /Ср/					4	ОПК-6
2.5	Принципы и формы аудита ИБ организации /Пр/			4			ОПК-13
3.0	Раздел 3. Стандарты проведения аудита ИБ	А	8	8		10	
3.1	Стандарты в области управления ИБ /Лек/		4				ОПК-6
3.2	Подготовка к практическим занятиям на тему «Стандарты в области управления ИБ» /Ср/					6	ОПК-6
3.3	Стандарты в области управления ИБ /Пр/			4	-		
3.4	Стандарты управление рисками ИБ /Лек/		4				ОПК-6
3.5	Подготовка к практическим занятиям на тему «Стандарты управление рисками ИБ» /Ср/					4	ОПК-6
3.6	Стандарты управление рисками ИБ /Пр/			4	-		ОПК-6
4.0	Раздел 4. Методология аудита ИБ. Организация процесса аудита ИБ	А	8	8		10	
4.1	Основные этапы и методы работ по проведению аудита /Лек/		2				ОПК-13
4.2	Подготовка к практическим занятиям на тему «Основные этапы и методы работ по проведению аудита ИБ» /Ср/					2	ОПК-6
4.3	Основные этапы и методы работ по проведению аудита ИБ /Пр/			4			ОПК-6
4.4	Сбор свидетельств (исходной информации) для проведения аудита ИБ /Лек/		4				ОПК-6 ОПК-13
4.5	Подготовка к практическим занятиям на тему «Сбор свидетельств (исходной информации) для проведения аудита» /Ср/					4	ОПК-6 ОПК-13
4.6	Сбор свидетельств (исходной информации) для проведения аудита /Пр/			2			ОПК-13
4.7	Рекомендации по планированию аудита ИБ /Лек/		2				ОПК-13
4.8	Подготовка к практическим занятиям на тему «Рекомендации по планированию аудита ИБ» /Ср/					4	ОПК-13
4.9	Рекомендации по планированию аудита ИБ /Пр/			2			
5.0	Раздел 5. Инструментальные средства аудита ИБ	А	2	4		2	ОПК-6 ОПК-13

5.1	Методы и инструментальные средства проведения аудита ИБ /Лек/		2	4		2	ОПК-13
6.0	Раздел 6. Экзамен					36	ОПК-6 ОПК-13
6.1	Завершающий экзамен по курсу /Экзамен/						

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	

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.1	В.В. Персианов, Е.З. Киреева, М.Н. Казакова	Электронное офисное делопроизводство: учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=434743	М. ; Берлин : Директ-Медиа, 2016	100% онлайн
6.1.2	А.Н. Кристалюк	Конфиденциальное делопроизводство и защита коммерческой тайны: курс лекций [Электронный ресурс] http://biblioclub.ru/index.php?page=book&id=428611	Орел : МАБИВ, 2014	100% онлайн
6.1.3	Ю.М. Краковский	Информационная безопасность и защита информации: учебное пособие	Иркутск: ИрГУПС, 2016	93

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	И.В. Минин, О.В. Минин	Защита конфиденциальной информации при электронном документообороте : учебное пособие [Электронный ресурс] biblioclub.ru/index.php?page=book&id=228779	Новосибирск : НГТУ, 2011	100% онлайн
6.1.2.2	М.А. Лапина, А.Г. Ревин, В.И. Лапин	Информационное право: учебное пособие [Электронный ресурс] biblioclub.ru/index.php?page=book&id=118624	М. : Юнити-Дана, 2015	100% онлайн
6.1.2.3	О.В. Порядина	Управление информационными ресурсами: учебно-методическое пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=439328	Поволжский государственный технологический университет. - Йошкар-Ола, 2015	100% онлайн

6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)

	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
6.1.3.1	Глухов Н.И.	Оценка информационных рисков предприятия:	- Иркутск:	67

		учеб. пособие/ Н. И. Глухов; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ... - 148 с	ИрГУПС, 2013	
6.1.3.2	А.А. Бутин	Методы и средства защиты информации от несанкционированного доступа. Программно-аппаратный уровень: учеб. пособие http://www.irgups.ru/ntb/Jirbis/index.php?option	Иркутск: ИрГУПС, 2015	100% онлайн

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»

6.2.1	Сайт ФСТЭК РФ http://fstec.ru/
6.2.2	Сайт ФСБ РФ http://www.fsb.ru/
6.2.3	Сайт производителя Dr. Web Cureit! http://free.drweb.ru/
6.2.4	Сайт «Код безопасности» http://www.securitycode.ru
6.2.5	Сайт производителя Acronis http://www.acronis.com/ru-ru/
6.2.6	Сайт производителя 360 Total Security http://360-total-security.besplatnyeprogrammy.ru/
6.2.7	Сайт производителя Dallas Lock https://www.dallaslock.ru/
6.2.8	Сайт производителя линейки «ViPNet» http://www.infotecs.ru/
6.2.9	Сайт производителя ruToken http://www.rutoken.ru/
6.2.10	Искусство управления информационной безопасностью http://www.iso27000.ru
6.2.11	DLP-системы https://www.infowatch.ru/dlp
6.2.12	Материалы «Комплексная защита информации в компьютерных системах» /http://padaread.com

