ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «7» июня 2021 г. № 78

Б1.О.43 Криптографические протоколы и стандарты
рабочая программа дисциплины

Специальность – *10.05.03 Информационная безопасность автоматизированных систем*
Квалификация выпускника –Специалист по защите информации
Форма и срок обучения – 5л 6м очная форма
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 8.

Распределение часов дисциплины по семестрам

Семестр	8	**Итого**
Число недель в семестре	17	
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в форме ПП*	**85**	**85**
– лекции	34	**34**
– практические (семинарские)	17	**17**
– лабораторные	34	**34**
Самостоятельная работа	**59**	**59**
Экзамен		
Итого	**144**	**144**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности), утверждённым приказом Минобрнауки России от 17.11.2020 г. № 1427.

Программу составил(и):
Ассистент _____ *А.С.Вергасов*

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «*ИСиЗИ*», протокол от «4» июня 2021 г №11/2

Зав. кафедрой*, канд. экон.наук* _____ *Т.К.Кириллова*

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цели дисциплины	
1	формирование представления о криптографических протоколах и стандартах
1.2 Задачи дисциплины	
1	ознакомление с основными понятиями в области криптографических протоколов и стандартов;
2	формирование глубоких и всесторонних знаний по используемым криптографическим протоколам и стандартам;
3	формирование навыков применения полученных знаний для решения практических задач по применению криптографических протоколов и стандартов.
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Цель воспитания обучающихся – разностороннее развитие личности будущего конкурентоспособного специалиста с высшим образованием, обладающего высокой культурой, интеллигентностью, социальной активностью, качествами гражданина-патриота. Задачи воспитательной работы с обучающимися: – развитие мировоззрения и актуализация системы базовых ценностей личности; – приобщение студенчества к общечеловеческим нормам морали, национальным устоям и академическим традициям; – воспитание уважения к закону, нормам коллективной жизни, развитие гражданской и социальной ответственности как важнейшей черты личности, проявляющейся в заботе о своей стране, сохранении человеческой цивилизации; – воспитание положительного отношения к труду, развитие потребности к творческому труду, воспитание социально значимой целеустремленности и ответственности в деловых отношениях; – обеспечение развития личности и ее социально-психологической поддержки, формирование личностных качеств, необходимых для эффективной профессиональной деятельности; – выявление и поддержка талантливых обучающихся, формирование организаторских навыков, творческого потенциала, вовлечение обучающихся в процессы саморазвития и самореализации;	

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
Б1.О.54 Методы и средства криптографической защиты информации	
Б1.О.37 Защита информации от утечки по техническим каналам	
Б1.О.35 Организация ЭВМ и вычислительных систем	
Б1.О.28 Технологии и методы программирования	
Б1.О.26 Языки программирования	
Б1.О.10 Математическая логика и теория алгоритмов	
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.50 Комплексная защита в информационных системах персональных данных
2	Б1.О.59 Проектирования систем защиты объектов информатизации
3	Б1.О.60 Защита информации от несанкционированного доступа
4	Б2.В.05(Пд) Производственная - преддипломная
5	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения**

