ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «08» мая 2020 г. № 266-1

Б1.Б.1.29 Разработка и эксплуатация защищенных автоматизированных систем

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
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 9, курсовая работа 9

Распределение часов дисциплины по семестрам

Семестр	9	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**54**	**54**
– лекции	18	18
– лабораторные	18	18
- практические	18	18
Самостоятельная работа	**54**	**54**
Экзамен	**36**	**36**
Итого	**144**	**144**

ИРКУТСК

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цели освоения дисциплины

1	Целью изучения дисциплины Информационная безопасность автоматизированных систем является формирование важнейших представлений о теории и практике создания защищенных автоматизированных систем.

1.2 Задачи освоения дисциплины

1	Задачей изучения дисциплины является передача студентам итоговых основ по защите информации, включая вопросы ее конфиденциальности, целостности и доступности; обучение умению применять полученные знания для решения прикладных задач по защите автоматизированных систем с учетом развития информационных технологий и программного обеспечения.

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Профессионально-трудовое воспитание обучающихся

Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда.

Цель достигается по мере решения в единстве следующих задач:
– формирование сознательного отношения к выбранной профессии;
– воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность;
– формирование психологии профессионала;
– формирование профессиональной культуры, этики профессионального общения;
– формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1 Требования к предварительной подготовке обучающегося

1	Б1.Б.1.22 Основы информационной безопасности
2	Б1.В.ДВ.07.01 Экономика защиты информации
3	Б1.В.ДВ.07.02 Методология определения ценности информации

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б1.В.06 Комплексная защита в информационных системах персональных данных
2	Б1.Б.1.30 Управление информационной безопасностью
3	Б2.Б.04(Н) Производственная - научно-исследовательская работа
4	Б2.Б.06(Пд) Производственная - преддипломная

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

ПК-6: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности

Минимальный уровень освоения компетенции	
Знать	основные концепции, связанные с автоматизированными системами
Уметь	использовать основные концепции и принципы, связанные с автоматизированными системами
Владеть	владеть основными концепциями, принципами, теориями и фактами, связанными с автоматизированными системами на нижнем уровне
Базовый уровень освоения компетенции	
Знать	применять на практике основные концепции, связанные с автоматизированными системами
Уметь	применять на практике основные концепции и принципы, связанные с автоматизированными системами
Владеть	владеть основными концепциями, принципами, теориями и фактами, связанными с автоматизированными системами на среднем уровне
Высокий уровень освоения компетенции	
Знать	основные концепции, принципы, теории и факты, связанные с информатикой

Уметь	применять на практике основные концепции, принципы, теории и факты, связанные с автоматизированными системами
Владеть	владеть основными концепциями, принципами, теориями и фактами, связанными с автоматизированными системами на высоком уровне

ПК-20: способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	
Минимальный уровень освоения компетенции	
Знать	стандарты информационной безопасности
Уметь	использовать средства защиты автоматизированных систем, включая технические и криптографические средства
Владеть	современными методами исследования, оценивания и представления результатов выполненной работы
Базовый уровень освоения компетенции	
Знать	криптографические методы защиты информации
Уметь	обеспечивать безопасность и целостность электронных сообщений
Владеть	руководящими документами по безопасности информации
Высокий уровень освоения компетенции	
Знать	организационные средства защиты информации
Уметь	Пользоваться методиками и методами обеспечения безопасности и целостности данных
Владеть	типовыми средствами защиты информации

ПК-27: способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	
Минимальный уровень освоения компетенции	
Знать	стандарты информационной безопасности
Уметь	использовать средства защиты автоматизированных систем, включая технические и криптографические средства
Владеть	современными методами исследования, оценивания и представления результатов выполненной работы
Базовый уровень освоения компетенции	
Знать	криптографические методы защиты информации
Уметь	обеспечивать безопасность и целостность электронных сообщений
Владеть	руководящими документами по безопасности информации
Высокий уровень освоения компетенции	
Знать	организационные средства защиты информации
Уметь	Пользоваться методиками и методами обеспечения безопасности и целостности данных
Владеть	типовыми средствами защиты информации

В результате освоения дисциплины обучающийся должен

Знать	
1	средства защиты автоматизированных систем, включая технические и криптографические средства;
2	стандарты информационной безопасности;
3	руководящие документы по безопасности информации;
Уметь	
1	обеспечивать безопасность и целостность электронных сообщений;
2	пользоваться криптографическими методами защиты информации;
Владеть	
1	типовыми средствами автоматизированных систем.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»

