

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.38 Организационное и правовое обеспечение 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 обучения – очная

Нормативный срок обучения – 5 лет 6 мес

Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5

Формы промежуточной аттестации в семестрах:

Часов по учебному плану – 180

экзамен 7

#### **Распределение часов дисциплины по семестрам**

Семестр	7	<b>Итого</b>
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	Часов по учебному плану
<b>Аудиторная контактная работа по видам учебных занятий в т.ч. в форме ПП</b>	<b>85</b>	<b>85</b>
– лекции	34	34
– практические (семинарские)	51	51
– лабораторные	-	-
<b>Самостоятельная работа</b>	<b>59</b>	<b>59</b>
<b>Экзамен</b>	<b>36</b>	<b>36</b>
<b>Итого</b>	<b>180</b>	<b>180</b>

\* В форме ПП – в форме практической подготовки.

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

<b>1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ</b>	
<b>1.1 Цели освоения дисциплины</b>	
1	изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем организационно - правового обеспечения информационной безопасности и защиты информации
<b>1.2 Задачи освоения дисциплины</b>	
1	раскрытие места информационной безопасности и защиты информации в системе информационных отношений;
2	раскрытие направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение информационной безопасности и защита информации
3	раскрытие взаимосвязи между информационной безопасностью и удовлетворением информационных потребностей субъектов информационных отношений;
4	раскрытие значения обеспечения информационной безопасности для предотвращения негативного информационного воздействия на субъекты информационных отношений;
5	определение места защиты информации в обеспечении сохранности документальной базы, раскрывающей различные стороны социально-экономического и культурного развития страны.
<b>1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины</b>	
1	<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"> <li>– развитие мировоззрения и актуализация системы базовых ценностей личности;</li> <li>– приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям;</li> <li>– 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;</li> <li>– воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях;</li> <li>– обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности;</li> <li>– выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;</li> </ul>

<b>2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП</b>	
<b>2.1 Требования к предварительной подготовке обучающегося</b>	
1	Основы информационной безопасности
2	Введение в специальность
3	Правоведение
4	Основы управленческой деятельности
5	Производственная – проектно-технологическая практика
<b>2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее</b>	
1	Управление информационной безопасностью
2	Комплексная защита в информационных системах персональных данных
3	Производственная - технологическая

### **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
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК -3.3 Знает принципы и методы командообразования	<b>Знать:</b> методы организации и способы руководства работой команды, вырабатывая командную стратегию для достижения поставленной цели <b>Уметь:</b> организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

		<b>Владеть:</b> навыками организации и способы руководства работой команды, вырабатывая командную стратегию для достижения поставленной цели
ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.1 Знает нормативно-правовые 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	<b>Знать:</b> нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации <b>Уметь:</b> применять нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации <b>Владеть:</b> навыками по применению нормативно-правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

#### 4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	Ср	
	<b>Раздел 1. Правовое обеспечение информационной безопасности</b>						ОПК-5.1 ОПК-5.2 ОПК-5.3
1.1	Правовое обеспечение информационной безопасности и пути его совершенствования /Лек/	7	4				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.2	Проработка лекционного материала темы «Правовое обеспечение информационной безопасности и пути его совершенствования» /Ср/	7			2		ОПК-5.1 ОПК-5.2 ОПК-5.3
1.2	Подготовка к семинарскому занятию на тему «Задачи и функции правовой защиты информации» /Ср/	7			2		ОПК-5.1 ОПК-5.2 ОПК-5.3
1.3	Задачи и функции правовой защиты информации /Пр/	7		4			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.4	Институт правовой защиты государственной тайны /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.5	Проработка лекционного материала темы «Институт правовой защиты государственной тайны» /Ср/	7			2		ОПК-5.1 ОПК-5.2 ОПК-5.3
1.6	Подготовка к семинарскому занятию на тему «Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ)» /Ср/	7			2		ОПК-5.1 ОПК-5.2 ОПК-5.3
1.7	Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ) /Пр/	7		4			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.8	Институт правовой защиты коммерческой тайны /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3