ОПК.10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК.10-1 Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности ОПК.10-2 Умеет применять доверенное хранение, защиту каналов связи и электронного документооборота ОПК.10-3 Имеет навыки работы с алгоритмами криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и для защиты информации от несанкционированного доступа при ее обработке и хранении.	**Знать:** – современные подходы к организации сложных криптосистем; – основные международные стандарты, регламентирующие применение криптографических методов защиты информации, а также нормативно-технические документы, регламентирующие проектирование, разработку и применение средств криптографической защиты информации (СКЗИ) в РФ; – принципы анализа стойкости криптографических протоколов; –принципы выявления уязвимостей СКЗИ. **Уметь:** – анализировать текущее состояние ИБ на предприятии с целью разработки требований к СКЗИ; – грамотно выбирать и корректно реализовывать криптографические методы защиты информации при создании средств и систем комплексной защиты информации; – применять формальные методы анализа криптографических протоколов; оценивать сложность реализации криптографических протоколов. **Владеть:** – навыками решения задач количественной оценки стойкости и производительности криптографических протоколов; – навыками разработки элементов технических заданий на создание СКЗИ.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работы	Семестр	Часы				*Код индикатора достижения компетенции
			Лек	Пр	Лаб	СР	
	Раздел 1. Криптографические протоколы и сервисы идентификации и аутентификации абонентов и объектов сети		**16**			**25**	
1.1	Введение. Определения, цели, задачи дисциплины. Основные термины и определения /Лек/	9	4				ОПК.10-1 ОПК.10-2 ОПК.10-3
1.2	Аутенфикация на основе паролей /Лек/	9	4				ОПК.10-1 ОПК.10-2 ОПК.10-3
1.3	Аутентификация Kerberos/Лек/	9	4				ОПК.10-1 ОПК.10-2 ОПК.10-3
1.4	Изучение механизмов аутенфикации, использующих криптографические протоколы /Ср/	9				15	ОПК.10-1 ОПК.10-2 ОПК.10-3
1.5	Программная реализация алгоритма DES /Лр/	9			2		ОПК.10-1 ОПК.10-2 ОПК.10-3
1.6	Механизмы одноразовой аутенфикации /См/	9				6	ОПК.10-1 ОПК.10-2 ОПК.10-3
1.7	Подготовка к текущему контролю (защита лабораторной работы)/Ср/	9				4	ОПК.10-1 ОПК.10-2 ОПК.10-3
	Раздел 2. Инфраструктура открытых ключей		**10**			**4**	
2.1	Криптографическая система с открытым ключом /Лек/	9	2				ОПК.10-1

							ОПК.10-2 ОПК.10-3
2.2	Программная реализация алгоритма RSA /Лр/	9			8		ОПК.10-1 ОПК.10-2 ОПК.10-3
2.3	Подготовка к текущему контролю (защита лабораторной работы) /Ср/	9				4	ОПК.10-1 ОПК.10-2 ОПК.10-3
2.4	Основные компоненты PKI /Лек/	9	2				ОПК.10-1 ОПК.10-2 ОПК.10-3
2.5	Базовые криптографические механизмы сервисов безопасности PKI /Лек/	9	6				ОПК.10-1 ОПК.10-2 ОПК.10-3
	Раздел 3. Национальные криптографические стандарты		**8**	**17**		**32**	
3.1	Национальные криптографические стандарты /Лек/	9	4				ОПК.10-1 ОПК.10-2 ОПК.10-3
3.2	Нормативная база по использованию ЭП в РФ /Лек/	9	4				ОПК.10-1 ОПК.10-2 ОПК.10-3
3.3	Анализ политик безопасности удостоверяющих центров /Пр/	9		11			ОПК.10-1 ОПК.10-2 ОПК.10-3
3.4	Требования ГОСТ к криптографическим протоколам /Пр/	9		6			ОПК.10-1 ОПК.10-2 ОПК.10-3
3.5	Решения для построения удостоверяющих центров/См/	9				8	ОПК.10-1 ОПК.10-2 ОПК.10-3
3.6	Подготовка к текущему контролю (защита лабораторной работы)/Ср/	9				4	ОПК.10-1 ОПК.10-2 ОПК.10-3
3.7	Подготовка к зачету /Ср/	9				18	ОПК.10-1 ОПК.10-2 ОПК.10-3