	Раздел 1. Угрозы безопасности информационных систем и их классификация.				
1.1	Цели и задачи безопасности и защиты программных систем. Основные виды угроз. Характеристика и классификация угроз и атак /Лек/	9	2	ПК-6	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
1.2	Проработка лекционного материала: цели и задачи безопасности и защиты программных систем, основные виды угроз, характеристика и классификация угроз и атак /Ср/	9	10	ПК-6	Л1.1 Л1.3 Л3.1
	Раздел 2. Управление информационными рисками.				
2.1	Неопределенность и риск. Модели оценки рисков. Трехфакторная модель оценки информационных рисков /Лек/	9	4	ПК-20	Л1.1 Л1.3 Л2.1 Л3.1
2.2	Проработка лекционного материала: неопределенность и риск, модели оценки рисков, трехфакторная модель оценки информационных рисков /Ср/	9	10	ПК-20	Л1.1 Л1.2 Л2.1 Л3.1
2.3	Подготовка к лабораторному занятию «Контроль целостности информации при случайных воздействиях» /Лаб/	9	6	ПК-6	Л1.1 Л1.3 Л2.1 Л3.1
2.4	Контроль целостности информации при случайных воздействиях /Лаб/	9	6	ПК-20	Л1.1 Л1.2 Л2.1 Л3.1
	Раздел 3. Обеспечение конфиденциальности обрабатываемой программой информации.				
3.1	Основные понятия криптографии. Российский алгоритм криптографического преобразования /Лек/	9	2	ПК-27	Л1.1 Л1.3 Л2.1 Л3.1
3.2	Проработка лекционного материала: основные понятия криптографии, российский алгоритм криптографического преобразования /Ср/	9	5	ПК-27	Л1.1 Л1.3 Л2.1 Л3.1
3.3	Двухключевые криптосистемы. Современный протокол шифрования информации /Лек/	9	2	ПК-27	Л1.1 Л1.3 Л2.1 Л3.1
3.4	Проработка лекционного материала: двухключевые криптосистемы, современный протокол шифрования информации /Ср/	9	5	ПК-20	Л1.1 Л1.3 Л2.1 Л3.1
3.5	Подготовка к лабораторному занятию «Методика определения информационных рисков» /Лаб/	9	4	ПК-20	Л1.1 Л1.3 Л2.1 Л3.1
3.6	Методика определения информационных рисков /Лаб/	9	2	ПК-27	Л1.1 Л1.3 Л2.1 Л3.1
	Раздел 4. Технология электронной подписи при обработке программой информации.				
4.1	Хэш-функции, российский стандарт. Правовое обеспечение электронной подписи /Лек/	9	2	ПК-6	Л1.1 Л1.3 Л2.1 Л3.1
4.2	Проработка лекционного материала: Хэш-функции, российский стандарт, правовое обеспечение электронной подписи /Ср/	9	5	ПК-6	Л1.1 Л1.2 Л1.3 Л3.1
4.3	Криптографические методы технологии электронной подписи, российский стандарт /Лек/	9	2	ПК6	Л1.1 Л1.3 Л2.1 Л3.1

4.4	Проработка лекционного материала: криптографические методы технологии электронной подписи, российский	9	5	ПК-271	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
4.5	Подготовка к Лабораторному занятию «Порядок проведения классификация информационных систем в РФ» /Лаб/	9	4	ПК-27	Л1.1 Л1.3 Л2.1 Л3.1, Л4.1
4.6	Порядок проведения классификация информационных систем в РФ /Лаб/	9	6	ПК-27	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1
	Раздел 5. Технологии и методы аутентификации				
5.1	Основные понятия и определения. Инфраструктура управления открытыми ключами /Лек/	9	2	ПК-20	Л1.1 Л1.3 Л2.1 Л3.1
5.2	Проработка лекционного материала: основные понятия и определения, инфраструктура управления открытыми	9	14	ПК-20	Л1.1 Л1.2 Л1.3 Л2.2 Л3.1
5.3	Подготовка к лабораторному занятию «Технология применения электронной подписи» /Лаб/	9	4	ПК-20	Л1.1 Л1.3 Л2.1 Л3.1, Л4.1
5.4	Технология применения электронной подписи /Лаб/	9	6	ПК-20	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1
	Экзамен	9	36	ПК-6, ПК-20, ПК-27	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л3.1

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 разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

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	Паршин К.А.	Оценка уровня информационной безопасности на объекте информатизации: учеб. пособие для вузов ж.-д. трансп.	М.: УМЦ по образованию на ж.-д. трансп., 2015	19
	Бутин А.А.	Методы и средства защиты информации от несанкционированного доступа. Программно-аппаратный уровень : учеб. пособие	Иркутск: ИрГУПС, 2015	45
	Ададуров С.Е., Глухов А.П., Диасамидзе С.В., Еремеев М.А., Корниенко А.А, Яковлев	Информационная безопасность и защита информации на железнодорожном транспорте: Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте: учебник	М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014	30