1.9	Проработка лекционного материала темы «Институт правовой защиты коммерческой тайны» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.10	Подготовка к семинарскому занятию на тему «Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.11	Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны /Пр/	7		4			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.12	Институт правовой защиты профессиональной тайны /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.13	Проработка лекционного материала темы «Институт правовой защиты профессиональной тайны» /Ср/	7				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.14	Подготовка к семинарскому занятию на тему «Банковская информация и обеспечение банковской тайны» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.15	Банковская информация и обеспечение банковской тайны /Пр/	7		4			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.16	Институт правовой защиты информации персонального характера (персональные данные) /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.17	Проработка лекционного материала темы «Институт правовой защиты информации персонального характера (персональные данные)» /Ср/	7				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.18	Подготовка к семинарскому занятию на тему «Международные и российские документы, касающиеся использования персональных данных и их правовой защиты» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.19	Международные и российские документы, касающиеся использования персональных данных и их правовой защиты /Пр/	7		4			ОПК-5.1 ОПК-5.2 ОПК-5.3
1.20	Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием объектов интеллектуальной собственности /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
1.21	Проработка лекционного материала темы «Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием объектов интеллектуальной собственности» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.22	Подготовка к семинарскому занятию на тему «Авторский договор» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
1.23	Авторский договор /Пр/	7		4			ОПК-5.1 ОПК-5.2 ОПК-5.3
	<b>Раздел 2. Организационное обеспечение информационной безопасности</b>						
2.1	Сущность организационного обеспечения информационной безопасности и его место в комплексном обеспечении информационной безопасности и системы защиты информации /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.2	Проработка лекционного материала темы «Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием объектов интеллектуальной собственности» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.3	Подготовка к семинарскому занятию на тему	7				2	ОПК-5.1

	«Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации» /Ср/						ОПК-5.2 ОПК-5.3 УК -3.3
2.4	Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации /Пр/	7		6			ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.5	Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.6	Проработка лекционного материала темы «Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.7	Подготовка к семинарскому занятию на тему «Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну» /Ср/	7				4	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.8	Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну /Пр/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.9	Оформление допуска сотрудников к конфиденциальной информации /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.10	Проработка лекционного материала темы «Оформление допуска сотрудников к конфиденциальной информации» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.11	Подготовка к семинарскому занятию на тему «Оформление допуска сотрудников к конфиденциальной информации» /Ср/	7				2	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.12	Оформление допуска сотрудников к конфиденциальной информации /Пр/	7		2			ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.13	Организация разрешительной системы доступа к конфиденциальной информации /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.14	Подготовка к семинарскому занятию, экзамену на тему «Организация разрешительной системы доступа к конфиденциальной информации» /Ср/	7				3	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.15	Организация разрешительной системы доступа к конфиденциальной информации /Пр/	7		4			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.16	Организация физической охраны предприятия /Лек/	7	2				ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.17	Подготовка к семинарскому занятию, экзамену на тему «Организация физической охраны предприятия» /Ср/	7				4	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3
2.18	Организация физической охраны предприятия /Пр/	7		4			ОПК-5.2 ОПК-5.3 УК -3.3
2.19	Организация пропускного и внутри объектового режимов /Лек/	7	2				ОПК-5.2 ОПК-5.3

							УК -3.3
2.20	Подготовка к семинарскому занятию, экзамену на тему «Организация пропускного и внутриобъектового режимов» /Ср/	7				4	ОПК-5.2 ОПК-5.3 УК -3.3
2.21	Организация пропускного и внутриобъектового режимов /Пр/	7		4			ОПК-5.2 ОПК-5.3
2.22	Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями /Лек/	7	2				ОПК-5.2 ОПК-5.3
2.23	Подготовка к семинарскому занятию на тему «Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями» /Ср/	7				2	ОПК-5.2 ОПК-5.3
2.24	Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями /Пр/	7		3			ОПК-5.2 ОПК-5.3
2.25	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам /Лек/	7	2				ОПК-5.2 ОПК-5.3
2.26	Подготовка к семинарскому занятию на тему «Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам» /Ср/	7				4	ОПК-5.2 ОПК-5.3
2.27	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам /Пр/	7		4			ОПК-5.2 ОПК-5.3
	<b>Раздел 3. Контроль знаний</b>						
3.1	Подготовка к промежуточной аттестации (Экзамен)	7	34	51		59 (36)	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК -3.3

