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.14 Криптографические методы защиты информации

рабочая программа дисциплины

Направление подготовки – 10.03.01 Информационная безопасность
Профиль – "Безопасность автоматизированных систем"
Квалификация выпускника – бакалавр
Форма обучения – очная
Нормативный срок обучения – 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 5
Часов по учебному плану – 180

Формы промежуточной аттестации в семестрах:
экзамен (6), курсовая работа

Распределение часов дисциплины по семестрам

Семестр	6	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**72**	**72**
– лекции	36	36
– практические (семинарские)	18	18
– лабораторные	18	18
Самостоятельная работа	**72**	**72**
Экзамен	**36**	**36**
Итого	**180**	**180**

ИРКУТСК

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	– освоение основополагающих способов защиты информации от угроз раскрытия и нарушения целостности на базе криптографических методов и примеров их практической реализации.
1.2 Задачи освоения дисциплины	
1	– дать основы: математического аппарата, используемого при проектировании шифров и оценке стойкости криптосистем; системного подхода к организации защиты информации, передаваемой, обрабатываемой и хранимой техническими средствами на основе применения криптографических методов; принципов синтеза и анализа криптосистем;
2	– изучить основные характеристики и структуру современных стандартизированных криптосистем.
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Научно-образовательное воспитание обучающихся	
Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества. Цель достигается по мере решения в единстве следующих задач: – формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности; – создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками; – популяризация научных знаний среди обучающихся; – содействие повышению привлекательности науки, поддержка научно-технического творчества; – создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества; – совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности	
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 психологи 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.10 «Дискретная математика»
2	Б1.Б.09 «Теория вероятностей и математическая статистика»
3	Б1.Б.08 «Теория информации»
4	Б1.В.02 «Теоретические основы компьютерной безопасности»
5	Б1.Б.19 «Языки программирования»
6	Б1.Б.20 «Технологии и методы программирования».
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем
2	Б1.В.05 Комплексная защита в информационных системах персональных данных
3	Б1.Б.13 Программно-аппаратные средства защиты информации
5	Б1.В.03 Безопасность вычислительных сетей

7	Б1.В.08 Методология построения защищенных автоматизированных систем
8	Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта
9	Б1.В.ДВ.02.01 Защита и обработка конфиденциальных документов
10	Б1.В.ДВ.02.02 Защита электронного документооборота
11	Б1.В.ДВ.06.01 Информационная безопасность открытых систем
12	Б2.В.03(П) Производственная практика - эксплуатационная
13	Б2.В.04(Пд) Производственная практика - преддипломная

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

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

Минимальный уровень освоения компетенции	
Знать	основные требования к шифрам;
Уметь	оценить необходимость применения средств криптографической защиты информации (СКЗИ);
Владеть	навыками установки СКЗИ;
Базовый уровень освоения компетенции	
Знать	основные характеристики современных криптосистем;
Уметь	формировать предложения по составу подсистемы криптографической защиты информации;
Владеть	навыками администрирования СКЗИ;
Высокий уровень освоения компетенции	
Знать	структуру базовых стандартизированных криптоалгоритмов;
Уметь	оценивать криптостойкость шифров;
Владеть	навыками установки, настройки и обслуживания СКЗИ.

В результате освоения дисциплины обучающийся должен

Знать	
1	основные задачи, этапы развития и понятия криптологии;
2	базовые характеристики и классификацию шифров;
3	модели шифров и математические методы их исследования;
4	принципы построения криптографических алгоритмов.
Уметь	
1	правильно выбирать тип шифра в соответствии с поставленной задачей;
2	программно реализовать алгоритмы криптографических протоколов;
3	программно реализовать алгоритмы шифрования;
4	применить/использовать СКЗИ;
Владеть	
1	терминологией в области криптографической защиты информации;
2	навыками использования типовых криптографических алгоритмов;
3	способами применения СКЗИ.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	Раздел 1. История криптографии. Характер криптографической деятельности. Простейшие шифры и их свойства				
1.1	История развития криптографии. Основные задачи и понятия криптографии. Требования к криптосистемам /Лек/	7	2	ПК-1	Л1.1 Л1.3 Л2.1 Л2.3 Э3
1.2	Исторический обзор. Открытые сообщения и их характеристики /Пр/	7	2	ПК-1	Л1.1 Л1.3 Л2.4