6.3 Программное обеспечение и информационные справочные системы

6.3.1 Базовое программное обеспечение

6.3.1.1	ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844, обновление - Контракт № 0334100010016000113-0000756-02 от 25.11.2016г., обновление - договор №31705062861 от 06.06.2017 АО СофтЛайнТрейд, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083, обновление - Контракт № 0334100010016000113-0000756-02 от 25.11.2016г., обновление - договор №31705062861 от 06.06.2017 АО СофтЛайнТрейд, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org

6.3.2 Специализированное программное обеспечение

6.3.2.1	Сканер MBSA (свободное ПО);
6.3.2.2	«Сканер-ВС» (свободное ПО для вузов);
6.3.2.3	СЗИ от НСД SecretNet (лицензия);
6.3.2.4	Персональные идентификаторы ruToken;
6.3.2.5	Электронный замок Соболь-РСИ;
6.3.2.6	СЗИ НСД Dallas Lock (свободное ПО для вузов);
6.3.2.7	Пакет PrZamena (свободное ПО);
6.3.2.8	Dr.Web Cureit! (свободное ПО);
6.3.2.9	360 Total Security (свободное ПО).

6.3.3 Информационные справочные системы

6.3.3.1	КонсультантПлюс – студенческая версия (Онлайн-версия КонсультантПлюс: Студент, https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.8160556428138959)
---------	--

6.4 Правовые и нормативные документы

6.4.1	Федеральный закон от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».
6.4.2	Федеральный закон от 26 июня 2017г. №187-ФЗ «О безопасности критической информационной

	инфраструктуры Российской Федерации».
6.4.3	Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) "О персональных данных"
6.4.4	Федеральный закон от 04 мая 2011г. №99-ФЗ «О лицензировании отдельных видов деятельности».
6.4.5	Федеральный закон от 29 июня 2015г. №162-ФЗ «О стандартизации отдельных видов деятельности».
6.4.6	Перечень сведений, отнесенных к государственной тайне. Утвержден указом Президента Российской Федерации от 30 ноября 1995г. №1203.
6.4.7	Правила категорирования объектов критической инфраструктуры Российской Федерации. Утверждены Постановлением Правительства Российской Федерации от 08 февраля 2018г. №127.
6.4.8	Нормативно-правовые акты государственных, муниципальных органов, предприятий в области ин-формационной безопасности

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 – по адресу г. Иркутск, ул. Лермонтова, д.80.
2	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины: Д-518,521,623,Д-216.
3	Учебная лаборатория «Информационной безопасности транспортной инфраструктуры» -Д-525. Оснащение лаборатории: Автоматизированное рабочее место преподавателя в составе: ПЭВМ, Принтер LCD. Операционная система. Офисные программы. Антивирусные программы. Автоматизированное рабочее место обучающегося (в расчете – одно рабочее место на одного обучающегося) в составе: ПЭВМ. Операционная система. Офисные программы. Антивирусные программы. Программное обеспечение для проведения компьютерных тестов. Учебные лабораторные комплексы для: Контроля сетевой безопасности (системы обнаружения вторжений и анализа защищенности, сетевые сканеры; Проведения анализа защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности.
4	Помещения для самостоятельной работы обучающихся: – Читальный зал А-606. Учебная мебель, стеллажи, витрина, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, мультимедийный проектор, экран. – Аудитория Д-523,508,514. Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, мультимедийный проектор, экран.
5	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.

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.

	<p>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. В конспект рекомендуется выписывать определения, формулировки и доказательства теорем, формулы и т.п. На полях конспекта следует пометить вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запомнились. Полезно составить краткий справочник, содержащий определения важнейших понятий и наиболее часто употребляемые формулы дисциплины. К каждой лекции 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. При этом необходимо воспроизводить на бумаге все рассуждения, как имеющиеся в учебнике или конспекте, так и пропущенные в силу их простоты. 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 удастся разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии</p>
<p>Практическое занятие</p>	<p>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.</p> <p>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.</p> <p>Особое внимание следует обращать на определение основных понятий дисциплины. Обучающийся должен подробно разбирать примеры, которые поясняют понятия</p>
<p>Самостоятельная работа</p>	<p>Обучение по дисциплине предусматривает активную самостоятельную работу обучающегося. На самостоятельную работу отводится 38 часов по очной форме обучения. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а так же 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). 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 удастся, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора.</p>
<p>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.</p>	

№ п/п	Часть текста, подлежавшего изменению в документе			Общее количество страниц		Основание для внесения изменения, № документа	Подпись отв. исп.	Дата
	№ раздела	№ пункта	№ подпункта	до внесения изменений	после внесения изменений			

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

**для проведения текущего контроля успеваемости
и промежуточной аттестации по дисциплине
Б1.О.46 Аудит информационных технологий и систем
обеспечения информационной безопасности**

Приложение № 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – № 5 "Безопасность открытых информационных систем"

ИРКУТСК

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 Университета, а так же 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 «Аудит информационных технологий и систем обеспечения информационной безопасности» участвует в формировании компетенции:

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

ОПК-13 Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем.