* 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 разработан 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 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	Ермакова А. Ю.	Криптографические методы защиты информации : учебно-методическое пособие Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563	Москва : РТУ МИРЭА, 2021.	100 % онлайн
6.1.1.2	Бутакова Н. Г., Федоров Н. В.	Криптографические методы и средства защиты информации: Учебное пособие Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161347	Санкт-Петербург : Интермедия, 2020.	100 % онлайн
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
6.1.2.1	Краковский Ю. М.	Методы защиты информации Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401	Санкт-Петербург : Лань, 2021.	100 % онлайн
6.1.2.2	Каширская Е. Н.	Криптографический анализ и методы защиты информации: Учебное пособие Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163861	Москва : РТУ МИРЭА, 2020.	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	Каширская Е. Н.	Основы криптографического анализа: Учебное пособие Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163805	Москва : РТУ МИРЭА, 2020.	100 % онлайн
6.1.3.2	Фомичев В. М.	Элементы теории информации в защите информации: Учебное пособие для академического бакалавриатаТекст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189744	Москва : Прометей, 2021.	100 % онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»				
6.2.1	pravo.gov.ru			
6.2..2	fsb.ru			
6.3 Программное обеспечение и информационные справочные системы				
6.3.1 Базовое программное обеспечение				
6.3.1.1	ОС Microsoft Windows 7 Professional, лицензия № 49379844, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд Windows Edu Per Device 10 Education, Соглашение № V6760694, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд		
6.3.1.2	Офисный пакет Microsoft Office 2010, Лицензия № 48288083, обновление - контракт №0334100010018000027-0000756-02 от 28.05.2018 АО СофтЛайн Трейд, обновление - контракт № 0334100010019000029-0000756-02 от 17.09.2019г. АО СофтЛайн Трейд, обновление - контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; Office Professional 2019 - Соглашение № V0709762, контракт № 0334100010020000010-0000756-02 от 16.06.2020 АО СофтЛайн Трейд; LibreOffice v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org		
6.3.2 Специализированное программное обеспечение				

6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.
6.3.2.2	Borland Delphi 7
6.3.3 Информационные справочные системы	
6.3.3.1	«Консультант +» http://www.consultant.ru/
6.3.3.2	ЭБС ИрГУПС http://www.irgups.ru/htb/;
6.3.3.3	ЭБС издательства «Лань» http://www.e.lanbook.com;
6.3.3.4	ЭБС «Университетская библиотека онлайн» http://www.biblioclub.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	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
4	Помещение для хранения и профилактического обслуживания учебного оборудования – А-521.
5	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.

Практическая подготовка – форма организации образовательной деятельности при освоении образовательных программ в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по профилю соответствующей образовательной программы. Образовательная деятельность в форме практической подготовки может быть организована при реализации учебных предметов, курсов, дисциплин (модулей), практики, иных компонентов образовательных программ, предусмотренных учебным планом.

Практическая подготовка при реализации учебных предметов, курсов, дисциплин (модулей) организуется путем проведения практических занятий, практикумов, лабораторных работ и иных аналогичных видов учебной деятельности, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью. Практическая подготовка может включать в себя отдельные занятия лекционного типа, которые предусматривают передачу учебной информации обучающимся, необходимой для последующего выполнения работ, связанных с будущей профессиональной деятельностью.

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

Лист регистрации дополнений и изменений рабочей программы дисциплины

№ п/п	Часть текста, подлежавшего изменению в документе			Общее количество страниц		Основание для внесения изменения, № документа	Подпись отв. исп.	Дата
	№ раздела	№ пункта	№ подпункта	до внесения изменений	после внесения изменений			

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине *Б1.О.43 Криптографические протоколы и стандарты*

Приложение № 1 к рабочей программе

Специальность– *10.05.03 Информационная безопасность автоматизированных систем*
Специализация– Специалист по защите информации

ИРКУТСК

1. Общие положения

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

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

Задачами ФОС являются:

– оценка достижений обучающихся в процессе *изучения дисциплины (модуля) или прохождения практики*;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

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

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

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

Дисциплина (модуль)/практика «*Наименование*» участвует в формировании компетенций:

ОПК.10-1 Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности

ОПК.10-2 Умеет применять доверенное хранение, защиту каналов связи и электронного документооборота

ОПК.10-3 Имеет навыки работы с алгоритмами криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и для защиты информации от несанкционированного доступа при ее обработке и хранении.

