

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.О.60 Защита информации от несанкционированного доступа
рабочая программа дисциплины

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»
Специализация – № 5 «Безопасность открытых информационных систем»
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – очная форма, 5 лет 6 месяцев
Кафедра-разработчик программы – Информационные системы и защита информации

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

Формы промежуточной аттестации в семестрах:
Зачет А

Распределение часов дисциплины по семестрам

Семестр	А	Итого
Число недель в семестре	17	
Вид занятий	Часов по УП	Часов по УП
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	68	68
– лекции	34	34
– лабораторные работы	17	17
– практические (семинарские)	17	17
Самостоятельная работа	76	76
Зачёт		
Итого	144	144

ИРКУТСК

Электронный документ выгружен из ЕИС ФГБОУ ВО ИрГУПС и соответствует оригиналу

Подписант ФГБОУ ВО ИрГУПС Трофимов Ю.А.

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

Подпись соответствует файлу документа



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

Программу составил:
к.ф.-м.н., доцент

_____ А.А. Бутин

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

И.о. зав. кафедрой, к.э.н, доцент

_____ Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	обучение студентов основным принципам и базовым методикам защиты информации от несанкционированного доступа (НСД) к информации, анализа защищенности автоматизированных систем (АС).
1.2 Задачи дисциплины	
1	овладение актуальными нормативно-правовыми документами по защите информации ограниченного доступа в АС от НСД;
2	изучение возможностей и способов использования безопасных информационных технологий в работе современной АС при практической реализации требований отечественных стандартов информационной безопасности (ИБ);
3	освоение навыков эксплуатации программно-аппаратных средств защиты информации от НСД в АС (на основе программно-технических и программных образцов).
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
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"> – развитие мировоззрения и актуализация системы базовых ценностей личности; – приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям; – воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности как важнейшей черты личности, проявляющейся в заботе о своей стране, сохранении человеческой цивилизации; – воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях; – обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности; – выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации; – формирование у обучающихся исследовательского и критического мышления.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
Б1.О.39 Программно-аппаратные средства защиты информации	
Б1.О.43 Криптографические протоколы и стандарты	
Б1.О.46 Аудит информационных технологий и систем обеспечения информационной безопасности	
Б1.О.48 Теоретические основы компьютерной безопасности	
Б1.О.49 Методология анализа информационных рисков	
Б1.О.51 Кибербезопасность	
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б2.В.05 (Пд) Производственная - преддипломная практика
2	Б3.02 (Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах	ОПК-6.1. Знает основные принципы административно-правовой защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы	<p>Знать:</p> <ul style="list-style-type: none"> – правовые основы защиты информации от НСД; – способы построения модели угроз ИБ в АС. <p>Уметь:</p> <ul style="list-style-type: none"> – организовывать защиту информации ограниченного доступа в АС. <p>Владеть:</p> <ul style="list-style-type: none"> – навыками использования средств защиты информации

в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	от НСД в АС.
	ОПК-6.2. Умеет быстро реагировать на различные угрозы информационной безопасности и организует защиту информации ограниченного доступа	
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.2. Умеет применять доверенное хранение, защиту каналов связи и электронного документооборота	<p>Знать:</p> <ul style="list-style-type: none"> – основные требования к криптосистемам; – способы доверенного хранения информации. <p>Уметь:</p> <ul style="list-style-type: none"> – производить выбор необходимых средств криптографической защиты информации. <p>Владеть:</p> <ul style="list-style-type: none"> – навыками использования криптографических средств доверенного хранения информации..
ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ОПК-15.1. Имеет базовые навыки контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем	<p>Знать:</p> <ul style="list-style-type: none"> – методы настройки программно-аппаратных средств защиты информации от НСД в АС; – способы администрирования штатных и добавочных механизмов защиты информации от НСД. <p>Уметь:</p> <ul style="list-style-type: none"> – устанавливать добавочные программно-аппаратные средства обеспечения ИБ; – организовать проведения мониторинга защищенности АС. <p>Владеть:</p> <ul style="list-style-type: none"> – базовыми навыками администрирования добавочных программно-аппаратных средств защиты информации от НСД.
	ОПК-15.2. Умеет администрировать средства и системы защиты информации автоматизированных систем	
	ОПК-15.3. Имеет базовые навыки контроля функционирования средств и систем управления информационной безопасностью автоматизированных систем	

