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 2021г. №78

Б1.0.41 Управление информационной безопасностью

рабочая программа дисциплины

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

Общая трудоемкость в з.е. – 5
Часов по учебному плану – 180

Формы промежуточной аттестации в семестрах:
экзамен 9 курсовая работа 9

Распределение часов дисциплины по семестрам

Семестр	9	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий в форме ПП*	**68/4**	**68/4**
– лекции	34	34
– практические (семинарские)	30/4	30/4
Самостоятельная работа	**76**	**76**
Экзамен	**36**	**36**
Итого	**180**	**180**

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитета), утвержденным Приказом Министерства образования и науки Российской Федерации от 26.11.2020 г. № 1457

Программу составил:
к.э.н. доцент кафедры «ИСиЗИ» Н.И. Глухов

Рабочая программа дисциплины обсуждена и рекомендована к применению в образовательном процессе для обучения обучающихся по специальности 10.05.03 Информационная безопасность автоматизированных систем на заседании кафедры «Информационные системы и защита информации».
Протокол от «04» 06 2021 г. № 11/2

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

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	изучение основных понятий, методологии и применения практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии
1.2 Задачи освоения дисциплины	
1	приобретение обучаемыми 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 обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ)
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
1	Цель воспитания обучающихся – разностороннее развитие личности будущего конкурентоспособного специалиста с высшим образованием, обладающего высокой культурой, интеллигентностью, социальной активностью, качествами гражданина-патриота. Задачи воспитательной работы с обучающимися: – 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;

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Правоведение
2	Основы управленческой деятельности
3	Основы информационной безопасности
4	Безопасность жизнедеятельности
5	Производственная – проектно-технологическая практика
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Аудит информационных технологий и систем обеспечения информационной безопасности
2	Производственная - преддипломная
3	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.1 Знает нормативно-правововые акты, нормативные и методические документы, регламентирующие деятельность по защите информации ОПК-5.2	**Знать:** нормативно-правововые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
		Уметь: применять нормативно-правововые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
		Владеть: навыками применения нормативно-правововых актов, нормативных и методических

	Способен использовать общеправовые знания для организационных мероприятий по защите информации ОПК-5.3 Имеет навыки оформления документов по организации защиты информации	документов, регламентирующих деятельность по защите информации
	ОПК-5.1.1 Знает особенности разработки политики информационной безопасности открытых информационных систем	**Знать:** особенности разработки политики информационной безопасности открытых информационных систем **Уметь:** готовить документы **по** разработке политики информационной безопасности открытых информационных систем **Владеть:** навыками по оформлению документов по разработке политики информационной безопасности открытых информационных систем
	ОПК-5.1.2. Умеет формировать исходные требования для разработки политики информационной безопасности	**Знать:** исходные требования для разработки политики информационной безопасности **Уметь:** готовить документы по разработке политики информационной безопасности **Владеть:** навыками по оформлению документов по разработке политики информационной безопасности
	ОПК-5.1.3. Имеет навыки обоснования целесообразности реализации политики информационной безопасности открытых информационных систем	**Знать:** особенности разработки политики информационной безопасности открытых информационных систем **Уметь:** готовить документы по разработке политики информационной безопасности открытых информационных систем **Владеть:** навыками по оформлению документов по разработке политики информационной безопасности открытых информационных систем

В разделе РПД **«3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ»** изменить наименования профессиональных компетенций.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр**	**Часы**				***Код индикатора достижения компетенции**
			Лек	**Пр**	**Лаб**	**Ср**	
	Раздел 1. Система управления информационной безопасностью						ОПК-5.1 ОПК-5.2 ОПК-5.3
1.1	Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты информации /Лек/	9	4				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.2	Проработка лекционного материала «Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии» /Ср/	9				8	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.3	Политика безопасности /Пр/	9		4			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.4	Проработка материала «Политика безопасности» /Ср/	9				4	ОПК-5.1 ОПК-5.2 ОПК-5.3

