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

Б1.0.33 Основы 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. – 4
Часов по учебному плану – 144

Формы промежуточной аттестации в семестрах:
экзамен 3, курсовая работа 3

Распределение часов дисциплины по семестрам

Семестр	3	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**51**	**51**
– лекции	17	17
– практические (семинарские)	34	34
Самостоятельная работа	**57**	**57**
Экзамен	**36**	**36**
Итого	**144**	**144**

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	раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристика составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.
1.2 Задачи освоения дисциплины	
1	изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации
2	изучение видов защищаемой информации, угроз информационной безопасности, методов и средств обеспечения информационной безопасности, механизмов защиты информации, моделей безопасности, критериев оценки защищенности и обеспечения безопасности информационных систем;

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.В.ДВ.05.01 Введение в специальность
2	Б1.0.08 Алгебра и геометрия
3	Б1.0.02 История
	Б1.0.18 Правоведение
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.0.41 Управление информационной безопасностью
2	Б1.0.38 Организационное и правовое обеспечение информационной безопасности
3	Б1.0.50 Комплексная защита в информационных системах персональных данных
4	Б1.0.46 Аудит информационной безопасности
5	Б2.В.03(П) Производственная – проектно-технологическая практика

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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства ОПК-1.2 Оценивает значение информационных технологий в развитии современного общества ОПК-1.3 Оценивает роль, сущность и значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства	**Знать:** сущность и значение информации, информационных технологий и информационной безопасности в современном обществе **Уметь:** реализовывать сущность и значение информации, информационных технологий и информационной безопасности в современном обществе **Владеть:** навыками работ по реализации сущности и значению информации, информационных технологий и информационной безопасности в современном обществе, понимать их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-5 Способен применять нормативные правовые акты, нормативные и	ОПК-5.1 Знает нормативно-правововые акты, нормативные и методические документы, регламентирующие	**Знать:** нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации; **Уметь:** применять нормативные правовые акты,

методические документы, регламентирующие деятельность по защите информации;	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	нормативные и методические документы, регламентирующие деятельность по защите информации; **Владеть:** навыками работ по применению нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации;

ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-5.1; ОПК-5.2; ОПК-5.3							
4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр**	**Часы**				***Код индикатора достижения компетенции**
			Лек	**Пр**	**Лаб**	**Срс**	
	Раздел 1. Теория информационной безопасности						ОПК-1.1 ОПК-1.2 ОПК-1.3
1.1	Введение /Лек/	3	1				ОПК-1.1
1.2	Сущность и понятие информационной безопасности /Лек/	3	1				ОПК-1.1 ОПК-1.2 ОПК-1.3
1.3	Проработка лекционного материала по теме «Сущность и понятие информационной безопасности» /Ср/	3				4	ОПК-1.1 ОПК-1.2 ОПК-1.3
1.4	Значение информационной безопасности и ее место в системе национальной безопасности /Пр/	3		1			ОПК-1.1 ОПК-1.2
1.5	Современная Доктрина информационной безопасности Российской Федерации /Лек/	3	2				ОПК-1.1 ОПК-1.2 ОПК-1.3
1.6	Проработка лекционного материала, подготовка к семинарскому занятию по теме «Современная Доктрина информационной безопасности Российской Федерации» /Ср/	3				4	ОПК-1.1 ОПК-1.2 ОПК-1.3
1.7	Современная Доктрина информационной безопасности Российской Федерации /Пр/	3		1			ОПК-1.1 ОПК-1.2 ОПК-1.3
	Раздел 2. Методология защиты информации						
2.1	Сущность и понятие защиты информации /Лек/	3	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.2	Проработка лекционного материала по теме «Сущность и понятие защиты информации» /Ср/	3				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.3	Цели и значение защиты информации /Пр/	3		1			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.4	Теоретические и концептуальные основы защиты информации /Лек/	3	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.5	Проработка лекционного материала и подготовка к семинарскому занятию по теме «Теоретические и концептуальные основы защиты информации» /Ср/	3			2		ОПК-5.1 ОПК-5.2 ОПК-5.3
2.6	Теоретические и концептуальные основы защиты информации /Пр/	3		1			ОПК-5.1 ОПК-5.2 ОПК-5.3