Программа контрольно-оценочных мероприятий

очная форма обучения

№	Недел я	Наименование контрольно- оценочного мероприятия	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатор а достижени я	Наименование оценочного средства (форма проведения*)
---	------------	--	--	---	--

				компете н и	
1.	23-28		Раздел 1. Базовые сведения о проверке и оценке уровня ИБ организации		
2.		Текущий контроль	Проверки и оценки уровня ИБ организации /Лек/	ОПК-13	Конспект (письменно). Компьютерные технологии
3.		Текущий контроль	Подготовка к практическим занятиям на тему «Проверки и оценки уровня ИБ организации» /Ср/	ОПК-6	Конспект (письменно). Компьютерные технологии
4.			Раздел 2. Аудит ИБ организации: общие понятия и определения		.
5.		Текущий контроль	Базовые определения /Лек/	ОПК-13	Конспект (письменно). Компьютерные технологии
6.		Текущий контроль	Подготовка к практическим занятиям на тему «Базовые определения» /Ср/	ОПК-6 ОПК-13	Конспект (письменно). Компьютерные технологии
7.		Текущий контроль	Базовые определения /Пр/	ОПК-13	Конспект (письменно). Дискуссия на практических занятиях
8.		Текущий контроль	Принципы и формы аудита ИБ организации /Лек/	ОПК-6	Конспект (письменно). Компьютерные технологии
9.		Текущий контроль	Подготовка к практическим занятиям на тему «Принципы и формы аудита ИБ организации» /Ср/	ОПК-6	Конспект (письменно). Компьютерные технологии
10.		Текущий контроль	Принципы и формы аудита ИБ организации /Пр/	ОПК-13	Конспект (письменно). Дискуссия на практических занятиях
11.	29.-35		Раздел 3. Стандарты проведения аудита ИБ		
12.		Текущий контроль	Стандарты в области управления ИБ /Лек/	ОПК-6	Конспект (письменно). Компьютерные технологии
13.		Текущий контроль	Подготовка к практическим занятиям на тему «Стандарты в области управления ИБ» /Ср/	ОПК-6	Конспект (письменно). Компьютерные технологии
14.		Текущий контроль	Стандарты в области управления ИБ /Пр/		Конспект (письменно). Дискуссия на практических занятиях
15.		Текущий контроль	Стандарты управление рисками ИБ /Лек/	ОПК-6	Конспект (письменно). Компьютерные технологии
16.		Текущий контроль	Подготовка к практическим занятиям на тему «Стандарты управление рисками ИБ» /Ср/	ОПК-6	Конспект (письменно). Компьютерные технологии
17.		Текущий контроль	Стандарты управление рисками ИБ /Пр/	ОПК-6 ОПК-13	Конспект (письменно). Дискуссия на практических занятиях
18.		Текущий контроль	Раздел 4. Методология аудита ИБ. Организация процесса аудита ИБ	ОПК-6 ОПК-13	Дискуссия на практических занятиях
19.		Текущий контроль	Раздел 5. Инструментальные средства аудита ИБ		
20.		Текущий контроль	Методы и инструментальные средства проведения аудита ИБ /Лек/	ОПК-13	Конспект (письменно).
21.	36-38	Тест	Тест по курсу	ОПК-6 ОПК-13	Тест Перечень вопросов к тестовому заданию.
22.	39	Экзамен	Экзамен по курсу		Собеседование (устно), комплект экзаменационных

					билетов
--	--	--	--	--	---------

Описание показателей и критериев оценивания компетенций.

Описание шкал оценивания

Контроль качества освоения дисциплины/прохождения практики 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/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а так же краткая характеристика этих средств приведены в таблице

№	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 по темам/разделам дисциплины
2	Реферат	Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор реферата раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Может быть использовано для оценки знаний и умений обучающихся	Темы рефератов
3	Сообщение, доклад	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
5	Зачет	Средство, позволяющее оценить знания, умения, навыки 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 (билетов) к зачету

**Критерии и шкалы оценивания компетенций в результате изучения дисциплины
«Аудит информационных технологий и систем обеспечения информационной
безопасности» при проведении промежуточной аттестации
в форме зачета. Шкала оценивания уровня освоения компетенций**

Шкалы 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 полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«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

**Критерии и шкалы оценивания результатов обучения при проведении
текущего контроля успеваемости**

Собеседование

Шкала оценивания	Критерии оценивания
«отлично»	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 было попытки выполнить задание

Реферат

Шкала оценивания	Критерии оценивания
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы
«удовлетворительно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод
«неудовлетворительно»	Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы. Реферат обучающимся не представлен

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Используются дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint, Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

Оценочное средство «Тест».

Тестирование с применением компьютерных технологий проводится по окончании каждого семестра (если дисциплина не является односеместровой) и по окончании изучения дисциплины и (или) в течение года по завершению изучения дисциплины (контроль/проверка остаточных знаний, умений, навыков и (или) опыта деятельности).

Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры тестов по итогам каждого семестра (если дисциплина не является односеместровой) и итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.