					Э2 Э3
1.3	Программная реализация шифра подстановки (квадрат Полибия) /Лаб/	7	2	ПК-1	Л1.3 Л2.3 Э3
1.4	Программная реализация шифра многоалфавитной замены /Лаб/	7	2	ПК-1	Л1.3 Л2.3 Э3
1.5	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	7	6	ПК-1	Л1.3 Л2.3 Л4.1 Э3
	Раздел 2. Требования к шифрам. Основные классы шифров и их свойства				
2.1	Шифры перестановки. Шифры замены. Поточные шифры.Блочные шифры. Сети Фейстеля /Лек/	7	2	ПК-1	Л1.1 Л1.3 Л2.1 Л2.3 Э3
2.2	Программная реализация шифрования методом постолбцовой транспозиции /Лаб/	7	2	ПК-1	Л1.1 Л1.3 Э3
2.3	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	7	8	ПК-1	Л1.3 Л2.3 Л4.1 Э3
	Раздел 3. Надёжность и криптографическая стойкость шифров. Совершенные шифры				
3.1	Основы теории К.Шеннона. Вопросы имитозащиты. Помехоустойчивость шифров /Лек/	7	2	ПК-1	Л1.2 Л2.4 Э3
3.2	Оценка криптостойкости различных алгоритмов: простых и многомерных подстановок, гаммирования по ключу /Пр/	7	2	ПК-1	Л1.2 Л2.4 Э3
3.4	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	7	8	ПК-1	Л1.2 Л2.4 Э3
	Раздел 4. Методы реализации криптографических алгоритмов с секретным ключом				
4.1	Принципы построения криптографических алгоритмов. Алгоритм DES. Усиления DES. Алгоритм IDEA. Алгоритм AES. Алгоритм ГОСТ 28147-89. Режимы выполнения симметричных криптоалгоритмов. Типовые генераторы псевдослучайных последовательностей. Генераторы на основе линейных регистров сдвига. /Лек/	7	12	ПК-1	Л1.1 Л1.3 Л2.1 Л2.3 Э2 Э3
4.2	Линейка СКЗИ Криптон /Пр/	7	2	ПК-1	Э4
4.3	СКЗИ КриптоАРМ, пакет PGP /Пр/	7	2	ПК-1	Э4
4.4	Программная реализация алгоритма получения псевдослучайной последовательности на основе конгруэнтного оператора /Лаб/	7	2	ПК-1	Л2.3 Л4.1 Э3
4.5	Программная реализация метода XOR - кодирования (схема С.Вернама) /Лаб/	7	2	ПК-1	Л2.3 Э3
4.7	Эксплуатация СКЗИ КриптоАРМ /Лаб/	7	3	ПК-1	Л2.3
4.8	Эксплуатация СКЗИ Криптон-10 /Лаб/	7	5	ПК-1	Э3 Э4
4.9	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	7	14	ПК-1	Л1.1 Л1.3 Л2.1 Л2.3 Э3
	Раздел 5. Методы реализации криптографических алгоритмов с открытым ключом				
5.1	Требования к асимметричным криптосистемам. Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосисте-	7	6	ПК-1	Л1.1 Л1.3 Л2.1 Л2.2 Л2.3 Э3