2.7	Организационные основы и методологические принципы защиты информации /Лек/	3	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.8	Проработка лекционного материала «Организационные основы и методологические принципы защиты информации» /Ср/	3				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.9	Современные факторы, влияющие на защиту информации /Пр/	3		1			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.10	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности /Лек/	3	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.11	Проработка лекционного материала по теме «Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности» /Ср/	3				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.12	Критерии, условия и принципы отнесения информации к защищаемой /Пр/	3		1			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.13	Каналы и методы несанкционированного доступа к конфиденциальной информации /Лек/	3	3				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.14	Подготовка к семинарскому занятию по теме «Состав и классификация носителей защищаемой информации» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.15	Состав и классификация носителей защищаемой информации /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.16	Классификация видов, методов и средств защиты информации /Лек/	3	2				ОПК-5.1 ОПК-5.2 ОПК-5.3
2.17	Проработка лекционного материала по теме «Классификация видов, методов и средств защиты информации» /Ср/	3				4	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.18	Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.19	подготовка к семинарскому занятию по теме «Классификация защищаемой информации по собственникам и владельцам» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.20	Классификация защищаемой информации по собственникам и владельцам /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.21	подготовка к семинарскому занятию по теме «Понятие и структура угроз защищаемой информации» /Ср/	3				3	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.22	Понятие и структура угроз защищаемой информации /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.23	подготовка к семинарскому занятию по теме «Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.24	Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.25	подготовка к семинарскому занятию по теме «Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.26	Причины, обстоятельства и условия дестабилизирующего воздействия на	3		2			ОПК-5.1 ОПК-5.2

	защищаемую информацию /Пр/						ОПК-5.3
2.27	подготовка к семинарскому занятию по теме «Каналы и методы несанкционированного доступа к конфиденциальной информации» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.28	Каналы и методы несанкционированного доступа к конфиденциальной информации /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.29	подготовка к семинарскому занятию по теме «Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.30	Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.31	подготовка к семинарскому занятию по теме «Объекты защиты информации» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.32	Объекты защиты информации /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.33	подготовка к семинарскому занятию по теме «Кадровое и ресурсное обеспечение защиты информации» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.34	Кадровое и ресурсное обеспечение защиты информации /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.35	подготовка к семинарскому занятию по теме «Технологическое обеспечение защиты информации» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.36	Технологическое обеспечение защиты информации /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.37	подготовка к семинарскому занятию по теме «Назначение и структура систем защиты информации» /Ср/	3				2	ОПК-5.1 ОПК-5.2 ОПК-5.3
2.38	Назначение и структура систем защиты информации /Пр/	3		2			ОПК-5.1 ОПК-5.2 ОПК-5.3
2.39	Проработка теоретической части курсовой работы /Ср/	3				2	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3
2.40	Разработка практической части курсовой работы /Ср/	3				3	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3
2.41	Защита курсовой работы /Пр/	3		4			ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3
	Раздел 3. Контроль знаний						
3.1	Подготовка к промежуточной аттестации (Экзамен)	3	17	34		57 (36)	ОПК-1.1 ОПК-1.2 ОПК-1.3

							ОПК-5.1 ОПК-5.2 ОПК-5.3

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	С.А. Нестеров	Основы информационной безопасности: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=363040	СПб:Издательство Политехнического университета, 2014	100% Онлайн
Л1.2	М.А. Лапина, А.Г. Ревин, В.И. Лапин	Информационное право: учебное пособие [Электронный ресурс] biblioclub.ru/index.php?page=book&id=118624	М. : Юнити-Дана, 2015	100% онлайн
Л1.3	О.В. Порядина	Управление информационными ресурсами: учебно-методическое пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=439328	Йошкар-Ола: ПГТУ, 2015	100% онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Ю.Ю. Громов, Ю.Ф. Мартемьянов, Ю.К. Букурако и др	Организация безопасной работы информационных систем: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php?page=book&id=277794	Издательство ФГБОУ ВПО «ТГТУ, 2014	100% онлайн
Л2.2	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
Л2.3	Аверченков, В.И.	Служба защиты информации: организация и управление: учебное пособие для вузов [Электронный ресурс] biblioclub.ru/index.php?page=book&id=93356	М. : Флинта, 2011	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-	- Иркутск: ИрГУПС, 2013	55