Результаты тестирования могут быть использованы при проведении промежуточной аттестации в экзаменах.

Промежуточная аттестация в форме экзамена – результаты тестирования могут являться допуском к экзамену:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	Обучающийся к экзамену допущен

Обучающийся набрал при тестировании менее 69 баллов	Обучающийся к экзамену не допущен
---	-----------------------------------

Преподаватель вправе предусмотреть тесты для самоконтроля обучающихся по разделам дисциплины, сформировав их из материалов фонда тестовых заданий дисциплины. Требования к тестам для самоконтроля аналогичны требованиям к итоговым тестам по семестрам и дисциплине в целом.

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

3.1 Собеседование

Вопросы для собеседования

1. Понятие аудита информационной безопасности, его цели и задачи
2. Основные направления аудита ИБ
3. Функционал аудита
4. Варианты решения проблемы несоответствия имеющихся систем ИБ современным возможностям
5. Возможности современных методик анализа рисков аудита ИБ, проектирования и сопровождения СБ
6. Аудит информационных систем определение
7. Этапы работ по аудиту безопасности информационных систем
8. Особенности автоматизированных информационных систем как объектов аудита ИБ.
9. Преимущества проведения этапа анализа рисков
10. Методы анализа данных аудита
11. Структура отчета по результатам аудита безопасности ИС и анализу рисков (рекомендации по результатам).

3.2 Реферат

Темы рефератов

1. Место и роль аудита в модели обеспечения ИБ учреждения
2. Сертификация и аттестация ИТ и систем управления ИБ (СУИБ) как разновидности аудита.
3. Понятия аудита и аудита ИБ.
4. Программа аудита ИБ.
5. Необходимость и актуальность аудита ИБ.
6. Особенности автоматизированных информационных систем как объектов аудита ИБ
7. Виды аудита информационной безопасности
8. Принципы и формы аудита ИБ организации
9. Стандарты проведения аудита ИБ
10. Нормативы для проведения аудита ИБ организации
11. Этапы проведения внутреннего и внешнего аудитов ИБ.
12. Стадии аудита ИБ.
13. Методы аудита ИБ.
14. Инициирование процедуры аудита ИБ.
15. Порядок планирования аудита.
16. Анализ значимости информационных ресурсов.
17. Анализ процесса обработки информации.
18. Взаимодействие аудиторской организации и проверяемой организации.
19. Методы обследования на этапе моделирования.
20. Цель, методы и порядок проведения тестирования для проведения аудита ИБ.

21. Тестовые испытания функций защиты от НСД и защиты от утечки по техническим каналам при проведении аудита ИБ.
22. Моделирование действий злоумышленника при реализации угрозы несанкционированного доступа.
23. Особенности тестовых испытаний рабочих станций (АРМ), серверного оборудования, межсетевых экранов, маршрутизаторов, коммутаторов VHN-устройств.
24. Анализ организационно—распорядительных документов, выполнения организационно-технических требований, деятельности персонала, сотрудников при проведении аудита ИБ.
33. Аудит информационной безопасности при обеспечении непрерывности бизнес процессов и восстановления после сбоев.

3.3 Перечень тем типовых докладов, сообщений

Темы доклада, сообщения:

1. Нормативно- правовая основа обеспечения аудита информационной безопасности.
2. Аудит выделенных помещений как этап аудита информационной безопасности организаций.
3. Проведение анализа рисков при проведении аудита информационно технических систем обеспечения информационной безопасности
4. Рекомендации по совершенствованию системы защиты информации, как заключительный этап аудита организации
5. Обзор программных продуктов, предназначенных для анализа безопасности информационных систем
6. Практический аудит информационной безопасности организаций и систем
7. Аудит информационной безопасности, основные понятия, определения, этапы, виды и направления деятельности
8. Сбор информации – этап проведения аудита
9. Анализ и обработка информации при проведении аудита
10. Отчет о результатах проведения Аудита ИБ

3.4 Перечень типовых теоретических вопросов к экзамену

Раздел 1 по раздел 5:

1. Что представляет собой аудит информационных систем?
2. Что представляет собой аудит информационной безопасности?
3. Раскройте три составляющие услуги аудита?
4. Раскройте основные направления деятельности в области аудита безопасности информации?
5. Что представляет собой аудит информационной безопасности информационных технологий?
6. Что представляет собой комплексный аудит информационной безопасности ИТ?
7. Что представляет собой аудит безопасности внешнего периметра корпоративной сети?
8. Что включает собой обследование внешнего периметра корпоративной сети на предмет защищенности?
9. Что представляет собой аудит безопасности отдельных объектов ИТ-инфраструктуры?
10. Что представляет собой техническая экспертиза продуктов и решений по обеспечению информационной безопасности?
11. Что представляет собой контроль защищенности информации ограниченного доступа?
12. Раскройте виды аудита информационной безопасности?
13. Что представляет собой активный аудит?
14. Что представляют собой результаты активного аудита
15. «Внутренний» активный аудит?