	В.А.			
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Краковский Ю.М.	Информационная безопасность и защита информации: учеб. пособие	М.: МарТ, 2008	20
Л2.2	Галатенко В.А., Бетелин В.Б.,	Основы информационной безопасности. Учебное пособин: дополнительная литература	М.: Издательство "Интернет-университет информационных технологий", 2008	10
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Бутырин О.В.	Теория языков программирования и методы трансляции : учебное пособие.	Иркутск : ИрГУПС, 2007.	98
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	Бутырин О.В.	Курс лекций «Теория языков программирования и методы трансляции».	Личный кабинет обучающегося	100% онлайн
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	Википедия: свободная энциклопедия. https://ru.wikipedia.org			
Э.2	Национальный открытый университет ИНТУИТ http://www.intuit.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 XP Professional with Service Pack 2, лицензия Open License, Количество - 427			
6.3.1.2	Офисный пакет Microsoft Office 2010, OpenLicense, Количество - 155			
6.3.2 Перечень специализированного программного обеспечения				
6.3.2.1	Borland Delphi 7			
6.3.3 Перечень информационных справочных систем				
6.3.3.1	Информационно-справочная система КонсультантПлюсhttp://www.consultant.ru			

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, плакаты, таблицы), обеспечивающие тематические иллюстрации содержания дисциплины.
3	Учебная лаборатория «Средства и методы защиты информации», Д-523.
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 для хранения и профилактического обслуживания учебного оборудования – А-521.

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.
Лабораторная работа	Внимательно ознакомиться с целью, задачами и описанием лабораторной работы. Изучить теоретический материал, выполнить практическое задание, используя необходимые программные и аппаратно-технические средства, оформить отчет в соответствии с заданием и требованиями нормоконтроля. Ответить на вопросы по теме лабораторной работы. В ходе выполнения лабораторных работ раскрываются основные вопросы в рамках рассматриваемой темы, делаются акценты на наиболее сложные, проблемные и моменты изучаемого материала, которые должны быть приняты студентами во внимание. Основной целью лабораторных занятий является расширение и углубление материала практического характера, контроль качества усвоения пройденного материала и ходом выполнения студентами заданий. При подготовке к зачету необходимо ориентироваться на лекции, результаты выполненных лабораторных работ и рекомендуемую литературу.
Практические (семинарские) занятия	Обобщение, расширение и углубление пройденного материала на лекции. Решение задач на закрепление практических навыков. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы, анализа литературных источников, публичного выступления и аргументации собственного мнения. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в дискуссиях и коллоквиумах. Контроль качества усвоения пройденного материала.
Курсовая работа	Изучение научной, учебной, нормативной и другой литературы. Отбор необходимого материала; формирование выводов и разработка конкретных рекомендаций по решению поставленной задачи; проведение практических исследований по заданной теме. Инструкция по выполнению требований к оформлению курсовой работы (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Самостоятельная работа	Изучение лекционного материала и восстановление в памяти изученного в ходе выполнения лабораторной работы материала, который необходим для защиты лабораторной работы, понимания нового материала, подготовки к экзамену. Работа с учебником, лекцией, лабораторным практикумом, сетью Интернет. Со стороны преподавателя: формулировка указаний и инструкций по выполнению самостоятельной работы, описание формы контроля и критериев оценивания.
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.	

Приложение 1 к рабочей программе по дисциплине Б1.Б1.29 «Разработка и эксплуатация защищенных автоматизированных систем»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.Б1.29 «Разработка и эксплуатация защищенных автоматизированных систем»

1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Дисциплина Б1.Б1.29 «Разработка и эксплуатация защищенных автоматизированных систем» формирует следующие компетенции:

ПК-6 - способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности

ПК-20 - способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

ПК-27: способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы

Таблица траекторий формирования компетенций ПК-6, ПК-20 и ПК-27 у обучающихся при освоении основной образовательной программы

Код компетен-ции	Наименование компетенции	Индекс и наименование дисциплины, участвующей в формировании компетенции	Семестр изучения дисциплины
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Б1.Б.1.22 Основы информационной безопасности	2
		Б1.В.ДВ.07.01 Экономика защиты информации	3
		Б1.В.ДВ.07.02 Методология определения ценности информации	5
		Б1.В.06 Комплексная защита в информационных системах персональных данных	6
		Б1.Б1.29 «Разработка и эксплуатация защищенных автоматизированных систем»	9
ПК-20	способностью организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Б1.Б.1.22 Основы информационной безопасности	2
		Б1.В.ДВ.07.01 Экономика защиты информации	3
		Б1.В.ДВ.07.02 Методология определения ценности информации	5
		Б1.В.06 Комплексная защита в информационных системах персональных данных	6
		Б1.Б1.29 «Разработка и эксплуатация защищенных автоматизированных систем»	9
ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик	Б1.Б1.29 «Разработка и эксплуатация защищенных автоматизированных систем»	9

	информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы		

Таблица соответствия уровней освоения компетенций ПК-6, ПК-20 и ПК-27 планируемым результатам обучения