### 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
ЛП.1	Ю. М. Краковский	Информационная безопасность и защита информации: учебное пособие	Иркутск: ИрГУПС, 2016	50
ЛП.2	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
ЛП.3	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 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/
--	---------------------	----------	---------------------------	---------------------------

				100% онлайн
Л2.1	Ю.Н. Загинайлов	Теория информационной безопасности и методология защиты информации: учебное пособие <a href="http://biblioclub.ru/index.php?page=book&amp;id=276557">//biblioclub.ru/index.php?page=book&amp;id=276557</a>	М. ; Берлин : Директ-Медиа, 2015	100% онлайн
Л2.2	О.В. Прохорова	Информационная безопасность и защита информации: Учебник [Электронный ресурс] <a href="http://biblioclub.ru/index.php?page=book&amp;id=438331">//biblioclub.ru/index.php?page=book&amp;id=438331</a>	Самара: СГА-СУ, 2014	100% онлайн
Л2.3	Коваленко, Ю.И	Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебные пособия [Электронный ресурс] <a href="http://e.lanbook.com/book/5163">http://e.lanbook.com/book/5163</a>	М. : Горячая линия-Телеком, 2012	100% Онлайн
<b>6.1.3 Методические разработки</b>				
	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
<b>6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине</b>				
	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
<b>6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»</b>				
Э.1	Линия защиты «Сюртель» <a href="http://www.suritel.ru">www.suritel.ru</a>			
Э.2	Федеральная служба по техническому и экспортному контролю, <a href="http://www.fstec.ru">www.fstec.ru</a>			
<b>6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)</b>				
<b>6.3.1 Перечень базового программного обеспечения</b>				
6.3.1.1	ОС Microsoft Windows 7 Professional, лицензия № 49379844, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд			
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, <a href="https://ru.libreoffice.org">https://ru.libreoffice.org</a>			
<b>6.3.2 Перечень специализированного программного обеспечения</b>				
6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.			
<b>6.3.3 Перечень информационных справочных систем</b>				
6.3.3.1	«Консультант +» <a href="http://www.consultant.ru/">http://www.consultant.ru/</a>			
6.3.3.2	«Техэксперт» <a href="http://www.cntd.ru/">http://www.cntd.ru/</a>			
<b>6.4 Перечень правовых и нормативных документов</b>				
6.4.1	Не предусмотрено			

## 7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ,



<b>НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ</b>	
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).

<b>8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ</b>	
Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; пометать 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 удастся разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить задание на самостоятельную работу и выучить лекционный материал к следующей теме. Систематическое выполнение заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины.
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 оформлением реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).

<p>Самостоятельная работа</p>	<p>Для эффективного освоения дисциплины изучение материала курса предполагает самостоятельную внеаудиторную работу, которая включает в себя выполнение индивидуальных заданий, подготовку к практическим занятиям, конспектирование. Для успешного выполнения домашних заданий следует обратиться к задачам, решенным на предыдущих практических занятиях, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделах основная и дополнительная литература. Если, несмотря на изученный материал, задание выполнить не удастся, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине.</p>
<p>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.</p>	



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.О.38 Организационное и правовое обеспечение информационной безопасности**

#### **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 «Организационное и правовое обеспечение информационной безопасности» участвует в формировании компетенций:

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

УК -3.3 Знает принципы и методы командообразования

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

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

ОПК-5.2Способен использовать общеправовые знания для организационных мероприятий по защите информации

ОПК-5.3Имеет навыки оформления документов по организации защиты информации

**Программа контрольно-оценочных мероприятий  
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)
<b>7 семестр</b>					
1	2	Текущий контроль	Правовое обеспечение информационной безопасности и пути его совершенствования /Лек/Подготовка к практической работе на тему «Задачи и функции правовой защиты информации» /Ср/Задачи и функции правовой защиты информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
2	4	Текущий контроль	Институт правовой защиты государственной тайны /Лек/Подготовка к практической работе на тему «Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ)» /Ср/Особенность уголовно-правовой защиты информации, составляющей государственную тайну (ГТ) /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
3	6	Текущий контроль	Институт правовой защиты коммерческой тайны /Лек/Подготовка к практической работе на тему «Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны» Ср/Особенности защиты прав на секреты производства (ноу-хау) в режиме коммерческой тайны /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
4	8	Текущий контроль	Институт правовой защиты профессиональной тайны /Лек/Подготовка к практической работе на тему «Банковская информация и обеспечение банковской тайны» /Ср/Банковская информация и обеспечение банковской тайны /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
5	9	Текущий контроль	Институт правовой защиты информации персонального характера (персональные данные) /Лек/Подготовка к практической работе на тему «Международные и российские документы, касающиеся использования персональных данных и их правовой защиты» /Ср/Международные и российские документы, касающиеся использования	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)