	ма на основе задачи об “укладке рюкзака”/Лек/				
5.2	Практические аспекты использования криптосистем с открытым ключом /Пр/	7	2	ПК-1	Л1.1 Л1.3 Л2.1 Л2.2 Л2.3 Э3
5.3	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	7	15	ПК-1	Л1.1 Л1.3 Л2.1 Л2.2 Л2.3 Э3
	Раздел 6. Криптоанализ шифров				
6.1	Подходы к анализу криптографических алгоритмов. Метод перебора. Частотный анализ. Корреляционный метод анализа поточных шифров. Линейный и дифференциальный методы анализа блочных шифров /Лек/	7	2	ПК-1	Л1.1 - Л1.3 Л2.3 - Л2.5 Л4.1 Э3
6.2	Частотный анализ шифров. Корреляционный метод анализа поточных шифров /Пр/	7	2	ПК-1	Л1.1 - Л1.3 Л2.3 - Л2.5 Л4.1 Э3
6.3	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	7	8	ПК-1	Л1.1 Л1.3 Л2.1 Л2.2 Л2.3 Э3
	Раздел 7. Хеш-функции и их криптографические приложения				
7.1	Целостность данных и аутентификация источника данных. Общие сведения о хеш-функциях. Требования к хэш-функциям. Понятие о стойкости хеш-функции. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Сильные хэш-функции: MD5, SHA и ГОСТ 3411 /Лек/	7	6	ПК-1	Л1.1 Л1.3 Л2.1 Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
7.2	Проработка лекционного материала /Ср/	7	5	ПК-1	Л1.1 Л1.3 Л2.1 Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
	Раздел 8. Электронная подпись. Инфраструктура PKI				
8.1	Общие положения. Задачи и назначения электронной подписи. Основные требования, прямая и арбитражная цифровая подпись. Классификация электронных подписей. Примеры цифровых подписей на основе алгоритмов RSA, Эль-Гамаля. Стандарты подписи ГОСТ 3410 и DSS. Инфраструктура открытых ключей /Лек/	7	4	ПК-1	Л1.1 Л1.3 Л2.1 Л2.2 Л2.3 Э2 Э3 Э4
8.2	Конструкции MAC на основе симметричного шифрования /Пр/	7	2	ПК-1	Л1.3 Л2.1 Л2.3 Э3
8.3	Схемы цифровых подписей на основе традиционных криптографических систем. Схемы цифровых подписей на основе криптосистем с открытым ключом /Пр/	7	2	ПК-1	Л1.3 Л2.1 Л2.3 Э3
8.4	Протоколы аутентификации Эль Гамаля, RSA, Диффи-Хэллмана, с использованием временных меток /Пр/	7	2	ПК-1	Л1.3 Л1.3 Л2.1 Л2.3 Э3
8.5	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	7	8	ПК-1	Л1.3 Л1.3 Л2.1 Л2.3 Э3
	Раздел 9 Аттестация				
9.1	Подготовка к экзамену /Экзамен/	7	36	ПК-1	Л1.1- Л1.3 Л2.1-Л2.5 Л4.1 Э1-Э4

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 дисциплиныи 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	Рябко Б.А., Фионов А.Н.	Основы современной криптографии и стеганографии; http://e.lanbook.com/view/book/63244/page2/	М.: Горячая линия- Телеком, 2013	100 % онлайн
Л1.2	Гатченко Н.А., Исаев А.С., Яковлев А.Д	Криптографическая защита информации; http://e.lanbook.com/books/element.php?pl1_id=40849: Учебное пособие	СПб: НИУ ИТМО, 2012	100 % онлайн
Л1.3	Лапонина О. Р.	Криптографические основы безопасности: Учебная литература для ВУЗов	М.: Национальный Открытый Университет «ИНТУИТ», 2016	100 % онлайн

6.1.2 Дополнительная литература

				Кол-во экз. в библиотеке/100% онлайн
Л2.1	Глухов М.М. и другие	Введение в теоретико-числовые методы криптографии; http://e.lanbook.com/view/book/68466/page279/: Учебники для вузов. Специальная литература	СПб.: Издательство "Лань", 2011	100 % онлайн
Л2.2	Краковский Ю.М.	Информационная безопасность и защита информации: Учеб. пособие	М.: МарТ, 2008	20
Л2.3	Полянская О. Ю. , Горбатов В. С.	Инфраструктуры открытых ключей; http://biblioclub.ru/index.php?page=book_red&id=233206: Учебное пособие	М.: Интернет-Университет Информационных Технологий, 2007	100 % онлайн
Л2.4		Средства защиты информации на железнодорожном транспорте (криптографические методы и средства): Учебное пособие	УМЦ ЖДТ (Учебно-методический центр по образованию на железнодорожном транспорте), 2006	100
Л2.5	Шубович Е.Г., Капитанчук В.В., Знаенко Н.С., Титаренко Ю.И.	Разработка моделей криптографической защиты информации : Монография	Ульяновск : УлГПУ, 2016	100