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенции (признаки проявления) - конкретизация формулировки компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	**Раздел 1. Угрозы безопасности информационных систем и их классификация**	Минимальный уровень освоения (уровень 1): способностью анализировать и обобщать информацию.	**Знать**: способность к обобщению, стандарты безопасности; **Уметь:** пользоваться руководящими документами по безопасности информации; **Владеть**: рганизационными средствами защиты информации.
		Раздел 2. Управление информационными рисками	Базовый уровень освоения (уровень 2): способностью определять угрозы информационной безопасности.	**Знать**: средства защиты информации, включая технические и криптографические средства; **Уметь**: обеспечивать безопасность и целостность электронных сообщений; **Владеть**: методиками и методами исследования и обеспечения безопасности и целостности данных.
ПК-20	способностью организовать разработку, внедрение, эксплуатацию	**Раздел 3. Обеспечение конфиденциальности обрабатываемой программой информации**	Высокий уровень освоения (уровень 3): способностью проводить анализ и исследовать модели защищенности информационных систем	**Знать**: способность к анализу, систематизации и прогнозированию. **Уметь:** пользоваться криптографическими методами защиты информации **Владеть**: типовыми средствами защиты

	и сопровождение автоматизированной системы с учетом требований информационной безопасности		Минимальный уровень освоения (уровень 1): способностью применять современные методы исследования	информации. **Знать:** стандарты информационной безопасности, современные методы исследования; **Уметь:** пользоваться руководящими документами по безопасности информации; **Владеть:** организационными средствами защиты информации.
		Раздел 4. Технология электронной подписи при обработке программой информации	Базовый уровень освоения (уровень 2): способностью представлять результаты выполненной работы	**Знать:** средства защиты информации, включая технические и криптографические средства; **Уметь:** обеспечивать безопасность и целостность электронных сообщений; **Владеть:** методиками и методами исследования и обеспечения безопасности и целостности данных.
		Раздел 5. Технологии и методы аутентификации	Высокий уровень освоения (уровень 3): способностью применять современные методы исследования и способностью представлять результаты выполненной работы	**Знать:** современные методы исследования, средства оценки и представления результатов выполненной работы. **Уметь:** пользоваться криптографическими методами защиты информации. **Владеть:** типовыми средствами защиты информации.
ПК-27	выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит	**Раздел 4. Технология электронной подписи при обработке программой информации**	Базовый уровень освоения (уровень 2): способностью представлять результаты выполненной работы	**Знать:** средства защиты информации, включая технические и криптографические средства; **Уметь:** обеспечивать безопасность и целостность электронных сообщений; **Владеть:** методиками и методами исследования и обеспечения безопасности и целостности данных.
		Раздел 5. Технологии и методы аутентификации	Высокий уровень освоения (уровень 3): способностью	**Знать:** средства защиты информации, включая

	безопасности автоматизированной системы способностью		применять современные методы исследования и способностью представлять результаты выполненной работы	технические и криптографические средства; **Уметь:** обеспечивать безопасность и целостность электронных сообщений; **Владеть:** методиками и методами исследования и обеспечения безопасности и целостности данных.

Программа контрольно-оценочных мероприятий на период изучения дисциплины (модуля)

№	Неделя	Название оценочного мероприятия	Объект контроля (компетенция, знание понятий, раздел дисциплины и т.д.)		Наименование оценочного средства, форма проведения
1	2	3	4	5	6
1	1,2,3,4	Текущий контроль	Раздел 1. Угрозы безопасности информационных систем и их классификация	ПК-6 ПК-20	Защита лабораторной работы (проверка на правильность выполнения и оформления лабораторного задания; собеседование - беседа с обучающимися на темы, связанные с изучаемой темой, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме).
2	5,6,7,8	Текущий контроль	Раздел 2. Управление информационными рисками	ПК-6 ПК-20	Защита лабораторной работы (проверка на правильность выполнения и оформления лабораторного задания; собеседование - беседа с обучающимися на темы, связанные с изучаемой темой, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме).
3	9,10,11	Текущий контроль	Раздел 3. Обеспечение конфиденциальност	ОПК-6 ПК-20	Защита лабораторной работы (проверка на правильность выполнения и оформления

			и обрабатываемой программой информации		лабораторного задания; собеседование - беседа с обучающимися на темы, связанные с изучаемой темой, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме).
4	12, 13	Текущий контроль	Раздел 4. Технология электронной подписи при обработке программой информации	ПК-20 ПК-27	Защита лабораторной работы (проверка на правильность выполнения и оформления лабораторного задания; собеседование - беседа с обучающимися на темы, связанные с изучаемой темой, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме).
5	14,15,16, 17	Текущий контроль	Раздел 5. Технологии и методы аутентификации	ПК-20 ПК-27	Защита лабораторной работы (проверка на правильность выполнения и оформления лабораторного задания; собеседование - беседа с обучающимися на темы, связанные с изучаемой темой, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме).
6	18	Промежуточный контроль (зачет).	**Все разделы.**	ПК-6 ПК-20 ПК-27	В устной и письменной формах (вопросы по разделам дисциплины).