1.5	Аудит информационной безопасности /Лек/	9	2				ОПК-5.1 ОПК-52 ОПК-5.3
1.6	Подготовка к семинарским занятиям; «Аудит информационной безопасности» /Ср/	9				4	ОПК-5.2 ОПК-5.3
1.7	Организация обеспечения информационной безопасности автоматизированных систем /Пр/	9		4/2			ОПК-5.2 ОПК-5.3
1.8	Проработка материала «Организация обеспечения информационной безопасности автоматизированных систем» /Ср/	9				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.9	Средства поддержки процессов управления информационной безопасностью /Лек/	9	4				ОПК-5.1 ОПК-5.2 ОПК-5.3
	Раздел 2. Комплексная система защиты информации						
2.1	Сущность и задачи комплексной системы защиты информации /Лек/	9	4				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.2	Проработка лекционного материала «Сущность и задачи комплексной системы защиты информации. Понятие и сущность КСЗИ. Назначение КСЗИ. Задачи КСЗИ» /Ср/	9				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.3	Факторы, влияющие на организацию комплексной системы защиты информации. /Пр	9		4			ОПК-5.1.1
2.4	Проработка материала «Факторы, влияющие на организацию комплексной системы защиты информации. Основные факторы, влияющие на организацию КСЗИ» /Ср/	9				6	ОПК-5.1.1
2.5	Определение компонентов комплексной системы защиты информации /Лек/	9	4				ОПК-5.1.1
2.6	Проработка лекционного материала «Определение компонентов комплексной системы защиты информации» /Ср/	9				4	ОПК-5.1.1
2.7	Определение условий функционирования комплексной системы защиты информации. /Пр/	9		4			ОПК-5.1.1
2.8	Проработка материала «Определение условий функционирования комплексной системы защиты информации» /Ср/	9				6	ОПК-5.1.1 ОПК-5.1.2
2.9	Разработка модели комплексной системы защиты информации /Лек/	9	4				ОПК-5.1.1 ОПК-5.1.2
2.10	Проработка лекционного материала «Разработка модели комплексной системы защиты информации» /Ср/	9				4	ОПК-5.1.1
2.11	Технологическое и организационное построение комплексной системы защиты /Пр/	9		4/2			ОПК-5.1.1 ОПК-5.1.2
2.12	Проработка лекционного материала «Технологическое и организационное построение комплексной системы защиты» /Ср/	9				4	ОПК-5.1.1
	Раздел 3. Управление комплексной системой защиты информации						
3.1	Назначение, структура и содержание управления комплексной системой защиты информации /Лек/	9	4				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.2	Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации /Ср/	9				4	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.3	Принципы и методы планирования комплексной системы защиты информации /Пр/	9		4			ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3

3.4	Проработка лекционного материала «Принципы и методы планирования функционирования комплексной системы защиты информации» /Ср/	9				6	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.5	Сущность и содержание контроля функционирования комплексной системы защиты информации /Лек/	9	4				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.6	Проработка лекционного материала «Сущность и содержание контроля функционирования комплексной системы защиты информации» /Ср/	9				4	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.7	Общая характеристика подходов к оценке эффективности систем защиты информации /Пр/	9		4			ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.8	Проработка лекционного материала «Общая характеристика подходов к оценке эффективности систем защиты информации» /Ср/	9				4	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.9	Методы и модели оценки эффективности комплексной системы защиты информации /Лек/	9	4				ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.10	Методы и модели оценки эффективности комплексной системы защиты информации /Ср/	9				4	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.11	Проработка теоретической части курсовой работы /Ср/	9				6	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.12	Разработка практической части курсовой работы /Ср/	9				6	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
3.13	Защита курсовой работы /Пр/	9		6			ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3
	Раздел 4. Контроль знаний						
4.1	Подготовка к промежуточной аттестации (Экзамен)	9	34	34		76 (36)	ОПК-5.1.1 ОПК-5.1.2 ОПК-5.1.3

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 данной дисциплине оформляется в виде приложения № 1 к рабочей программе дисциплины и размещаются 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
Л1.1	Ю.М. Краковский	Информационная безопасность и защита информации: учебное пособие	М: ИрГУПС, 2016	50