Программа контрольно-оценочных мероприятий очная форма обучения

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятие/тем/раздел и т.д. дисциплины)	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
8 семестр					
1	4	Текущий контроль	Механизмы одноразовой аутенфикации /См/	ОПК.10-1 ОПК.10-2 ОПК.10-3	Сообщение, доклад
2	8	Текущий контроль	Программная реализация алгоритма DES /Лр/	ОПК.10-1 ОПК.10-2 ОПК.10-3	Защита ЛР (отчет, устный ответ на вопросы)
3	12	Текущий контроль	Программная реализация алгоритма RSA /Лр/	ОПК.10-1 ОПК.10-2 ОПК.10-3	Защита ЛР (отчет, устный ответ на вопросы)
4	17	Промежуточная аттестация – зачет	Разделы 1, 2, 3	ОПК.10-1 ОПК.10-2 ОПК.10-3	Зачет

*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 так же 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. Тестирование проводится два раза за семестр ─ в середине семестра и за две недели до его окончания	Фонд тестовых заданий

Критерии и шкалы оценивания компетенций в результате *изучения дисциплины/ прохождении практики* 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	Компетенция не сформирована

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация Power Point, 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 Power Point, 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

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

Перечень докладов

1. Криптоанализ блочных симметричных алгоритмов.
2. Криптоанализ поточных симметричных шифров.
3. Криптоанализ хэш функций.
4. Исследование безопасности генераторов ПСЧ.
5. Системы аутентификации с нулевым разглашением.
6. Идентификация пользователей по клавиатурному почерку.

7. Криптосистемы на основе эллиптических кривых.
8. Реализация криптосистемы Хилла
9. Исследование методов реализации безопасных постквантовых криптосистем.
10. Стенографические системы.
11. Цифровые водяные знаки и их применение.
12. Генерирование псевдослучайных чисел на основе клеточных автоматов.

Раздел дисциплины	Тема раздела	Объекты темы	Количество тестовых заданий (ТЗ), типы ТЗ
Раздел 1. Криптографические протоколы и сервисы идентификации и аутентификации абонентов и объектов сети	Введение. Определения, цели, задачи дисциплины. Основные термины и определения /Лек/		10 – тип А 10 – тип В
	Аутенфикация на основе паролей /Лек/		10 – тип А
	Аутентификация Kerberos/Лек/		4 – тип А
	Изучение механизмов аутенфикации, использующих криптографические протоколы /Ср/		8 – тип А
	Программная реализация алгоритма DES /Лр/		8– тип А
	Механизмы одноразовой аутенфикации /См/		7– тип А
		Итого по разделу	∑ 57 47– тип А 10 – тип В

Раздел 2. Инфраструктура открытых ключей	Криптографическая система с открытым ключом /Лек/		10 – тип А
	Программная реализация алгоритма RSA /Лр/		3 – тип А
	Основные компоненты PKI /Лек/		9 – тип А
	Базовые криптографические механизмы сервисов безопасности PKI /Лек/		11– тип А
		Итого по разделу	∑ 33 33 – тип А
Раздел 3. Национальные криптографические стандарты	Национальные криптографические стандарты /Лек/		6– тип А
	Нормативная база по использованию ЭП в РФ /Лек/		3 – тип А
	Анализ политик безопасности удостоверяющих центров /Пр/		2 – тип А 2 – тип В
	Требования ГОСТ к криптографическим протоколам /Пр/		4– тип В
	Решения для построения удостоверяющих центров/Ср/		1 – тип В
		Итого по разделу	**∑18** **11 – тип А** **7 – тип В**
		Итого по дисциплине	**∑ 108** **91 – тип А** **17 – тип В**

Типовые тесты

Шифрование – это…

А) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

Б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
В) удобная среда для вычисления конечного пользователя

Кодирование – это…
А) преобразование обычного, понятного текста в код
Б) преобразование
В) написание программы

Что требуется для восстановления зашифрованного текста
А) ключ
Б) матрица
В) вектор

Когда появилось шифрование
А) четыре тысячи лет назад
Б) две тысячи лет назад
В) пять тысяч лет назад

Первым известным применением шифра считается
А) египетский текст
Б) русский
В) нет правильного ответа

Какую секретную информацию хранит Windows
А) пароли для доступа к сетевым ресурсам
Б) пароли для доступа в Интернет
В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