2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений, обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания заносятся преподавателем в журнал и 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 сформированности компетенций представлен в нижеследующей таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС

Текущий контроль успеваемости			
1	Отчет по лабораторной работе	Средство для проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по разделу дисциплины. Рекомендуется для оценки знаний, умений и владений обучающихся	Комплекты заданий для выполнения лабораторных работ по темам/разделам дисциплины
2	Конспект	Средство, позволяющее формировать и оценивать способность обучающегося к восприятию, обобщению и анализу информации. Рекомендуется для оценки знаний и умений обучающихся	Темы конспектов по дисциплине
Промежуточная аттестация			
8	экзамен	Средство, позволяющее оценить знания, умения и владения обучающегося по дисциплине. Рекомендуется для оценки знаний, умений и владений навыками обучающихся	Комплект теоретических вопросов и практических заданий к экзамену по разделам

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме экзамена (в конце семестра), а также шкала для оценивания уровня освоения компетенций представлена в следующей таблице

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенций
«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	Минимальный

		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	
«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	Компетенции не сформированы

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

Критерии и шкала оценивания лабораторной работы

Выполнение отчета по лабораторной работе (письменно) и защита лабораторной работы (устно):

Оценка	Критерий оценки
«отлично»	Обучающийся полностью и правильно выполнил задание лабораторной работы. Показал отличные знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Отчет по лабораторной работе оформлен аккуратно и в соответствии с предъявляемыми требованиями. Ответил на все дополнительные вопросы на защите
«хорошо»	Обучающийся выполнил задание лабораторной работы с небольшими неточностями. Показал хорошие знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Есть недостатки в оформлении отчета по лабораторной работе. Ответил на большинство дополнительных вопросов на защите
«удовлетворительно»	Обучающийся выполнил задание лабораторной работы с существенными неточностями. Показал удовлетворительные знания, умения и владения навыками применения их при решении задач в рамках усвоенного учебного материала. Качество оформления отчета по лабораторной работе имеет недостаточный уровень. При ответах на дополнительные вопросы на защите было допущено много неточностей
«неудовлетворительно»	При выполнении лабораторной работы обучающийся продемонстрировал недостаточный уровень знаний, умений и владения ими при решении задач в рамках усвоенного учебного материала. Обучающийся неспособен пояснить полученные результаты. При ответах на дополнительные вопросы на защите было допущено множество неточностей

Критерии и шкала оценивания конспекта

Оценка	Критерий оценки

«отлично»	Конспект полный. В конспектируемом материале выделена главная и второстепенная информация. Установлена логическая связь между элементами конспектируемого материала. Даны определения основных понятий; основные формулы приведены с выводом, дана геометрическая иллюстрация. Приведены примеры
«хорошо»	Конспект полный. В конспектируемом материале выделена главная и второстепенная информация. Установлена не в полном объеме логическая связь между элементами конспектируемого материала. Даны определения основных понятий; основные формулы приведены без вывода, частично дана геометрическая иллюстрация. Примеры приведены частично
«удовлетворительно»	Конспект не полный. В конспектируемом материале не выделена главная и второстепенная информация. Не установлена логическая связь между элементами конспектируемого материала. Даны определения основных понятий; основные формулы приведены без вывода, нет геометрической иллюстрации. Примеры отсутствуют
«неудовлетворительно»	Конспект не удовлетворяет ни одному из критериев, приведенных выше

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 Типовые контрольные задания

«Контроль целостности информации при случайных воздействиях»

Целью работы является изучение различных методов обнаружения ошибок при передаче сообщений и их сравнение.

Введение

Целостность информации может быть нарушена путем ее модификации, уничтожения, замены, повтора или другого типа искажения. Целостность информации может нарушиться либо злоумышленником, либо случайным воздействием внешней и внутренней среды, включая людей.

В контрольной работе рассматриваются методы контроля целостности информации (сообщений) при случайных воздействиях. Предполагается, что одна сторона (отправитель) отправляет сообщение, а другая (получатель)

получает его. При передаче в канале связи возможно нарушение целостности сообщения.

Методы контроля целостности информации от случайных воздействий делят на методы обнаружения ошибок (обнаружения самого факта ошибок без определения их положения в сообщении) и методы обнаружения ошибок с определением их положения в сообщении и последующим исправлением. В обоих этих случаях рассматривают одиночную ошибку и случай более одной ошибки.

В контрольной работе рассматриваются методы обнаружения ошибок. Предполагается, что одна сторона (отправитель) отправляет сообщение, а другая (получатель) получает его. При передаче в канале связи возможно нарушение целостности сообщения от случайных воздействий. Получатель должен иметь возможность проверить нарушена или нет целостность информации.

Технология и методы контроля целостности информации

Технология контроля целостности следующая:

1) отправитель, используя метод контроля, формирует контрольное значение для сообщения ($КО_m$), которое передает совместно с сообщением m;

2) получатель, получив сообщение m и контрольное значение отправителя $КО_m$, используя тот же метод контроля, создает свое контрольное значение ($КР_m$);

3) получатель сравнивает контрольные значения: $КО_m = КР_m$. Если они совпадают, то получатель считает, что целостность информации не нарушена; иначе она нарушена и надо повторить передачу сообщения.

В случае обнаружения одиночной ошибки на практике используются метод контроля четности и метод контрольной суммы.