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	Завгородний В.И.	«Комплексная защита информации в компьютерных системах»; http://www.proklondike.com/books/defence/zavgorodniy_complex_defence.html; http://bezopasnik.org/article/book/zavgorodniy_-_Complex_Defend.pdf		100% онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»		
Э1	Сайт ФСБ РФ	http://www.fsb.ru/
Э2	Сайт производителя ruToken	http://www.rutoken.ru/
Э3	Форум "Криптография"	http://www.cyberforum.ru/cryptography/
Э4	Сайт производителя линейки "Криптон"	http://ancud.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	ОС Microsoft Windows 7;
6.3.1.3	Офисный пакет Microsoft Office 2010, OpenLicense; количество – 155;
6.3.1.4	BorlandDelphi 7
6.3.2 Перечень специализированных средств и программного обеспечения	
6.3.2.1	СКЗИ КриптоАрм (демо-версия);
6.3.2.2	СКЗИ Криптон-10;
6.3.2.3	Криптопакет PGP (Pretty Good Privacy) (свободная версия ПО).
6.3.3 Перечень информационных справочных систем	
6.3.3.1	Информационно-справочная система КонсультантПлюс http://www.consultant.ru

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

1	Учебные аудитории для проведения занятий лекционного типа, 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.
2	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечена доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: MicrosoftOffice 2010, OpenOffice 3.0.1, 7-zip, BorlandDelphi 7, AbodeReaderXI, MicrosoftSecurityEssentials, а также специализированное ПО.
3	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО 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 лабораторной работе.
Практические (семинарские) занятия	Обобщение, расширение и углубление пройденного материала на лекции. 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. Контроль качества усвоения пройденного материала.
Лабораторная работа	Один из видов практической работы, проводимой с целью углубления и закрепления теоретических знаний, развития навыков самостоятельной деятельности. Включает подготовку необходимых программно-аппаратных средств, составление плана работы, ее проведение и написание отчета.
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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1 Перечень компетенций, в формировании которых участвует дисциплина.

Программа контрольно-оценочных мероприятий. Показатели оценивания компетенций, критерии оценки

Дисциплина «Методы и средства криптографической защиты информации» участвует в формировании компетенций:

ПК-1. способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
6 семестр				
1.0	**Раздел 1. Криптографические методы защиты информации на основе симметричных криптосистем**			
1.1	Текущий контроль	Тема 1. Основные понятия криптографии. Поточное шифрование.	ПК-1	Собеседование (устно)
1.2	Текущий контроль	Лабораторная работа № 1. «Контроль целостности информации при случайных воздействиях».	ПК-1	Лабораторная работа (письменно/устно)
1.3	Текущий контроль	Тема 2. Блочные симметричные криптосистемы. Российский алгоритм криптографического преобразования, ГОСТ 34.13-2018.	ПК-1	Собеседование (устно)
1.4	Текущий контроль	Лабораторная работа № 2. «Поточное шифрование».	ПК-1	Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Криптографические методы защиты информации на основе двухключевых криптосистем**			
2.1	Текущий контроль	Тема 3. Определение двухключевых криптосистем. Обмен Диффи-Хеллмана.	ПК-1	Собеседование (устно)
2.2	Текущий контроль	Лабораторная работа № 3. «Обмен Диффи-Хеллмана».	ПК-1	Лабораторная работа (письменно/устно)
2.3	Текущий контроль	Тема 4. Двухключевые криптосистемы шифрования. Современные технологии шифрования.	ПК-1	Тестирование (компьютерные технологии)
2.4	Текущий контроль	Лабораторная работа № 4. «Шифрование сообщений криптосистемой RSA».	ПК-1	Лабораторная работа (письменно/устно)
3.0	**Раздел 3. Криптографические методы защиты электронного документооборота**			
3.1	Текущий контроль	Тема 5. Хеш-функция. Правовое обеспечение электронной подписи.	ПК-1	Собеседование (устно)
3.2	Текущий контроль	Тема 6. Российские стандарты электронной подписи. . Инфраструктура управления открытыми ключами. Технологии и методы аутентификации.	ПК-1	Собеседование (устно)
3.3	Текущий контроль	Лабораторная работа № 5. «Технология электронной под-	ПК-1	Лабораторная работа (письменно/устно)