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	СР	
1.0	Эксплуатация объектов информатизации: стадии и нормативные документы. Виды НСД и условия работы средств защиты. Цели и задачи создания системы защиты информации (СЗИ) в АС	А	16	12	9	42	ОПК-6.1, ОПК-15.2, ОПК-15.3
1.1	Виды НСД. Принципы построения СЗИ в АС		4				
1.2	Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации		6				
1.3	Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации		6				
1.4	Подсистема управления доступом			3		6	
1.5	Подсистема регистрации и учета			3		6	
1.6	Криптографическая подсистема			3		6	
1.7	Подсистема обеспечения целостности			3		6	

1.8	Администрирование средства создания модели системы разграничения доступа (Ревизор 1 XP)				3	6	
1.9	Администрирование программы контроля полномочий доступа к информационным ресурсам (Ревизор 2 XP)				3	6	
1.10	Администрирование сетевого сканера (Ревизор сети)				3	6	
2.0	Эволюция системы требований к СЗИ. Современная система требований к СЗИ от НСД. Получение доказательств соответствия классу СЗИ	A	18	5	8	34	ОПК-6.2, ОПК-10.2, ОПК-15.1.
2.1	Меры и средства защиты информации от НСД		4				
2.2	Методы и средства контроля защищенности информации от НСД		4				
2.3	Формирование требований по защите информации и создание системы защиты информации от НСД.		4				
2.4	Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну		6				
2.5	Защищаемые информационные ресурсы, объекты защиты			5		6	
2.6	Администрирование программного обеспечения поиска и гарантированного уничтожения информации на дисках (Terrier 3.0)				3	6	
2.7	Администрирование программного обеспечения фиксации и контроля исходного состояния программного комплекса (ФИКС 2.0.2)				2	6	
2.8	Администрирование программного обеспечения сбора информации о программном и аппаратном обеспечении (Агент инвентаризации)				3	6	
2.9	Зачет					10	

* Код индикатора достижения компетенции проставляется или для всего раздела, или для каждой темы или для каждого вида работы.

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине: оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.1.1	А.А. Криулин, В.С. Нефедов, С.И. Смирнов	Основы безопасности прикладных информационных технологий и систем: учебное пособие https://reader.lanbook.com/book/167606#2	М.: МИРЭА, 2020	100% Онлайн
6.1.1.2	А.А. Миняев, Д.В. Юркин, М.М. Ковцур, К.А. Ахрамеева	Сертификация средств защиты информации: учебное пособие https://reader.lanbook.com/book/180100#3	СПб.: СПбГУС, 2020	100% Онлайн
6.1.1.3	Т. А. Поляковой, А. А. Стрельцова	Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов https://urait.ru/bcode/498844	М.: Юрайт, 2022	100% Онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	Прохорова О.В.	Информационная безопасность и защита информации: https://e.lanbook.com/reader/book/133924/#1	СПб: Издательство «Лань», 2020	100% Онлайн
6.1.2.2	А. В. Зенков	Информационная безопасность и защита информации : учебное пособие для вузов https://urait.ru/bcode/497002	М.: Юрайт, 2022	100% Онлайн
6.1.2.3	Г. М. Суворова	Информационная безопасность: учебное пособие для вузов https://urait.ru/bcode/496741	М.: Юрайт, 2022	100% Онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
6.1.3.1	Бутин А.А.	Методы и средства защиты информации от несанкционированного доступа. Программно-аппаратный уровень: учебное пособие	Иркутск: ИрГУПС, 2015	30
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»				
6.2.1	Сайт ФСТЭК РФ	http://fstec.ru/		
6.2.2	Сайт ФСБ РФ	http://www.fsb.ru/		
6.3 Программное обеспечение и информационные справочные системы				
6.3.1 Базовое программное обеспечение				
6.3.1.1	ОС MicrosoftWindows 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 WindowsEduPerDevice 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд			
6.3.1.2	Офисный пакет MicrosoftOffice 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; OfficeProfessional 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			
6.3.1.3	BorlandDelphi 7.			
6.3.2 Специализированное программное обеспечение				
6.3.2.1	VirtualBox. Бесплатное программное обеспечение (ПО). Количество не ограничено;			
6.3.2.2	Fierfox (браузер). Бесплатное ПО. Количество не ограничено			
6.3.2.3	ПО «Ревизор 1 XP», 15 лицензий			
6.3.2.4	ПО «Ревизор 2 XP», 15 лицензий			
6.3.2.5	ПО «Ревизор сети», 15 лицензий			
6.3.2.6	ПО «Terrier 3.0», 15 лицензий			
6.3.2.7	ПО «ФИКС 2.0.2», 15 лицензий			
6.3.2.8	ПО «Агент инвентаризации», 15 лицензий.			
6.3.3 Информационные справочные системы				
6.3.3.1	Научная электронная библиотека www.e-library.ru			
6.3.3.2	Национальная электронная библиотека https://нэб.рф			
6.4 Правовые и нормативные документы				
6.4.1	Консультант плюс consultant.ru			
6.4.2	ПСС Техэксперт www.cntd.ru			