16. Что представляет собой экспертный аудит?
17. Что представляет собой аудит на соответствие стандартам?
18. Что представляют собой зарубежные и международные стандарты по Аудиту ИБ?
19. Что представляют собой аудит выделенных помещений?
20. Что представляют собой аудит предварительный осмотр объекта?
21. Назовите основной перечень специального оборудования и технических средств, рекомендуемых для проведения аудита помещений.
22. Раскройте этапы непосредственного проведения аудита.
23. Что представляют собой международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности?
24. В чем заключается основная роль стандартов по аудиту информационной безопасности?
25. Раскройте влияние международных стандартов на национальные стандарты и руководства по основам аудита информационной безопасности?
26. Что представляет собой оценивание результатов аудита и самооценки информационной безопасности?
27. Что представляет собой риск-ориентированная интерпретация полученных оценок информационной безопасности?
28. Раскройте особенности аудита информационной безопасности организаций банковской системы Российской Федерации.
29. Раскройте особенности развития средств и систем автоматизации.
30. Раскройте основные направления обеспечения и оценки информационной безопасности.
31. Назовите основные цели аудита информационной безопасности.
32. Назовите основные вопросы, рассматриваемые при аудите информационной безопасности.
33. Назовите основные особенности аудита информационной безопасности организаций, использующих аутсорсинг.

3.5 Тестирование по дисциплине

3.5.1 Структура фонда тестовых заданий по дисциплине

Структура фонда тестовых заданий по дисциплине «Аудит информационных технологий и систем защиты информации»

Раздел дисциплины	Тема раздела	Объект темы	Количество тестовых заданий (ТЗ), типы ТЗ
1. Базовые сведения о проверке и оценке уровня ИБ организации	1.1 Проверки и оценки уровня ИБ организации 1.2 Уровни защищенности ИС	1.1.1 Объекты проверки	5 – тип А
		1.1.2 Уровни оценки защищенности информации	5 – тип А
		1.1.3 Носители защищаемой информации как объект аудита	5 – тип А
	1.3 Проверки и оценки уровня ИБ организации	1.2.1. Способы оценки ИБ	5 – тип А
		1.2.2. Методы оценки ИБ	4 – тип А 6 – тип В 6 – тип Д
Итого по разделу			\sum 36 24 – тип А 6 – тип В 6 – тип Д
2. Аудит ИБ организации: общие понятия и определения	2.1 Базовые определения	2.1.1 Глоссарий	5 – тип А
		2.1.2 Базовые определения и термины по Аудиту ИБ	5 – тип А

		2.1.3 Основные характеристики объектов защиты	5 – тип А
	2.2 Принципы и формы аудита ИБ организации	2.2.1 Принципы аудита	5 – тип А 4 – тип Д
		2.2.2 Формы и виды аудита	4 – тип А 6 – тип В 2 – тип Д
Итого по разделу			$\sum 36$ 24 – тип А 6 – тип В 6 – тип Д
3. Стандарты проведения аудита ИБ	3.1 Классификация стандартов	3.1.1 Виды стандартов	6 – тип А
		3.1.2 Стандарты по аудиту ИБ	4 – тип С
	3.2 Технические регламенты аудита	3.2.1 Требования РД и ТР	6 – тип А 4 – тип Д
		3.2.2 Области применения	3 – тип А 4 – тип Д
		3.2.3 Международные стандарты по аудиту	3 – тип А 6 – тип В
Итого по разделу			$\sum 36$ 18 – тип А 6 – тип В 4 – тип С 8 – тип Д
4. Методология аудита ИБ. Организация процесса аудита ИБ	4.1. Основные этапы и методы работ по проведению аудита	4.1.1 Подготовка плана аудита	1 – тип А
		4.2. Сбор свидетельств (исходной информации) для проведения аудита ИБ	4.2.1 Сбор предварительной информации об объекте
	4.2.2 Техническое задание		1 – тип А
	4.3. Рекомендации по планированию аудита ИБ	4.3.1 Необходимые условия для реализации требований	1 – тип А 1 – тип Д
		4.3.2 Условия для заключения договора на аудит	1 – тип С 1 – тип Д
	4.4. Определение границ аудита	4.4.1 Исследование ИС объекта	1 – тип А 1 – тип Д
		4.4.2 Предварительный анализ данных	1 – тип В 1 – тип Д
			4.4.3 Согласование объема и границ работ
	4.5 Подготовка отчета	4.5.1 Необходимые мероприятия по исследованию ИС на проникновение	1 – тип А
		4.5.2. Анализ данных исследований	1 – тип А 1 – тип В 1 – тип С 1 – тип Д
	4.6 Рекомендации по итогам аудита	4.6.1 Основные требования по подготовке рекомендаций	1 – тип А
		4.6.2 Структура документа	1 – тип А
	4.7. Процедура аудита	4.7.1 Сбор и анализ данных	1 – тип А