		писи».		
3.4	Текущий контроль	Тема 7. Характеристика криптографических методов защиты в КриптоПро CSP. Характеристика зарубежных криптосистем.	ПК-1	Собеседование (устно)
3.5	Текущий контроль	Лабораторная работа № 6. «Взаимная аутентификация субъектов на основе ЭП».	ПК-1	Лабораторная работа (письменно/устно)
	Промежуточная аттестация	Все разделы	ПК-1	Курсовая работа (письменно) Курсовая работа (устно)
	Промежуточная аттестация	Все разделы	ПК-1	Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

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

2 Описание показателей и критериев оценивания компетенций. Описание шкал оценивания

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

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Собеседование	Средство контроля на практическом занятии, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п. Может быть использовано для оценки знаний обучающихся	Вопросы для собеседования по темам/разделам дисциплины
2	Тестирование (компьютерные технологии)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
3	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабо-	Образец задания для выполнения лабораторной работы и при-

		раторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	мерный перечень вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (образец экзаменационного билета) к экзамену
2	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
3	Курсовая работа	Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме экзамена. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	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»	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

Тест – промежуточная аттестация в форме экзамена

Критерии оценивания	Шкала оценивания
Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования	«отлично»
Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования	«хорошо»
Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования	«удовлетворительно»
Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования	«неудовлетворительно»

Курсовая работа

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсовой работы в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся демонстрирует слабое понимание программного материала. Курсовая работа не представлена преподавателю. Обучающийся не явился на защиту курсовой работы

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Собеседование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Глубокое и прочное усвоение программного материала. Полные, последовательные, грамотные и логически излагаемые ответы при видоизменении задания. Обучающийся свободно справляется с поставленными задачами, может обосновать принятые решения, демонстрирует владение разносторонними навыками и приемами выполнения практических работ
«хорошо»		Знание программного материала, грамотное изложение, без существенных неточностей в ответе на вопрос, правильное применение теоретических знаний, владение необходимыми навыками при выполнении практических задач
«удовлетворительно»		Обучающийся демонстрирует усвоение основного материала, при ответе допускаются неточности, при ответе недостаточно правильные формулировки, нарушение последовательности в изложении программного материала, затруднения в выполнении практических заданий Слабое знание программного материала, при ответе возникают ошибки, затруднения при выполнении практических работ
«неудовлетворительно»	«не зачтено»	Не было попытки выполнить задание

Тестирование

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Обучающийся верно ответил на 90 – 100 % тестовых заданий при прохождении тестирования
«хорошо»		Обучающийся верно ответил на 80 – 89 % тестовых заданий при прохождении тестирования
«удовлетворительно»		Обучающийся верно ответил на 70 – 79 % тестовых заданий при прохождении тестирования
«неудовлетворительно»	«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Лабораторная работа

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	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»	«не зачтено»	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

3.1 Типовые контрольные задания для проведения собеседования

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведены образцы типовых вариантов заданий для проведения собеседований.

Образец типового варианта вопросов для проведения собеседования
«Тема 1. Основные понятия криптографии. Поточное шифрование.»

1. Основные понятия криптографии.
2. Классификация криптосистем.
3. Способы формирования ключей для поточного шифрования.
4. Что такое отводная последовательность.
5. Как работает РСЛОС.