**7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ,
НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ УЧЕБНОГО ПРОЦЕССА
ПО ДИСЦИПЛИНЕ**

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
---	--

2	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины. Помещения для хранения и профилактического обслуживания учебного оборудования – А-521.
3	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечена доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: MicrosoftOffice 2010, OpenOffice 3.0.1, 7-zip, BorlandDelphi 7, AbodeReaderXI, MicrosoftSecurityEssentials, а также специализированное ПО
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.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮДИСЦИПЛИНЫ

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 удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практическое (семинарское) занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины. Особое внимание следует обращать на определение основных понятий дисциплины. Обучающийся должен подробно разбирать примеры, которые поясняют понятия
Лабораторная работа	Один из видов практической работы, проводимой с целью углубления и закрепления теоретических знаний, развития навыков самостоятельной деятельности. Включает подготовку необходимых программно-аппаратных средств, составление плана работы, ее проведение и написание отчета.
Самостоятельная работа	Обучение по дисциплине «Защита информации от несанкционированного доступа» предусматривает активную самостоятельную работу обучающегося. На самостоятельную работу отводится 76 часов по очной форме обучения. Все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и отвечает на возникшие вопросы, обращаясь к сети интернет. Если этого будет недостаточно, можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удастся, то в обязательном

	порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

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.60 Защита информации от несанкционированного доступа**

Приложение № 1 к рабочей программе

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

ИРКУТСК

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией Университета, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

- оценка достижений обучающихся в процессе изучения дисциплины;
- обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;
- самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

- минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;
- базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;
- высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина. Программа контрольно-оценочных мероприятий. Показатели оценивания компетенций, критерии оценки

Дисциплина «Защита информации от несанкционированного доступа» участвует в формировании компетенций:

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

ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем

Программа контрольно-оценочных мероприятий очная форма обучения

№	Неделя	Наименование контрольно-	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства
---	--------	--------------------------	--	---------------------------------------	----------------------------------

		оценочного мероприятия	плины)	тенции	(форма проведения*)
А семестр					
1	1-17	Текущий контроль	Разделы 1-2 РПД	ОПК-6.1, 6.2; ОПК-15.1-15.3	Защита лабораторных работ (устно)
3	1-17	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с п. 4 РПД по данной дисциплине	ОПК-6.1, 6.2; ОПК-15.1-15.3	Сообщение, доклад (устно); наличие презентации
4	17	Промежуточная аттестация – зачёт	Разделы 1-2 РПД	ОПК-6.1, 6.2; ОПК 10.2; ОПК-15.1 - 15.3	зачет (устно)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

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 также краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
2	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите
3	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
4	Зачет	Средство, позволяющее оценить знания, умения, навыки и (или) опыта деятельности обучающегося по дисциплине.	Перечень теоретических вопросов и

	Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	практических заданий (билетов) к зачету
--	---	---

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

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

Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»	Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся, не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

Оценочное средство «Тест».

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

Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.

Результаты тестирования могут быть использованы при проведении промежуточной аттестации.

Промежуточная аттестация в форме зачета:

Критерии оценивания	Шкала оценивания
Обучающийся набрал при тестировании более 69 баллов	«зачтено»
Обучающийся набрал при тестировании менее 69 баллов	«не зачтено»

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

3.1 Перечень типовых тем докладов (сообщений)

См. п. 4 РПД

3.2 Перечень теоретических вопросов к зачету

Раздел 1

- 1.1. Виды НСД. Принципы построения СЗИ в АС;
- 1.2. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
- 1.3. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

Раздел 2

- 2.1. Меры и средства защиты информации от НСД;
- 2.2. Методы и средства контроля защищенности информации от НСД;
- 2.3. Формирование требований по защите информации и создание системы защиты информации от НСД;
- 2.4. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.