		т путей сообщ... - 148 с		
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	Середкин С.П.	Материалы для самостоятельной работы студентов	Личный кабинет обучающегося	100% онлайн
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	Федеральная служба по техническому и экспортному контролю, www.fstec.ru			
Э.2	СЗИ от НСД Secret Net, СКриптЗИ М-506А-ХР, www.securitycode.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 №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, 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.
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 оформление реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
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).
Самостоятельная работа	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 удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия или лектора по дисциплине.
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

Б1.0.33 Основы 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 **«Основы информационной безопасности»** участвует в формировании компетенций:

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

ОПК-1.1Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

ОПК-1.2Оценивает значение информационных технологий в развитии современного общества

ОПК-1.3Оценивает роль, сущность и значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;
ОПК-5.1Знает нормативно-правововые 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 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)
2 семестр					
1	2	Текущий контроль	Введение /Лек/ Сущность и понятие информационной безопасности /Лек/ Проработка лекционного материала по теме «Сущность и понятие информационной безопасности» /Ср/	ОПК-1.1	Собеседование (устно)
2	4	Текущий контроль	Значение информационной безопасности и ее место в системе национальной безопасности /Пр/	ОПК-1.1	Собеседование (устно)
3	6	Текущий контроль	«Современная Доктрина ИБ Российской Федерации» /Ср/ Современная Доктрина информационной безопасности Российской Федерации /Пр/	ОПК-1.1 ОПК-1.2	Собеседование (устно)
4	8	Текущий контроль	Сущность и понятие защиты информации /Лек/ Подготовка к практическому занятию по теме «Цели и значение защиты информации» /Ср/ Цели и значение защиты информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
5	9	Текущий контроль	Теоретические и концептуальные основы защиты информации /Лек/ Подготовка к практическому занятию по теме «Теоретические и концептуальные основы защиты информации» /Ср/ Теоретические и концептуальные основы защиты информации /Пр	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
6	10	Текущий контроль	Организационные основы и методологические принципы защиты информации /Лек	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование

7	12	Текущий контроль	Подготовка к практическому занятию по теме «Критерии, условия и принципы отнесения информации к защищаемой» /Ср/ Критерии, условия и принципы отнесения информации к защищаемой /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
8	13	Текущий контроль	Каналы и методы несанкционированного доступа к конфиденциальной информации /Лек/ Подготовка к практическому занятию по теме «Состав и классификация носителей защищаемой информации» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
9	14	Текущий контроль	Подготовка к практическому занятию по теме «Понятие и структура угроз защищаемой информации» /Ср/ Понятие и структура угроз защищаемой информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно
10	16	Текущий контроль	Подготовка к практическому занятию по теме «Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию» /Ср/ Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
11	17	Текущий контроль	Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию /Пр/ Подготовка к практическому занятию по теме «Каналы и методы несанкционированного доступа к конфиденциальной информации» /Ср/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
12	3	Текущий контроль	Подготовка к практическому занятию по теме «Каналы и методы несанкционированного доступа к конфиденциальной информации» /Ср/ Каналы и методы несанкционированного доступа к конфиденциальной информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
13	5	Текущий контроль	Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации /Пр	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
14	6	Текущий контроль	Подготовка к практическому занятию по теме «Объекты защиты информации» /Ср/ Объекты защиты информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
15	11	Текущий контроль	Подготовка к практическому занятию по теме «Кадровое и ресурсное обеспечение защиты	ОПК-5.1 ОПК-5.2	тестирование

			информации» /Ср/ Кадровое и ресурсное обеспечение защиты информации /Пр/	ОПК-5.3	
16		Текущий контроль	Подготовка к практическому занятию по теме «Технологическое обеспечение защиты информации» /Ср/ Технологическое обеспечение защиты информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	Собеседование (устно)
16	12	Текущий контроль	Подготовка к практическому занятию по теме «Технологическое обеспечение защиты информации» /Ср/ Технологическое обеспечение защиты информации /Пр/	ОПК-5.1 ОПК-5.2 ОПК-5.3	тестирование
11	14	Промежуточная аттестация – экзамен	Проработка теоретической части курсовой работы /Ср/ Разработка практической части курсовой работы /Ср/ Защита курсовой работы /Пр/	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-5.1 ОПК-5.2 ОПК-5.3	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.	Темы типовых групповых и /

		Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	или индивидуальных проектов и типовое задание на курсовой проект (работу)
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

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. Виды и состав угроз информационной безопасности.
2. Задачи, принципы и методы обеспечения информационной безопасности.
3. Критерии, условия, принципы и формы отнесения информации к защищаемой.
4. Анализ существующих подходов к классификации конфиденциальной информации по видам тайны.
5. Виды и характеристика носителей защищаемой информации.
6. Структура и характеристика угроз защищаемой информации.
7. Соотношение угроз защищаемой информации с видами носителей и формами проявления уязвимости информации.
8. Соотношение видов разведывательной деятельности с каналами и методами несанкционированного доступа к конфиденциальной информации.
9. Классификация и характеристика объектов защиты информации.
10. Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты.
11. Сущность, назначение и структура систем защиты информации.
12. Состав угроз информационной безопасности.
13. Методы обеспечения информационной безопасности.
14. Значение защиты информации во внешнеполитической деятельности.
15. Значение защиты информации в военной области.
16. Значение защиты информации в экономической сфере.
17. Социальные последствия защиты информации.
18. Влияние политико-правовых и социально-экономических реальностей на защиту информации.
19. Основные положения теории защиты информации.
20. Понятие и назначение концепции защиты информации.
21. Социально-экономические и организационно-правовые аспекты концепции защиты информации.
22. Требования к концепции защиты информации.
23. Уровни концепции защиты информации.
24. Понятие «носитель защищаемой информации». Способы фиксирования информации в носителях.
25. Свойства и значение типов носителей защищаемой информации. Соотношение видов носителей информации с категориями защищаемой информации и формами проявления ее уязвимости.
26. Показатели разделения конфиденциальной информации на виды тайны.
27. Общее и различия между степенью и грифом конфиденциальности (секретности).
28. Сферы действия государственной и служебной тайны.
29. Сферы действия коммерческой тайны.
30. Сферы действия личной и профессиональной тайны.
31. Формы собственности на информацию.
32. Собственники и владельцы информации, составляющей различные виды тайны.
33. Современные подходы к понятию угрозы защищаемой информации.
34. Признаки и составляющие угрозы защищаемой информации.
35. Состав и характеристика источников дестабилизирующего воздействия на информацию.
36. Виды и способы дестабилизирующего воздействия на информацию со стороны людей.

37. Виды и способы дестабилизирующего воздействия на информацию средств обработки, передачи информации и систем обеспечения их функционирования.
38. Соотношение видов дестабилизирующего воздействия на информацию с формами проявления уязвимости информации.
39. Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию.
40. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию со стороны людей.
41. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию средств обработки, передачи информации и систем обеспечения их функционирования.
42. Соотношение каналов несанкционированного доступа к информации с каналами утечки информации.
43. Соотношение каналов несанкционированного доступа к информации с источниками дестабилизирующего воздействия на информацию.
44. Методы несанкционированного доступа к информации через допущенных к ней лиц.
45. Методы несанкционированного доступа к информации через агентуру.
46. Методы несанкционированного доступа к информации через средства обработки, передачи информации и системы обеспечения их функционирования.
47. Методы несанкционированного физического проникновения на защищаемый объект.
48. Соотношение методов несанкционированного доступа к информации с используемыми техническими средствами.
49. Органы политической, военной и радиотехнической разведки в США.
50. Органы политической и военной разведки ведущих стран Западной Европы.
51. Соотношение между видами и направлениями разведывательной деятельности.
52. Состав подлежащих защите объектов хранения информации.
53. Состав подлежащих защите технических средств изготовления, обработки, воспроизведения и передачи информации.
54. Виды и способы дестабилизирующего воздействия на объекты защиты информации.
55. Классификация видов защиты информации.
56. Классификация методов защиты информации.
57. Классификация программных и криптографических средств защиты информации.
58. Классификация технических средств защиты информации.
59. Полномочия руководства предприятия и служб защиты информации в области защиты информации.
60. Состав и значение ресурсного обеспечения защиты информации.
61. Состав и сферы действия систем защиты информации.
62. Сущность и значение комплексной системы защиты информации.

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
Курсовой проект (работа)	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

ИРГУПС 2021-202 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