Алфавит – это…
А) конечное множество используемых для кодирования информации знаков
Б) буквы текста
В) нет правильного ответа

Текст – это…
А) упорядоченный набор из элементов алфавита
Б) конечное множество используемых для кодирования информации знаков
В) все правильные

Примеры алфавитов:
А) Z256 – символы, входящие в стандартные коды ASCII и КОИ-8
Б) восьмеричный и шестнадцатеричный алфавиты
В) AEE

Шифрование – это…
А) преобразовательный процесс исходного текста в зашифрованный
Б) упорядоченный набор из элементов алфавита
В) нет правильного ответа

Дешифрование – это…
А) на основе ключа шифрованный текст преобразуется в исходный

Б) пароли для доступа к сетевым ресурсам
В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

Криптографическая система представляет собой…
А) семейство T преобразований открытого текста, члены его семейства индексируются символом k
Б) программу
В) систему

Пространство ключей k – это…

А) набор возможных значений ключа
Б) длина ключа
В) нет правильного ответа

Криптосистемы разделяются на:
А) симметричные
Б) ассиметричные
В) с открытым ключом

Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования
А) 1
Б) 2
В) 3

Сколько ключей используется в системах с открытым ключом
А) 2
Б) 3
В) 1

Какие ключи используются в системах с открытым ключом
А) открытый
Б) закрытый
В) нет правильного ответа

Как связаны ключи друг с другом в системе с открытым ключом
А) математически
Б) логически
В) алгоритмически

Электронной подписью называется…
А) присоединяемое к тексту его криптографическое преобразование
Б) текст
В) зашифрованный текст

Криптостойкость – это…
А) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
Б) свойство гаммы
В) все ответы верны

Показатели криптостойкости:
А) количество всех возможных ключей
Б) среднее время, необходимое для криптоанализа
В) количество символов в ключе

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
А) знание алгоритма шифрования не должно влиять на надежность защиты
Б) структурные элементы алгоритма шифрования должны быть неизменными
В) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
А) длина шифрованного текста должна быть равной лине исходного текста
Б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа
В) нет правильного ответа

Основные современные методы шифрования:
А) алгоритма гаммирования
Б) алгоритмы сложных математических преобразований
В) алгоритм перестановки

Символы исходного текста складываются с символами некой случайной последовательности – это…
А) алгоритм гаммирования
Б) алгоритм перестановки
В) алгоритм аналитических преобразований

Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это…
А) алгоритм перестановки
Б) алгоритм подстановки
В) алгоритм гаммрования

Самой простой разновидность подстановки является
А) простая замена
Б) перестановка
В) простая перестановка

Из скольки последовательностей состоит расшифровка текста по таблице Вижинера
А) 3
Б) 4
В) 5

Какие таблицы Вижинера можно использовать для повышения стойкости шифрования
А) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке
Б) в качестве ключа используется случайность последовательных чисел
В) нет правильного ответа

В чем суть метода перестановки

А) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
Б) замена алфавита
В) все правильные

Сколько существует способов гаммирования
А) 2
Б) 5
В) 3

Чем определяется стойкость шифрования методом гаммирования
А) свойством гаммы
Б) длина ключа
В) нет правильного ответа

Что может использоваться в качестве гаммы
А) любая последовательность случайных символов
Б) число
В) все ответы верны

Какой метод используется при шифровании с помощью аналитических преобразований
А) алгебры матриц
Б) матрица
В) факториал

Что используется в качестве ключа при шифровании с помощью аналитических преобразований
А) матрица А
Б) вектор
В) обратная матрица

Как осуществляется дешифрование текста при аналитических преобразованиях
А) умножение матрицы на вектор
Б) деление матрицы на вектор
В) перемножение матриц

Комбинации комбинированного метода шифрования:
А) подстановка+гаммирование
Б) гаммирование+гаммирование
В) подстановка+перестановка

Для чего использовался DES-алгоритм из-за небольшого размер ключа
А) закрытия коммерческой информации
Б) шифрования секретной информации
В) нет правильного ответа

Основные области применения DES-алгоритма
А) хранение данных на компьютере
Б) электронная система платежей
В) аутентификация сообщений