			персональных данных и их правовой защиты /Пр/		
6	10	Текущий контроль	Основные законодательные акты, регулирующие отношения, связанные с правовой защитой и использованием объектов интеллектуальной собственности /Лек/Подготовка к практической работе на тему «Авторский договор» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
7	12	Текущий контроль	Сущность организационного обеспечения информационной безопасности и его место в комплексном обеспечении информационной безопасности и системы защиты информации /Лек/Подготовка к практической работе по определению состава, засекречиванию и рассекречиванию конфиденциальной информации» /Ср/Организация работы по определению состава, засекречиванию и рассекречиванию конфиденциальной информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	Собеседование (устно)
8	13	Текущий контроль	Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну /Лек/Подготовка к практической работе на тему «Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну» /Ср/Лицензирование деятельности предприятия по проведению работ, связанных с использованием сведений, составляющих гостайну /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
9	14	Текущий контроль	Оформление допуска сотрудников к конфиденциальной информации /Лек/Подготовка к практической работе на тему «Оформление допуска сотрудников к конфиденциальной информации» /Ср/Оформление допуска сотрудников к конфиденциальной информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	Собеседование (устно)
10	16	Текущий контроль	Подготовка к практической работе на тему «Оформление допуска сотрудников к конфиденциальной информации» /Ср/Оформление	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	тестирование

			допуска сотрудников к конфиденциальной информации /Пр/		
11	17	Текущий контроль	Организация физической охраны предприятия /Лек/Подготовка к практической работе на тему «Организация физической охраны предприятия» /Ср/Организация физической охраны предприятия /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	Собеседование (устно)
12	3	Текущий контроль	Организация пропускного и внутриобъектового режимов /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	Собеседование (устно)
13	5	Текущий контроль	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам /Лек/ Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	Собеседование (устно)
14	6	Текущий контроль	Подготовка к практической работе на тему «Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	Собеседование (устно)
15	11	Текущий контроль	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	тестирование
16	16	Текущий контроль	Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями /Лек/Подготовка к практической работе на тему «Требования к помещениям, в которых ведутся работы с конфиденциальными документами, работами, изделиями» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
17	18	Промежуточная аттестация – экзамен		ОПК-5.1 ОПК-5.2 ОПК-5.3 УК- 3.3	Собеседование (устно)

## **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	6	Тестовые задания со свободно	7

освоения компетенции		конструируемым ответом (интервью, эссе) Структурированный тест Кейсы	
----------------------	--	----------------------------------------------------------------------------	--

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**

- Выберите правильное определение термина «информация»:
  - совокупность содержащихся в базах данных сведений;
  - совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях;
  - сведения (сообщения, данные) воспроизводимые различными системами;
  - сведения (сообщения, данные) независимо от формы их представления.
- Выберите правильное определение термина «обладатель информации»:
  - лицо, самостоятельно создавшее информацию;
  - лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;
  - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
  - лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
- Выберите правильное определение термина «предоставление информации»:
  - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
  - действия, направленные на распространение сведений в средствах массовой информации;
  - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
  - действия, направленные на получение информации как определённым, так и неопределённым кругом лиц или передачу информации как определенному, так и неопределённым кругом лиц.
- 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) формирования 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) асимметричные;
  - 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 идентификаторе?  
(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 РСІ.

### **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.

## **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	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения

### **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

 <p>ИРГУПС 2021-2022 учебный год</p>	<p>Экзаменационный билет № 1 по дисциплине « _____ » _____ семестр</p>	<p>Утверждаю: Заведующий кафедрой « _____ » ИРГУПС _____</p>
<p>1. .... 2. .... 3. .... 4. .... 5. .... Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм</p>		

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