Л1.2	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=276557	М. ; Берлин : Директ-Медиа, 2015	100% онлайн
Л1.3	О.В. Прохорова	Информационная безопасность и защита информации: учебник [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=438331	Самара: СГА-СУ, 2014	100% онлайн
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	С.А. Нестеров	Основы информационной безопасности: Учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=363040	СПб. : Политехнический университет, 2014	100% онлайн
Л2.2	А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов, Э.Р. Газизова	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учебные пособия [Электронный ресурс] http://e.lanbook.com/book/5114	М. : Горячая линия-Телеком, 2012	100% онлайн
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия: учеб. пособие/ Н. И. Глухов; Федер. агентство ж.-д. трансп., Иркут. гос. ун-т путей сообщ... - 148 с	Иркутск: ИрГУПС, 2013	55
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л4.1	Глухов Н.И.	Материалы для самостоятельной работы студентов	Личный кабинет обучающегося	100% онлайн
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	Линия защиты «Сюртель» www.suritel.ru			
Э.2	Федеральная служба по техническому и экспортному контролю, www.fstec.ru			
6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)				
6.3.1 Перечень базового программного обеспечения				
6.3.1.1	ОС Microsoft Windows 7 Professional, лицензия № 49379844, обновление - контракт №03341000100180000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 03341000100190000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 03341000100200000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 03341000100200000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд		
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №03341000100180000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 03341000100190000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 03341000100200000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 03341000100200000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org		
6.3.2 Перечень специализированного программного обеспечения				

6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.
6.3.3 Перечень информационных справочных систем	
6.3.3.1	«Консультант +» http://www.consultant.ru/
6.3.3.2	«Техэксперт» http://www.cntd.ru/
6.4 Перечень правовых и нормативных документов	
6.4.1	Не предусмотрено

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО 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).
3	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
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.
5	Помещение А-521 (для хранения и профилактического обслуживания учебного оборудования).

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	
Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. 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. Уделить внимание следующим понятиям (перечисление понятий) и др.
Практическая работа (семинар)	Обобщение, расширение и углубление пройденного лекционного материала. Решение задач, позволяющих закрепить практические навыки студентов. Выступление с докладами (рефератами) по заданной преподавателем теме, формирование навыков самостоятельной работы, анализа основных и вспомогательных литературных источников, публичное выступление и аргументации собственного мнения, а также дискуссия. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в коллоквиумах. Контроль качества усвоения пройденного материала.
Курсовая работа	Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной задачи; проведение практических исследований по заданной теме.

	Инструкция по выполнению требований к оформлению курсовой работы (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Реферат	Реферат – краткое письменное изложение материала по определенной теме, выполняется; цель – привить обучающимся навыков самостоятельного поиска и анализа информации, формирования умения подбора и изучения литературных источников, используя при этом дополнительную научную, методическую и периодическую литературу. Реферат – это самостоятельная учебно-исследовательская работа обучающегося, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным, изложение материала носит проблемно-поисковый характер. Ознакомиться со структурой и оформление реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Самостоятельная работа студента	Для успешного выполнения самостоятельной работы, студенту необходимо обратиться к лекционному материалу, основным и дополнительным источникам литературы, указанным в рабочей программе. Если этого будет не достаточно для выполнения поставленного задания, необходимо в обязательном порядке посетить консультацию преподавателя.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

Лист регистрации дополнений и изменений рабочей программы дисциплины

№ 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 АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.0.41 Управление информационной безопасностью

Приложение № 1 к рабочей программе

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – 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 (модуля) или прохождения практики*;

– 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 **«Управление информационнойф информационной безопасности»** участвует в формировании компетенций:

ОПК-5.Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ОПК-5.1 Знает нормативно-правововые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

ОПК-5.2 Способен использовать общеправовые знания для организационных

мероприятий по защите информации
ОПК-5.3 Имеет навыки оформления документов по организации защиты информации
ОПК-5.1.1. Знает особенности разработки политики информационной безопасности открытых информационных систем
ОПК-5.1.2. Умеет формировать исходные требования для разработки политики информационной безопасности
ОПК-5.1.3. Имеет навыки обоснования целесообразности реализации политики информационной безопасности открытых информационных систем