Когда был введен в действие ГОСТ 28147-89

А) 1990
Б) 1890
В) 1995

Достоинства ГОСТа 28147-89
А) высокая стойкость
Б) цена
В) гибкость

Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма
А) отсутствием начальной перестановки и числом циклов шифрования
Б) длиной ключа
В) методом шифрования

Ключ алгоритма ГОСТ – это…
А) массив, состоящий из 32-мерных векторов
Б) последовательность чисел
В) алфавит

Какой ключ используется в шифре ГОСТ
А) 256-битовый
Б) 246-битовый
В) 356-битовый

Примеры программных шифраторов:
А) PGP
Б)BestCrypt 6.04
В) PTR

Плюсы программных шифраторов:
А) цена
Б) гибкость
В) быстродействие

УКЗД – это…
А) устройство криптографической защиты данных
Б) устройство криптографической заданности данных
В) нет правильного ответа

Блок управления – это…
А) основной модуль шифратора, который «заведует» работой всех остальных
Б) устройство криптографической заданности данных
В) проходной шифратор

Вычислитель – это…
А) набор регистров, сумматоров, блоков подстановки, связанных собой шинами передачи данных
Б) файлы, использующие различные методы кэширования
В) язык описания данных

Блок управления – это…
А) аппаратно реализованная программа, управляющая вычислителем

Б) язык описания данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

Какой шифратор можно использовать для защиты передаваемой в Сеть информации
А) обычный шифратор
Б) проходной шифратор
В) табличный шифратор

Египетский текст дотировался примерно…
А) 1900 г. д. н.э.
Б) 1890 г. д. н.э.
В) 1990 г.

Один из самых известных методов шифрования носит имя…
А) Цезаря
Б) Гейца
В) Вижинера

Из каких структурных единиц состоит шифропроцессор
А) вычислитель
Б) блок управления
В) буфер ввода-вывода

Криптографические действия выполняет…
А) вычислитель
Б) буфер ввода-вывода
В) блок управления

Наиболее известные разновидности полиалфавита:
А) одноконтурные
Б) многоконтурные
В) поликрнтурные

Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск – это…
А) виртуальный контейнер
Б) файл
В) программа

Устройство, дающее статически случайный шум – это…
А) генератор случайных чисел
Б) контроль ввода на компьютер
В) УКЗД

Какие дополнительные порты ввода-вывода содержит УКЗД:
А) COM
Б) USB
В) FGR

Сколько существует перестановок в стандарте DES
А) 3

Б) 4
В) 2

Какие перестановки существуют в стандарте DES
А) простые
Б) расширенные
В) сокращенные

Как называется модификация DESa
А) Triple Des
Б) M-506
В) Deh

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/практики.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Защита лабораторной работы	Преподаватель информирует обучающихся о результатах проверки работы на следующем занятии после проведения контрольно-оценочного мероприятия (или указание другого срока информирования); оцененные/проверенные работы преподаватель возвращает обучающимся. Обучаемый выполняет работу самостоятельно или по указаниям преподавателя, готовит отчет по ЛР, отвечает на вопросы преподавателя. Оценка ставится по результатам защиты ЛР. Если работа связана с разработкой или использованием программно-инструментальных средств, необходимо продемонстрировать владение этим средством и/или полученный с его помощью результат
Сообщение, доклад	Преподаватель информирует обучающихся о результатах проверки работы на следующем занятии после проведения контрольно-оценочного мероприятия (или указание другого срока информирования); оцененные/проверенные работы преподаватель возвращает обучающимся. Обучаемый выполняет работу самостоятельно или по указаниям преподавателя, готовит сообщение, доклад по теме исследования, отвечает на вопросы преподавателя. Оценка ставится по результатам доклада и ответа на дополнительные вопросы.

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/экзамену для оценки знаний;

– перечень типовых простых практических заданий к зачету/экзамену для оценки умений;

– перечень типовых практических заданий к зачету/экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету/экзамену 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. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, 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).

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	*Оценка*
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»*