Образец типового варианта вопросов для проведения собеседования
«Тема 2. Блочные симметричные криптосистемы. Российский алгоритм криптографического преобразования, ГОСТ 34.13-2018.»

1. Общая схема симметричного шифрования.
2. В чем отличие шифрования от дешифрования.
3. Дать характеристику режимов шифрования российского алгоритма по ГОСТ-89.
4. Дать характеристику режимов шифрования российского алгоритма по ГОСТ-34.13-2018.
5. Назначение и технология работы режима имитовставки.

Образец типового варианта вопросов для проведения собеседования
«Тема 3. Определение двухключевых криптосистем. Обмен Диффи-Хеллмана.»

1. Что такое двухключевая криптосистема.
2. Как осуществляется шифрование на основе двухключевой криптосистемы.
3. Назначение обмена Диффи-Хеллмана.
4. Что такое односторонняя функция. Примеры односторонней функции.

Образец типового варианта вопросов для проведения собеседования
«Тема 5. Хеш-функция. Правовое обеспечение электронной подписи.»

1. Что такое хэш-функция.
2. Технология работы хэш-функции.
3. Дать характеристику ФЗ «Об электронной подписи».
4. В чем отличие простой ЭП от усиленной ЭП.

Образец типового варианта вопросов для проведения собеседования

«Тема 6. Российские стандарты электронной подписи. Инфраструктура управления открытыми ключами. Технологии и методы аутентификации.»

1. Перечислите российские стандарты электронной подписи. В чем их сходство и отличия.
2. Почему в технологии ЭП используется хэш-функция.
3. Что такое технология PKI.
4. Что осуществляет процедура аутентификации.
5. Что такое взаимная аутентификация.

Образец типового варианта вопросов для проведения собеседования

«Тема 7. Характеристика криптографических методов защиты в КриптоПро CSP. Характеристика зарубежных криптосистем.»

1. Дать общую характеристику КриптоПро CSP.
2. Какие разновидности ключей используются в КриптоПро CSP.
3. Дать характеристику криптосистемы DES.
4. Дать характеристику криптосистемы AES.

3.2 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД/РПП	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ПК-1	Тема 1. Основные понятия криптографии. Поточное шифрование.	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-1	Лабораторная работа № 1. «Контроль целостности информации при случайных воздействиях».	Знание	6 – ОТЗ 6 – ЗТЗ
ПК-1	Тема 2. Блочные симметричные криптосистемы. Российский алгоритм криптографического преобразования, ГОСТ 34.13-2018.	Знание	6 – ОТЗ 6 – ЗТЗ
ПК-1	Лабораторная работа № 2. «Поточное шифрование».	Умение	4 – ОТЗ 4 – ЗТЗ
ПК-1	Тема 3. Определение двухключевых криптосистем. Обмен Диффи-Хеллмана.	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-1	Лабораторная работа № 3. «Обмен Диффи-Хеллмана».	Навыки	3 – ОТЗ 3 – ЗТЗ
ПК-1	Тема 4. Двухключевые криптосистемы шифрования. Современные технологии шифрования.	Знание	3 – ОТЗ 3 – ЗТЗ
		Умение	3 – ОТЗ 3 – ЗТЗ
ПК-1	Лабораторная работа № 4. «Шифрование сообщений криптосистемой RSA».	Навыки	3 – ОТЗ 3 – ЗТЗ
ПК-1	Тема 5. Хеш-функция. Правовое обеспечение электронной подписи.	Знание	3 – ОТЗ 3 – ЗТЗ
ПК-1	Тема 6. Российские стандарты электронной подписи. . Инфраструктура управления открытыми ключами. Технологии и методы аутентификации.	Знание	4 – ОТЗ 4 – ЗТЗ
ПК-1	Лабораторная работа № 5. «Технология электронной подписи».	Навыки	4 – ОТЗ 4 – ЗТЗ
ПК-1	Тема 7. Характеристика криптографических методов защиты в КриптоПро CSP. Характеристика зарубежных криптосистем.	Умение	4 – ОТЗ 4 – ЗТЗ
ПК-1	Лабораторная работа № 6. «Взаимная аутентификация субъектов на основе ЭП».	Умение	4 – ОТЗ 4 – ЗТЗ

	Итого	55 – ОТЗ 55 – ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

Раздел 1. Криптографические методы защиты информации на основе симметричных криптосистем

1. В ФЗ № 149 информация это _____
   Ответ: Сведения (сообщение, данные) независимо от формы их представления.