Программа контрольно-оценочных мероприятий очная форма за период изучения дисциплины

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения)
9 семестр					
1	2	Текущий контроль	Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии информационных ресурсов и защиты информации /Лек	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
2	4	Текущий контроль	Проработка лекционного материала «Системный подход к проектированию, внедрению и поддержанию системы обеспечения ИБ на предприятии» /Ср/Политика безопасности /Пр/Проработка материала «Политика безопасности» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
3	6	Текущий контроль	Аудит информационной безопасности /Лек/ Подготовка к семинарским занятиям; «Аудит информационной безопасности» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
4	8	Текущий контроль	Организация обеспечения информационной безопасности автоматизированных систем /Пр/ Проработка материала «Организация обеспечения информационной безопасности автоматизированных систем» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
5	9	Текущий контроль	Сущность и задачи комплексной системы защиты информации /Лек/ Проработка лекционного материала «Сущность и задачи комплексной системы защиты информации. Понятие и сущность КСЗИ. Назначение	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)

			КСЗИ. Задачи КСЗИ» /Ср/		
6	10	Текущий контроль	Разработка модели комплексной системы защиты информации /Лек/ Проработка лекционного материала «Разработка модели комплексной системы защиты информации» /Ср/ Технологическое и организационное построение комплексной системы защиты /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
7	12	Текущий контроль	Технологическое и организационное построение комплексной системы защиты /Пр/ Проработка лекционного материала «Технологическое и организационное построение комплексной системы защиты» /Ср/	ОПК-5.1.1. ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
8	13	Текущий контроль	Назначение, структура и содержание управления комплексной системой защиты информации /Лек/ Проработка лекционного материала Назначение, структура и содержание управления комплексной системой защиты информации	ОПК-5.1.1. ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
9	14	Текущий контроль	Принципы и методы планирования комплексной системы защиты информации /Пр/ Проработка лекционного материала «Принципы и методы планирования функционирования комплексной системы защиты информации» /Ср/	ОПК-5.1.1. ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно
10	16	Текущий контроль	Проработка лекционного материала «Сущность и содержание контроля функционирования комплексной системы защиты информации» /Ср/ Общая характеристика подходов к оценке эффективности систем защиты информации /Пр/	ОПК-5.1.1. ОПК-5.1.2 ОПК-5.1.3	тестирование
11	17	Текущий контроль	Проработка лекционного материала «Общая характеристика подходов к оценке эффективности систем защиты информации» /Ср/ Методы и модели оценки	ОПК-5.1.1. ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)

			эффективности комплексной системы защиты информации /Лек/		
12	3	Текущий контроль	Методы и модели оценки эффективности комплексной системы защиты информации /Лек/ Методы и модели оценки эффективности комплексной системы защиты информации /Ср/	ОПК-5.1.1. ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)
11	14	Промежуточная аттестация – экзамен	Проработка теоретической части курсовой работы /Ср/ Разработка практической части курсовой работы /Ср/ Защита курсовой работы /Пр/	ОПК-5.1.1. ОПК-5.1.2 ОПК-5.1.3	Собеседование (устно)

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	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
3	Курсовой проект (работа)	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. 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	Темы типовых групповых и / или индивидуальных проектов и типовое задание на курсовой проект (работу)

		группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	
4	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 (билетов) к экзамену

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета и/или 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 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»	«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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Использованы 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

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, 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».

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, 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, позволяющее оценить умение обучающегося излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Перечень вопросов и заданий для обсуждения
2	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
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 (билетов) к экзамену

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Тест (структура теста по компетенциям)

Проверяемый уровень освоения компетенции компетенций (части компетенций, элементов компетенций)	Минимальное количество тестовых заданий на один раздел программы	Рекомендуемые формы тестовых заданий	Количество баллов за одно тестовое задание
Минимальный уровень освоения компетенции	19	Тестовые задания с выбором одного правильного ответа из нескольких	1
		Тестовые задания с выбором нескольких правильных ответов из множества ответов	
		Тестовые задания на установление соответствия	
		Тестовые задания на установление правильной последовательности	
Базовый уровень освоения компетенции	8	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)	4
Высокий уровень освоения компетенции	6	Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы	7