При использовании метода контроля четности для каждого байта информации резервируется один разряд (бит), который и является контрольным значением. Значение бита четности является результатом сложения по модулю 2 байта сообщения. Например: 10010010 1; 00010100 0.

Напомним, что таблица истинности для сложения по модулю 2 имеет вид: 0(+)0=0; 1(+)0=1; 0(+)1=1; 1(+)1=0. Отличие от обычного сложения заключается в том, что в последней комбинации при сложении по модулю 2 отсутствует единица переноса, что существенно повышает быстродействие этой операции.

Если сообщение представляется двумерной структурой, то бит четности формируется по каждому столбцу, который является также результатом сложения по модулю 2. Совокупность этих битов четности образует контрольное значение, которое называют контрольной суммой (КС). Размерность контрольной суммы определяется размерностью данных в файле. Например: 2-х, 4-х, 8-и байтовое слово. Рассмотрим пример для 2-х байтового слова (рис. 1).

10010100 01100101

10100010 00011101
10000110 00011101
КС 10110000 01100101

Рис. 1. Создание контрольной суммы

Используя операцию сложения по модулю 2, для первого столбца получим 1, для второго 0 и т.д.

Метод контрольной суммы используется в сетевых технологиях, например, в протоколе TCP для Интернета. При сетевой передаче сообщение разбивается на пакеты, далее для каждого пакета формируется своя контрольная сумма. Если контрольные суммы отправителя и получателя совпадают, то считается, что целостность пакета не нарушена. Метод контрольной суммы является достаточно быстродействующим, но он обнаруживает одиночную ошибку по каждому столбцу файла. В связи с этим, в настоящее время в сетевых протоколах используется метод циклического контроля (CRC), который позволяет обнаруживать более одной ошибки.

При методе CRC сообщение рассматривается как N-разрядное двоичное число, где N – количество битов в сообщении. Далее оно специальным образом делится на простое целое число до получения остатка. Этот остаток иногда по аналогии с методом контрольной суммы называют контрольной суммой. Остаток является искомым контрольным значением. Его вычисляет как отправитель, так и получатель.

При делении N-разрядного числа на простое число (его еще называют полиномом) используется деление по модулю два. Разрядность полинома должна быть на один бит больше, чем разрядность остатка. Для однобайтового остатка рекомендуется полином 100011011 или 10110000 1.

Деление по модулю 2 осуществляется сложением по модулю 2. Рассмотрим этот метод на примере (рис. 2): сообщение 101111001110, полином 10011 (простое число), остаток имеет четыре бита.

```
⊕ 101111001110 | 10011
  10011        |
  -----        |
⊕   10010
    10011
    -----
⊕     10111
      10011
      -----
         1000
```

Рис. 2. Деление по модулю 2

Остаток от деления равен 1000. На практике для больших значений N при делении используется специально составленная таблица размером 2^nxn, где n – разрядность остатка (контрольного значения).

Помимо современных сетевых протоколов, метод CRC, например, используется при обмене информацией между оперативной и внешней памятью (винчестером).

Список контрольных вопросов

1. Что такое целостность информации.
2. Что понимается под случайным воздействием на информацию.
3. Опишите технологию контроля информации при случайных воздействиях.
4. В чем отличие методов обнаружения ошибок от методов обнаружения и исправления ошибок.
5. Отличие сложения по модулю 2 от обычного сложения.

Содержание контрольной работы

1. Используя данные своего варианта (табл. 1), записать файл (сообщение m) в виде матрицы, длина строки равна байту, число строк равно четырем. При переходе от 16-ричной системы к двоичной можно использовать таблицу 3.1 из лабораторной работы №3.
2. Найти контрольную сумму отправителя ($КО_m$);
3. Изменить один бит (выбрать самому) в исходном сообщении и найти контрольную сумму получателя ($КР_m$);
4. Убедиться, что контрольные суммы не совпадают;
5. Изменить два бита в одном столбце исходного сообщения;
6. Найти контрольную сумму получателя ($КР_m$) и убедиться, что контрольные суммы отправителя и получателя совпадают. Объяснить почему;
7. Найти остаток от деления по модулю 2 для исходного сообщения (значение полинома имеется в таблице 1) – (ОО);
8. Найти остаток от деления по модулю 2 для сообщения с двумя ошибками – (ОР);
9. Убедиться, что остатки не совпадают. Объяснить почему.