		4.7.2 Мероприятия по проверке СЗИ ИС	1 – тип А
	4.8 Организационные мероприятия для проведения аудита	4.8.1 Требования к составу рабочей группы Заказчика	1 – тип А
		4.8.2 Проектное задание на аудит	1– тип А 1– тип В 1– тип С 1– тип Д
	4.9 Особенности аудита при передаче услуг на аутсорсинг	4.9.1 Границы аудита при аутсорсинге	2– тип А 1– тип В 1– тип С 1– тип Д
		4.9.2 Требования к процедуре аудита при аутсорсинге	1– тип А 1– тип В 1– тип С 1– тип Д
Итого по разделу			$\sum 36$ 17– тип А 5– тип В 5– тип С 9– тип Д
5.Инструментальные средства аудита ИБ	5.1. Классификация инструментальных средств для аудита	5.1.1 Инструментальные средства для аудита, требования	5 – тип А
		5.1.2. Нормативно-методические требования к инструментальным средствам	5 – тип А
	5.2Преимущества и недостатки инструментальных средств аудита. Заключение	5.2.1 Основные возможности инструментальных средств	5 – тип А 4 – тип Д
		5.2.2 Требования к оформлению результатов исследования	5 – тип А 4– тип Д
		5.2.3 Оформление результатов	5 – тип А 3 – тип Д
Итого по разделу			$\sum 36$ 25– тип А 11– тип Д
Итого по дисциплине			$\sum 180$ 108– тип А 23– тип В 9– тип С 40– тип Д

Используемые типы тестовых заданий (ТЗ):

ТЗ типа А: тестовое задание закрытой формы (ТЗ с выбором одного или нескольких правильных ответов);

ТЗ типа В: тестовое задание открытой формы (с конструируемым ответом: ТЗ с кратким регламентируемым ответом (ТЗ дополнения); ТЗ свободного изложения (с развернутым ответом в произвольной форме);

ТЗ типа С: тестовое задание на установление соответствия;

ТЗ типа Д: тестовое задание на установление правильной последовательности.

3.5.2. Структура и образец типового итогового теста по дисциплине

**«Аудит информационных технологий и систем защиты информации»
за весь период ее освоения**

Структура типового итогового теста по дисциплине за весь период ее освоения

Раздел дисциплины	Тема раздела	Объект темы	Количество тестовых заданий (ТЗ), типы ТЗ
1. Базовые сведения о проверке и оценке уровня ИБ организации	1.1 Проверки и оценки уровня ИБ организации 1.2 Уровни защищенности ИС	1.1.1 Объекты проверки	5 – тип А
		1.1.2 Уровни оценки защищенности информации	5 – тип А
		1.1.3 Носители защищаемой информации как объект аудита	5 – тип А
	1.3 Проверки и оценки уровня ИБ организации	1.2.1. Способы оценки ИБ	5 – тип А
		1.2.2. Методы оценки ИБ	4 – тип А 6 – тип В 6 – тип Д
Итого по разделу			$\sum 36$ 24 – тип А 6 – тип В 6 – тип Д
2. Аудит ИБ организации: общие понятия и определения	2.1 Базовые определения	2.1.1 Глоссарий	5 – тип А
		2.1.2 Базовые определения и термины по Аудиту ИБ	5 – тип А
		2.1.3 Основные характеристики объектов защиты	5 – тип А
	2.2 Принципы и формы аудита ИБ организации	2.2.1 Принципы аудита	5 – тип А 4 – тип Д
		2.2.2 Формы и виды аудита	4 – тип А 6 – тип В 2 – тип Д
Итого по разделу			$\sum 36$ 24 – тип А 6 – тип В 6 – тип Д
3. Стандарты проведения аудита ИБ	3.1 Классификация стандартов	3.1.1 Виды стандартов	6 – тип А
		3.1.2 Стандарты по аудиту ИБ	4 – тип С
	3.2 Технические регламенты аудита	3.2.1 Требования РД и ТР	6 – тип А 4 – тип Д
		3.2.2 Области применения	3 – тип А 4 – тип Д
		3.2.3 Международные стандарты по аудиту	3 – тип А 6 – тип В
Итого по разделу			$\sum 36$ 18 – тип А 6 – тип В 4 – тип С 8 – тип Д
4. Методология аудита ИБ. Организация процесса аудита ИБ	4.1. Основные этапы и методы работ по проведению аудита	4.1.1 Подготовка плана аудита	1 – тип А
		4.2.1 Сбор предварительной информации об объекте	1 – тип А