3.3 Перечень типовых простых практических заданий к зачету

1. Предложить программные и (или) программно-аппаратные средства защиты информации от НСД в АС по классу 3Б;
2. Предложить программные и (или) программно-аппаратные средства защиты информации от НСД в АС по классу 2Б;
3. Предложить программные и (или) программно-аппаратные средства защиты информации от НСД в АС по классу 1Г.

3.5 Структура фонда тестовых заданий

3.5.1 Защита информации от несанкционированного доступа

Структура фонда тестовых заданий по дисциплине «Защита информации от несанкционированного доступа»

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ
1. Эксплуатация объектов информатизации: стадии и нормативные документы. Виды НСД и условия работы средств защиты. Цели и задачи создания системы защиты информации (СЗИ) в АС	Виды НСД. Принципы построения СЗИ в АС. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.	34 – тип А 1 – тип В 1 – тип D
Итого по разделу		∑ 36 34– тип А 1- тип В

		1- тип D
2. Эволюция системы требований к СЗИ. Современная система требований к СЗИ от НСД. Получение доказательств соответствия классу СЗИ	Меры и средства защиты информации от НСД. Методы и средства контроля защищенности информации от НСД. Формирование требований по защите информации и создание системы защиты информации от НСД. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну	36 – тип А
	Итого по разделу	Σ 36 36– тип А
	Итого по дисциплине	Σ 72 70 – тип А 1 – тип В 1 – тип D

Используемые типы тестовых заданий (ТЗ):

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

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

ТЗ типа С: тестовое задание на установление соответствия;

ТЗ типа D: тестовое задание на установление правильной последовательности.

3.5.2 Структура фонда тестовых заданий

Структура типового итогового теста по дисциплине за весь период ее освоения

Раздел дисциплины	Тема раздела	Количество тестовых заданий (ТЗ), типы ТЗ
1. Эксплуатация объектов информатизации: стадии и нормативные документы. Виды НСД и условия работы средств защиты. Цели и задачи создания системы защиты информации (СЗИ) в АС	Виды НСД. Принципы построения СЗИ в АС. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.	11 – тип А 1 – тип В 1 – тип D
	Итого по разделу	Σ 13 11– тип А 1- тип В 1- тип D
2. Эволюция системы требований к СЗИ. Современная система требований к СЗИ от НСД. Получение доказательств соответствия классу СЗИ	Меры и средства защиты информации от НСД. Методы и средства контроля защищенности информации от НСД. Формирование требований по защите информации и создание системы защиты информации от НСД. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну	12 – тип А
	Итого по разделу	Σ 12 12– тип А
	Итого по дисциплине	Σ 25 23 – тип А

**Образец типового
итогового теста по дисциплине за весь период ее освоения**

Описание требований к тесту тест считается сданным, если обучающийся наберет более 69 баллов, время решения теста 90 минут, разрешается использовать лекционный материал для решения теста..

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

1. Основными этапами классификации АС являются:

- А) разработка и анализ исходных данных
- Б) выявление основных признаков АС, необходимых для классификации
- В) сравнение выявленных признаков АС с классифицируемыми
- Г) присвоение АС соответствующего класса защиты информации от НСД

2. Кем осуществляется выбор класса АС?

- А) заказчиком;
- Б) разработчиком;
- В) заказчиком и разработчиком;
- Г) контролирующими органами.

3. Сколько установлено классов защищенности АС от НСД:

- А) 9;
- Б) 8;
- В) 3;
- Г) 10.

4. Сколько установлено групп защищенности АС от НСД:

- А) 3;
- Б) 9;
- В) 5;
- Г) 1.

5. Каковы требования для подсистемы регистрации и учёта доступом по ЗБ?

- А) входа (выхода) субъектов доступа в (из) систему(ы) (узел сети);
- Б) запуска (завершения) программ и процессов (заданий, задач);
- В) создаваемых защищаемых объектов доступа;
- Г) доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей

6. Требования, предъявляемые к криптографической подсистеме по классу 2:

- А) шифрование конфиденциальной информации;
- Б) шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах;
- В) использование аттестованных (сертифицированных) криптографических средств

7. Каким требованиям должна соответствовать подсистема обеспечения целостности по классу 1Г:

- А) физическая охрана средств вычислительной техники и носителей информации;
- Б) периодическое тестирование СЗИ НСД;
- В) наличие средств восстановления СЗИ НСД;
- Г) использование сертифицированных средств защиты

8. Какие функции реализует Ревизор 1ХР?