Варианты контрольной работы

Таблица 1

№	Исходное сообщение	Полином
1	A6, BC, 67, 9F	100011011
2	C6, BC, D7, 9F	100011011

3	D6, BC, A5, 3A	100011011
4	B4, B1, 6A, 9E	100011011
5	A6, BE, 62, 8C	100011011
6	A7, CC, DA, 9F	100011011
7	B6, AC, 67, 7E	100011011
8	A6, 4C, 52, 9D	100011011
9	CA, B4, D7, 97	101100001
10	D6, BC, A5, 3A	101100001
11	F4, B1, 6A, 9E	101100001
12	C6, BE, 62, 8C	101100001
13	B7, C5, D1, 9F	101100001
14	E3, AC, 6A, 7E	101100001
15	A2, 4C, C2, 9D	101100001
16	A8, BC, E7, 9F	101100001
17	FA, B4, 37, 97	100011011
18	E6, BC, D7, 3A	100011011
19	A4, B1, 6A, 9E	100011011
20	CB, BE, 62, 8C	101100001

Список контрольных вопросов к разделу 2

1. Стандарты информационной безопасности.
2. Характеристика и классификация угроз информационной безопасности.
3. Методы оценки субъективных вероятностей.
4. Управление рисками информационной безопасности.
5. Понятие уязвимости системы защиты информации.
6. Возможные подходы к оценке рисков.
7. Этапы процесса управления рисками.
8. Назначение и функции программных продуктов для аудита информационной безопасности и анализа рисков.
9. Вопросы по методике определения информационных рисков.

Список контрольных вопросов к разделу 3

1. Информационная безопасность и безопасность информации.
2. Аспекты безопасности информации.
3. Основные понятия криптографии.
4. Классификация криптосистем.
5. Общая схема шифрования.
6. Способы формирования ключей для поточного шифрования.
7. Вопросы по поточному шифрованию.
8. Что такое угроза и уязвимость.
9. Конфиденциальность информации и методы ее защиты.

Тестовые задания к разделу 4

1) Укажите двухключевую криптосистему:
А) DES
Б) RSA
В) AES
Г) ГОСТ 28147-89

2) Укажите одностороннюю функцию для алгоритма RSA:
А) $(e \cdot d) \bmod k = 1;\ k=p \cdot (q-1);$
Б) $y = a^x \bmod p;$
В) $n = p \cdot q;$
Г) $c = m^e \bmod (n-1);$

3) При зашифровании данных несимметричной криптосистемой, используется:
А) секретный ключ
Б) открытый ключ
В) сначала открытый, а затем секретный ключ
Г) сначала секретный, а затем открытый ключ

4) Размер хэш-образа по российскому стандарту (ГОСТ-2012) равен:
А) 256 бит или 512 бит
Б) 512 бит или 160 бит
В) 160 бит
Г) 320 бит

5) Двухключевая криптосистема по сравнению с одноключевой имеет более высокую производительность при шифровании данных:
А) ДА
Б) НЕТ

6) Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и несимметричной:
А) ДА
Б) НЕТ

7) Хэш-функция – это криптографическое преобразование информации, переводящее строку битов произвольной длины в строку битов фиксированной длины:
А) ДА
Б) НЕТ

8) В электронном документообороте наилучшим способом контроля целостности данных является:

А) шифрование

Б) электронная цифровая подпись

В) хэширование

9) Увеличение длины ЭЦП в 2 раза по сравнению с хэш-образом это свойство ЭЦП:

А) ДА

Б) НЕТ

10) Размер ЭЦП по российскому стандарту (ГОСТ-2012) равен:

А) 256 бит 512 бит

Б) 512 бит или 1024 бит

В) 1024 бит

Г) 320 бит

11) При шифровании данных несимметричной криптосистемой, используется:

А) секретный ключ

Б) открытый ключ

В) сначала открытый, а затем секретный ключ

Г) сначала секретный, а затем открытый ключ

12) При создании ЭЦП секретный ключ по длине больше, чем открытый:

А) ДА

Б) НЕТ

13) Размер хэш-образа по американскому стандарту SHA-1 равен:

А) 256 бит

Б) 512 бит

В) 160 бит

Г) 320 бит

Тестовые задания к разделу 5

14) В современном протоколе шифрования данных при шифровании сообщений используется двухключевая криптосистема:

А) ДА

Б) НЕТ

15) Размер ЭЦП по американскому стандарту DSS равен:

А) 256 бит

Б) 512 бит
В) 1024 бит
Г) 320 бит

16) В электронном документообороте наилучшим способом обеспечения конфиденциальности данных является:
А) шифрование
Б) электронная цифровая подпись
В) хэширование

17) Укажите одностороннюю функцию для алгоритма Эль-Гамаля:
А) $(e \cdot d) \bmod k = 1;\ k = p \cdot (q-1)$;
Б) $y = a^x \bmod p$;
В) $n = p \cdot q$;
Г) $c = m^e \bmod (n-1)$;

18) Выберите наиболее эффективную криптосистему для шифрования незначительных по объему данных:
А) RSA
Б) AES
В) DES
Г) ГОСТ 28147-89

19) Двухключевую криптосистему называют криптосистемой с открытым ключом, т.к. при шифровании открытый ключ создает отправитель, а секретный – получатель:
А) ДА
Б) НЕТ

20) Пару ключей при шифровании данных криптосистемой с открытым ключом создает отправитель:
А) ДА
Б) НЕТ

21) Владельцем пары ключей при создании ЭЦП является отправитель:
А) ДА
Б) НЕТ

22) Хэширование сообщения при создании ЭЦП осуществляется, чтобы:
А) обеспечить конфиденциальность информации
Б) увеличить время создания ЭЦП
В) стандартизовать время создания ЭЦП и ее размер

23) Хэш-функция может применяться в следующих случаях:

А) для создания сжатого образа сообщения, используемого в механизме цифровой подписи;

Б) для защиты пароля;

В) при контроле целостности данных;

Г) для сохранения конфиденциальности информации.