	4.2. Сбор свидетельств (исходной информации) для проведения аудита ИБ	4.2.2 Техническое задание	1 – тип А
	4.3. Рекомендации по планированию аудита ИБ	4.3.1 Необходимые условия для реализации требований	1 – тип А 1 – тип Д
		4.3.2 Условия для заключения договора на аудит	1 – тип С 1 – тип Д
	4.4. Определение границ аудита	4.4.1 Исследование ИС объекта	1 – тип А 1 – тип Д
		4.4.2 Предварительный анализ данных	1 – тип В 1 – тип Д
		4.4.3 Согласование объема и границ работ	1 – тип А 1 – тип Д
	4.5 Подготовка отчета	4.5.1 Необходимые мероприятия по исследованию ИС на проникновение	1 – тип А
		4.5.2. Анализ данных исследований	1– тип А 1– тип В 1– тип С 1– тип Д
	4.6 Рекомендации по итогам аудита	4.6.1 Основные требования по подготовке рекомендаций	1 – тип А
		4.6.2 Структура документа	1 – тип А
	4.7. Процедура аудита	4.7.1 Сбор и анализ данных	1 – тип А
		4.7.2 Мероприятия по проверке СЗИ ИС	1 – тип А
	4.8 Организационные мероприятия для проведения аудита	4.8.1 Требования к составу рабочей группы Заказчика	1 – тип А
		4.8.2 Проектное задание на аудит	1– тип А 1– тип В 1– тип С 1– тип Д
	4.9 Особенности аудита при передаче услуг на аутсорсинг	4.9.1 Границы аудита при аутсорсинге	2– тип А 1– тип В 1– тип С 1– тип Д
		4.9.2 Требования к процедуре аудита при аутсорсинге	1– тип А 1– тип В 1– тип С 1– тип Д
Итого по разделу			∑ 36 17– тип А 5– тип В 5– тип С 9– тип Д
5.Инструментальные средства аудита ИБ	5.1. Классификация инструментальных средств для аудита	5.1.1 Инструментальные средства для аудита, требования	5 – тип А
		5.1.2. Нормативно-методические требования к инструментальным средствам	5 – тип А
	5.2Преимущества и недостатки инструментальных средств аудита. Заключение	5.2.1 Основные возможности инструментальных средств	5 – тип А 4 – тип Д
		5.2.2 Требования к оформлению результатов исследования	5 – тип А 4– тип Д

	5.2.3 Оформление результатов	5 – тип А 3 – тип Д
Итого по разделу		$\sum 36$ 25– тип А 11– тип Д
.....	Итого по дисциплине	$\sum 180$ 108– тип А 23– тип В 9– тип С 40– тип Д

Образец типового итогового теста по дисциплине за весь период ее освоения

Описание требований к тесту: тематика теста; перечень знать, уметь, владеть; виды и количество предъявляемых обучающемуся тестовых заданий; проходной балл; критерии оценки; норма времени; дополнительные требования, включая необходимость использования справочных таблиц и проч.

Описание требований к тесту.

1. Тестирование осуществляется по изученным разделам;
2. Обучающемуся случайным образом дается 25 тестовых заданий из ФТЗ. Время на подготовку – 60 минут.
3. Оценивание осуществляется по 100-балльной системе. Для получения допуска к экзамену обучающийся должен набрать более 69 баллов.

Описание требований к тесту: итоговый тест по дисциплине предполагает оценку того, насколько студент:

– знает: Базовый понятийный аппарат в области экономических методов защиты информации; Виды и состав угроз в экономике защиты информации; Методы выявления рисков реализации угроз информационной безопасности; Принципы и общие методы определения ценности информации;

Основные положения государственной политики обеспечения информационной безопасности; Критерии, условия и принципы отнесения информации к защищаемой; Виды носителей защищаемой информации; Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;

Классификацию видов, методов и средств защиты информации.

– умеет: Анализировать состояние экономической безопасности организации и правильно определять роль защиты информации в ее обеспечении; Выбирать методы определения ущерба, наносимого владельцу информации в результате противоправного ее использования; Определять расчетным и экспертным методами стоимостные оценки ущерба, наносимого владельцу информации; Анализировать экономическую информацию, возникающую в процессе производственно-хозяйственной деятельности, и выработать рекомендации по экономической целесообразности ее защиты; Выбирать методы сопоставительного анализа эффективности инвестиционных проектов в защиту информации; Анализировать и классифицировать риски, возникающие при защите информации, изыскивать методы их расчетов; Определять объекты систем защиты информации, подлежащие первоочередному страхованию, и участвовать в разработке договоров о страховании.

- владеть навыками: Основами экономики защиты информации; Специальной профессиональной терминологией; Основными экономическими методами защиты информации.

Студенту необходимо выполнить 41 тестовых заданий. Максимальное количество составляет 100%. Проходной составляет 75%. Обучающийся, набравший более 75% правильных ответов

сдал тест, менее 75% – нет. Время на выполнение тестового задания – 60 минут.

Образец типового теста содержит задания для оценки знаний, для оценки умений, для оценки навыков и (или) опыта деятельности (необходимо указать все правильные ответы).

Образец типового теста содержит задания для оценки знаний, для оценки умений, для оценки навыков и (или) опыта деятельности.