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся при тестировании набрал 86-93 баллов	Высокий
«хорошо»		Обучающийся при тестировании набрал 69-85 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 53-68 баллов	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-52 баллов	Компетенция не сформирована

3. 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

3.1. Тест

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. Выберите правильное определение термина «предоставление информации»:
а) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
б) действия, направленные на распространение сведений в средствах массовой информации;
в) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
г) действия, направленные на получение информации как определённым, так и неопределённым кругом лиц или передачу информации как определенному, так и неопределённому кругу лиц.

4. Выберите правильное определение термина «защищаемые помещения»:
а) помещения, специально предназначенные для хранения носителей конфиденциальной информации;
б) помещения, специально предназначенные для размещения технических средств информационной системы;
в) помещения, специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы;
г) 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. Средствами защиты информации, подлежащими сертификации, являются (выберите все верные варианты ответов):

а) строительные материалы, используемые для отделки помещений, в которых размещаются отдельные элементы АС;
б) детали интерьера, используемые для размещения АИС;
в) средства контроля эффективности применения средств защиты информации;
г) средства контроля эффективности прочности ограждений;
д) средства защиты информации (технические, программные, программно-аппаратные) от НСД, блокировки доступа и нарушения целостности.

8. 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.

9. “Технический канал утечки информации” - это:
а) совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
б) совокупность средств доступа к информации, нарушающих правила разграничения доступа с использованием штатных средств;
в) совокупность физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
г) совокупность объекта технической разведки и средств, которыми добывается защищаемая информация.

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:
а) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
б) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;
в) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;
г) доступ к информации, реализуемый путём уничтожения технических средств информационной системы.

12. «Персональный идентификатор» — это
а) устройство для хранения зашифрованной информации пользователя;
б) устройство для хранения информации, необходимой при идентификации и аутентификации пользователя;
в) устройство для хранения журнала аудита.

13. Механизм контроля целостности СЗИ Secret Net предназначен для
а) формирония цифровых отпечатков данных;
б) контроля информационных потоков;
в) слежения за неизменностью содержимого ресурсов компьютера.

14. 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.
15. В СЗИ Secret Net пользователю с уровнем допуска "конфиденциально" разрешается выполнять чтение файлов с категориями
    а) «конфиденциально»;
    б) «секретно»;
    в) «строго конфиденциально»,
    г) «неконфиденциально».
16. Длина ключа шифрования алгоритма ГОСТ 28147-89 равна
    а) 56 бит;
    б) 256 бит;
    в) 1024 бит;
    г) 128 бит.
17. К какому типу криптосистем относится алгоритм AES?
    а) несимметричные;
    б) асиммеричные;
    в) симметричные;
    г) полусимметричные.
18. Пассивными способами защиты информации являются:
    а) создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств;
    б) ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны;
    в) создание маскирующих электромагнитных помех в цепях заземления;
    г) выставление постов охраны у помещений, в которых размещаются технические средства обработки информации.
19. Межсетевой экран служит для:
    а) разграничения доступа в помещения АИС;
    б) фильтрации трафика при передачи данных;
    в) защиты от утечек информации путем экранирования стен;
    г) контроля целостности программного обеспечения.
20. Максимально возможное количество категорий конфиденциальности в СЗИ Secret Net 7.x равно _____ (16).
21. В СЗИ Secret Net категорию конфиденциальности можно назначить для следующих ресурсов: каталоги и файлы на дисках с файловой системой _____ (NTFS).
22. Практическая стойкость алгоритма RSA основана на сложности решения задачи _____ (факторизации).
23. Практическая стойкость алгоритма Диффи-Хеллмана основана на сложности решения задачи нахождения дискретного_____ (логарифма).
24. Эффективным средством защиты от утечки информации из АИС показали себя _____ (DLP) – системы.
25. Хэш-функции предназначены, главным образом, для контроля _____(целостности) данных.
26. Технология электронной подписи разработана с целью подтверждения _____ (авторства) и _____ (подлинности) сообщений.
27. Длина хэш-кода алгоритма MD5 составляет _____ (128) бит.
28. Как в СЗИ Secret Net происходит включение режима хранения пароля в идентифика торе?