- А) построение по результатам сканирования дерева ресурсов, соответствующего структуре ресурсов АРМ и ЛВС;
- Б) автоматическое сканирование локальных логических дисков, а также доступных сетевых папок. Выбор ресурсов для сканирования осуществляется администратором АРМ;
- В) установка прав доступа пользователей к объектам доступа, а также грифов секретности объектов доступа;
- Г) автоматическая регистрация в ПРД пользователей и удаление их уровней доступа

9. Признаки, по которым группируют АС в классы?

- А) наличие в АС информации различного уровня конфиденциальности;
- Б) уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- В) наличие функциональных возможностей обработки государственной тайны иностранных государств

10. Определить к какой группе будет относиться АС, в которой у пользователей одинаковые права доступа ко всей информации.

- А) третья группа;
- Б) первая группа;
- В) вторая группа

11. Какие АС попадают в первую группу?

- А) многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности;
- Б) многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация единого уровня конфиденциальности;
- В) АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности

12. Требования к криптографической подсистеме по 1А:

- А) шифрование конфиденциальной информации;
- Б) шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах;
- В) использование аттестованных (сертифицированных) криптографических средств

13. Требования к подсистеме обеспечения целостности по 3Б:

- А) обеспечение целостности программных средств и обрабатываемой информации;
- Б) использование сертифицированных средств защиты;
- В) периодическое тестирование СЗИ НСД

14. По требованиям к классу защищенности 3Б в параметрах регистрации подсистеме регистрации и учёта указывается:

- А) дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- Б) учёт всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку);
- В) результат попытки входа: успешная или неуспешная (при НСД)

15. По требованиям к классу защищенности 2Б подсистема обеспечения целостности:
- А) целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;
 - Б) целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;
 - В) целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

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

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Сообщение, доклад	Обучаемый самостоятельно или под руководством преподавателя выбирает тему, изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит сообщение или доклад по результатам освоения темы, объемом до 20 стр. текста размером 12 пунктов, интервал 1,5; представляет сообщение/доклад преподавателю, отвечает на его вопросы.
Защита лабораторной работы	Обучаемый самостоятельно, под руководством преподавателя выполняет лабораторную работу на заданную тему. Тема (задание) предлагается в конкретном виде. Методы и инструменты для ее разработки предлагаются преподавателем. После выполнения задания обучаемый готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования (защиты). Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся
Тест	<p>Тестирование с применением компьютерных технологий проводится по окончании каждого семестра и по окончании изучения дисциплины и (или) в течение года по завершению изучения дисциплины (контроль/проверка остаточных знаний, умений, навыков и (или) опыта деятельности). Тесты формируются из фонда тестовых заданий по дисциплине. Структура фонда тестовых заданий по дисциплине, структуры тестов по итогам каждого семестра и итогового теста по дисциплине и типовые примеры тестов приведены в разделе 3 данного документа.</p> <p>Результаты тестирования могут быть использованы при проведении промежуточной аттестации, как в форме зачета, так и в форме экзамена.</p> <p>Описание требований, выполнение которых необходимо для успешного выполнения теста: тематика теста; перечень знать, уметь, владеть; виды и количество предъявляемых обучающемуся тестовых заданий; проходной балл; критерии оценки; норма времени; дополнительные требования, включая необходимость использования справочных таблиц и проч.</p> <p>Тесты для самоконтроля обучающихся по разделам дисциплины, сформированы их из материалов фонда тестовых заданий дисциплины. Требования к тестам для самоконтроля аналогичны требованиям к итоговым тестам по семестрам и дисциплине в целом</p>

Для организации и проведения промежуточной аттестации (в форме зачета/экзамена) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

– перечень теоретических вопросов к зачету для оценки знаний, умений и навыков.

Перечень теоретических вопросов к зачету обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

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

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра и результатами тестирования по материалам, изученным в течении семестра. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, в совокупности с тестированием, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок). Время проведения тестирования объявляется обучающимся заранее.

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

Средняя оценка уровня сформированности компетенций по результатам текущего контроля и тестирования за семестр	Оценка
Оценка не менее 3.0, нет ни одной неудовлетворительной оценки по текущему контролю и обучающийся набрал при тестировании более 69 баллов	«зачтено»
Оценка менее 3.0, или получена хотя бы одна неудовлетворительная оценка по текущему контролю, или обучающийся набрал при тестировании менее 69 баллов	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация в форме зачета проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач (не более двух теоретических и двух практических). Промежуточная аттестация в форме зачета с проведением аттестационного испытания в форме собеседования проходит на последнем занятии по дисциплине.