24) Коллизия в хэш-функции, это когда разные сообщения имеют одинаковый хэш-образ:

А) ДА

Б) НЕТ

25) В современном протоколе шифрования данных для шифрования секретного ключа симмеричной криптосистемы используется двухключевая криптосистема:

А) ДА

Б) НЕТ

26) Двухключевая криптосистема может применяться в следующих случаях:

А) для шифрования небольших по объему данных;

Б) при создании электронно-цифровой подписи;

В) в задачах аутентификации;

Г) для обеспечения доступности информации.

3.2 Перечень вопросов к экзамену по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем»

1. Информационная безопасность и безопасность информации.
2. Понятия приоритета, охраны и защиты интеллектуальной собственности.
3. Аспекты безопасности информации.
4. Основные виды угроз.
5. Правовое обеспечение интеллектуальной собственности и информационной безопасности. Содержание конфиденциальной информации, определенной Указом Президента РФ.
6. Особенности обработки персональных данных.
7. Виды ИСПДн, уровни защищенности ПДн.
8. Технология и методы контроля целостности информации при случайных воздействиях.
9. Характеристика ФЗ об электронной подписи, виды ЭП.
10. Основные понятия криптографии.
11. Поточное шифрование сообщений.
12. Характеристика блочных симметричных криптосистем.
13. Алгоритм DES и его развитие.
14. Стандарт криптографической защиты AES.
15. Российский алгоритм криптографического преобразования: режимы шифрования.
16. Российский алгоритм криптографического преобразования: режим имитовставки.

17. Несимметричные системы шифрования. Современный протокол шифрования данных.
18. Алгоритм RSA. Сравнение симметричных и несимметричных криптосистем.
19. Определение и назначение хэш-функции, российский стандарт.
20. Электронная подпись: определения, назначение, роль в электронном документообороте.
21. Российский стандарт ЭП: технология создания и проверки.
22. Обмен Диффи-Хеллмана. Назначение мастер-ключа.
23. Биометрическая аутентификация пользователя.
24. Цели, структура и функции системы защиты информации.
25. Инфраструктура управления открытыми ключами.

4 Методические материалы, определяющие процедуру оценивания формирования компетенций

В таблице дано описание процедур проведения контрольно-оценочных мероприятий, соответствующих рабочей программе дисциплины, и процедур оценивания результатов обучения с помощью спланированных оценочных средств.

<table>
<tr><th>Наименование оценочного средства</th><th>Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения</th></tr>
<tr><td>Отчет по лабораторной работе</td><td>Преподаватель непосредственно перед началом проведения лабораторной работы выдает каждому обучающемуся исходные данные для проведения лабораторной работы. После проведения лабораторной работы необходимо составить отчет. Отчет должна быть выполнен в установленный преподавателем срок и в соответствии с требованиями к оформлению отчета (текстовой и графической частей), сформулированными в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции. Отчеты в назначенный срок сдаются на проверку. Если предусмотрена устная защита отчета лабораторной работы, то обучающийся объясняет решение задач, указанных преподавателем и отвечает на его вопросы</td></tr>
<tr><td>Конспект</td><td>Преподаватель не мене, чем за неделю до срока выполнения конспекта должен довести до сведения обучающихся тему конспекта и указать необходимую учебную литературу. Перечень необходимой учебной литературы выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет. Конспект должен быть выполнены в установленный преподавателем срок. Конспекты в назначенный срок сдаются на проверку</td></tr>
<tr><td>Зачет</td><td>Проведение промежуточной аттестации в форме зачета позволяет сформировать среднюю оценку по дисциплине по результатам текущего контроля. Так как оценочные средства, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. Для чего преподаватель находит среднюю оценку уровня сформированности компетенций у обучающегося, как сумму всех полученных оценок, деленную на число этих оценок.

Шкала и критерии оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля
<table>
<tr><th>Средняя оценка уровня</th><th>Оценка</th></tr>
</table>
</td></tr>
</table>

	сформированности компетенций по результатам текущего контроля	
	Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
	Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»
	Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета, то обучающийся сдает зачет. Зачет проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач (не более двух теоретических и двух практических). Перечень теоретических вопросов и перечень типовых практических заданий разного уровня сложности обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося). Обучающиеся, не защитившие в течение семестра отчеты по лабораторным работам, предусмотренную рабочей программой дисциплины, должны, прежде чем взять билет, защитить отчет.	

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 положением о формировании фонда оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.250000.06.7.188-2015 (формы оформления оценочных средств приведены ниже), не выставляются в электронную информационно-образовательную среду ИрГУПС, а хранятся на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.