1. Аудит информационных систем определение
 - А) Экспертная проверка ИТ-инфраструктуры с целью оценки работы всех процессов, связанных с хранением и передачей информации в организации;
 - Б) Проверка средств защиты информации целью оценки работы всех процессов, связанных с хранением и передачей информации в организации;
 - В) Проверка ИТ-инфраструктуры с целью оценки работы всех процессов, связанных с хранением и передачей информации в организации.
2. Что представляет собой аудит информационной безопасности
 - А) Системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности.
 - Б) Оценка уровня защищённости ИТ;
 - В) Процесс получения оценки уровня защиты информации.
3. Этапы проведения аудита
 - А) инициирование процедуры аудита;
 - Б) сбор информации по составу средств защиты информации;
 - В) анализ угроз безопасности.
4. Виды аудита информационной безопасности
 - А) Внутренний аудит;
 - Б) Внутренний аудит;
 - В) Экспертный аудит.
5. Аудит на соответствие стандартам
 - А) Состояние ИБ сравнивается с требованием стандартов;
 - Б) Состояние ИБ сравнивается с неким абстрактным описанием, приводимым в стандартах;
 - В) Состояние ИБ сравнивается с требованием руководящих документов.
6. Что представляет собой экспертный аудит

- А) Представляет собой сравнение состояния ИБ с "идеальным" описанием;
 - Б) Представляет собой сравнение состояния ИБ с требованием стандартов;
 - В) Представляет собой оценку экспертов.
7. Активный аудит, определение
- А) Исследование состояния защищенности информационной системы со стороны внешнего периметра;
 - Б) Оценка состояния защищенности информационной системы в границах внутреннего периметра сети;
 - В) Исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий).
8. Цели аудита информационной безопасности
- А) Оценка соответствия ИС существующим стандартам в области информационной безопасности;
 - Б) Подготовка аудиторского отчета;
 - В) Анализ рисков ИБ.
9. Что представляет собой комплексный аудит информационной безопасности:
- А) Процесс получения объективных качественных и количественных оценок о текущем состоянии защищенности информационных ресурсов компании в соответствии с российскими и международными нормативами.
 - Б) Исследование текущего состояние информационной безопасности организации;
 - В) Исследование системы для подготовки рекомендаций по повышению эффективности средств защиты информации.
10. Границы аудита, определение
- А) Перечень обследуемых информационных ресурсов и информационных систем;
 - Б) Перечень зданий в пределах, которых будет проводиться аудит;
 - В) Основные средства защиты, которые необходимо подвергнуть аудиту;
11. Необходимость и актуальность аудита ИБ.
- А) Оценка текущего уровня защищенности ИС;
 - Б) Оценка эффективности мероприятия по ЗИ ИС;
 - В) Наличие потенциальных угроз ИБ для ИС.
12. Назовите основные особенности аудита информационной безопасности организаций, использующих аутсорсинг

- А) Дополнительный объем работ;
- Б) Увеличения рисков ИБ;
- В) Снижение эффективности аудита.

13. Отчет о результатах проведения Аудита ИБ:

- А) Является обязательным этапом аудита;
- Б) Является составной частью рекомендация по результатам аудита;
- В) Является частью акта выполненных работ по договору аудита.

14. Рекомендации по результатам аудита:

- А) Являются обязательными для выполнения Заказчиком;
- Б) Являются не обязательным для выполнения Заказчиком;
- В) Носят рекомендательный характер для Заказчика.

15. Что представляют собой аудит выделенных помещений?

- А) Представляет собой оценку текущего состояния защищенности и безопасности помещений для реализации мероприятий по аудиту;
- Б) Представляет собой оценку текущего состояния защищенности и безопасности помещений для проведения мероприятий речевого характера по секретным или конфиденциальным вопросам;
- В) Представляет собой оценку текущего состояния безопасности помещений для хранения баз данных.

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	Темы собеседований, предусмотренные рабочей программой дисциплины, проводятся во время практических занятий. Преподаватель задает не менее двух вопросов по темам собеседований.. Во время выполнения собеседования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения собеседований, доводит до учащихся темы собеседований.
Реферат	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит реферат по результатам освоения темы, объемом до 15 стр. текста размером 12 пунктов, интервал 1,5; представляет сообщение/доклад преподавателю.
Сообщение, доклад	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в

	интернете), готовит сообщение или доклад по результатам освоения темы, объемом до 20 стр. текста размером 12 пунктов, интервал 1,5; представляет сообщение/доклад преподавателю, отвечает на его вопросы.
--	---

Для организации и проведения промежуточной аттестации (в форме экзамена) 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 к экзамену для оценки знаний;
- перечень типовых простых практических заданий к экзамену для оценки умений;
- перечень типовых практических заданий к экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к экзамену 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

При проведении промежуточной аттестации в форме экзамена могут быть использованы результаты тестирования:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	Обучающийся к экзамену допущен
Обучающийся набрал при тестировании менее 69 баллов	Обучающийся к экзамену не допущен

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что в 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; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье 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 ФОС на бумажном носителе в составе ФОС по дисциплине.

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.

Образец экзаменационного билета

 <p>ИрГУПС 2021-2022 учебный год</p>	<p>Экзаменационный билет № 1 по дисциплине «Аудит информационных технологий и систем обеспечения информационной безопасности»</p> <p>Специализация/профиль «Безопасность информационных систем и технологий»</p> <p>А семестр</p>	<p>Утверждаю: Заведующий кафедрой «ИСиЗИ» ИрГУПС Т.К. Кириллова</p>
---	---	---

1. Что представляет собой активный аудит?
2. Что представляют собой результаты активного аудита
3. «Внутренний» активный аудит Варианты размеров билета:
Билет формата А5 – 148*210мм
Билет формата А4 – 210*297мм