(Основной тезис: происходит добавление в базу данных Secret Net сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора).

29. Каким образом в СЗИ Secret Net происходит присвоение пользователю персонального идентификатора?

(Основной тезис: происходит добавление в базу данных Secret Net сведений о том, что пользователю принадлежит персональный идентификатор данного типа с уникальным серийным номером).

30. Каким образом в СЗИ Secret Net реализуется затирание файлов?

(Основной тезис: при действии механизма затирания в область диска, где физически было расположено содержимое удаленного файла, записывается последовательность случайных чисел).

31. Что происходит при выборе способа очистки журнала СЗИ Secret Net при его переполнении «Затирать события по мере необходимости»?

(Основной тезис: при переполнении журнала система защиты автоматически удаляет из журнала необходимое количество самых старых записей).

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

(Основной тезис: настройка дискреционного разграничения доступа к файлам и папкам производится штатными средствами операционной системы).

33. Кратко описать назначение и функции Удостоверяющего Центра в системе PCI.

3.2. Перечень теоретических вопросов к семинарам

1. Резервирование и восстановление информации; повышение надежности АИС;
2. Блокировка ошибочных операций пользователей; минимизация ущерба от аварий и стихийных бедствий;
3. Инженерно-физическая защита объектов информатизации; система контроля и управления доступом;
4. Организация работ с конфиденциальными информационными ресурсами;
5. защита от злоумышленных действий обслуживающего персонала и пользователей;
6. Понятие и возможности DLP-систем;
7. Методы и средства защиты информации в АИС от утечек по техническим каналам;
8. Противодействие наблюдению в оптическом диапазоне; противодействие утечкам по группе акустических каналов;
9. Методы и средства защиты от побочных электромагнитных излучений и наводок;
10. Компьютерные вирусы; троянские программы; сетевые черви; сертифицированные средства антивирусной защиты;
11. Средства сетевой безопасности: межсетевые экраны, сканеры безопасности;
12. Средства сетевой безопасности: средства построения виртуальных частных сетей (VPN), системы обнаружения вторжений.

3.3. 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;
6. Архитектура системы защиты информации (СЗИ) от НСД SecretNet;
7. СЗИ от НСД SecretNet: дискреционное разграничение доступа, полномочное разграничение доступа;
8. СЗИ от НСД Dallas Lock: основные функциональные возможности;
9. Электронный замок Соболь-PCI: настройка и эксплуатация; управление пользователями; диагностика устройства; настройка контроля целостности; регистрация событий;
10. Классификация методов криптографического преобразования информации; методы стеганографии и кодирования;
11. Требования к симметричным и асимметричным криптосистемам;
12. Алгоритм DES; свойства стандарта AES;
13. Стандарт ГОСТ 28145-89;
14. Функции хэширования, алгоритм MD5;
15. Электронная подпись; инфраструктура открытых ключей;

3.4. Перечень типовых простых практических заданий к экзамену

Формируется на основании требований теоретических вопросов.

3.5. 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 системы 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.

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

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
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Собеседование	Обучаемый грамотно с наличием умений и навыков отвечает на поставленные практические вопросы на заданную тему. Тема (задание) предлагается в конкретном виде. Методы и инструменты для ее разработки предлагаются преподавателем. Оценка ставится по результатам собеседования.

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

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

ИРГУПС 2021-2022 учебный год	**Экзаменационный билет № 1** **по дисциплине «_____»** **__ ____ семестр**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____

1. …… 2. …… 3. …….. 4. …….. 5 ……..……. Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм

В разделе «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» приведены типовые контрольные задания, для оценки результатов освоения образовательной программы. Задания, по которым проводятся контрольно-оценочные мероприятия, оформляются в соответствии с формами оформления оценочных средств, приведенными ниже, и не выставляются в электронную информационно-образовательную среду ИрГУПС, а хранятся на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

Составитель _____к.э.н, доцент Н.И. Глухов