2. Целостность это ____

   Ответ: Неискаженность передаваемой, хранимой или обрабатываемой информации.

3. Асимметричная криптосистема использует ___ ключа.
   Ответ: Два

4. Укажите симметричную криптосистему:
   А) **DES**
   Б) RSA
   В) AES
   Г) **ГОСТ 28147-89**

5. Первый стандарт шифрования данных США имеет наименование:
   А) AES
   Б) IDEA
   В) **DES**
   Г) SEAL

6. Размер блока и размер ключа в первом стандарте шифрования данных США имеют следующие значения в битах:
   А) 64 и 64
   Б) 64 и 256
   В) 64 и 48
   Г) **64 и 56**

Раздел 2. Криптографические методы защиты информации на основе двухключевых криптосистем

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

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

9. 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) $\mathbf{n = p \cdot q}$

Г) $c = m^e \bmod (n-1)$

10. При зашифровании данных асимметричной криптосистемой, используется:

А) закрытый ключ

Б) **открытый ключ**

В) сначала открытый, а затем секретный ключ

Г) сначала секретный, а затем открытый ключ

11. При расшифровании данных асимметричной криптосистемой, используется ____ ключ.

Ответ: закрытый

12. При шифровании асимметричной криптосистемой владельцем пары ключей является _____

Ответ: получатель

Раздел 3. Криптографические методы защиты электронного документооборота

13. Размер хэш-кода по российскому стандарту (ГОСТ-94) равен ____

Ответ: 256 бит

14. Размер хэш-образа по российскому стандарту (ГОСТ-2018) равен ____

Ответ: 256 или 512 битов

15. Размер электронной подписи по российскому стандарту (ГОСТ-2018) равен ____

Ответ: 512 или 1024 битов

16. Размер электронной подписи по российскому стандарту (ГОСТ-94) равен ____

Ответ: 512 бит

17. При шифровании данных несимметричной криптосистемой, используется:

А) закрытый ключ

Б) открытый ключ

В) **сначала открытый, а затем закрытый ключ**

Г) сначала секретный, а затем открытый ключ

18. В электронном документообороте наилучшим способом контроля целостности данных является:

А) шифрование

Б) **электронная подпись**

В) хэширование

3.3 Типовые задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 1. «Контроль целостности информации при случайных воздействиях».»

Целью работы является изучение различных методов контроля целостности информации при ее передаче от случайных воздействий.

Метод контрольных сумм

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 КС определяется размерностью данных в файле. Например: 2, 4, 8-байтовое слово. Рассмотрим пример для 2-байтовых слов:

10010100 01100101
10100010 00011101
10000110 00011101
КС 10110000 01100101

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

Метод КС используется в сетевых технологиях, например, в протоколе *TCP* для Интернета. При сетевой передаче сообщение разбивается на пакеты, далее для каждого пакета формируется своя КС. Если КС отправителя и получателя совпадают (1.1), то считается, что целостность пакета не нарушена. Иначе требуется повторная передача этого пакета.

Метод КС является достаточно быстродействующим, но он обнаруживает одиночную ошибку по каждому столбцу пакета. Это является недостатком этого метода.

При создании пакетов число слов в нем выбирают таким образом, чтобы вероятностью более одной ошибки можно было пренебречь (она должна быть маленькой). Пакетная передача позволяет достаточно эффективно передавать сообщения даже по не очень надежным каналам.

С учетом недостатка метода КС его в настоящее время стараются не применять. Чтобы контролировать более одной ошибки используют сложение по модулю 2^n, метод циклического контроля и другие методы. Контрольные значения в этих методах также часто называют контрольными суммами.

Рассмотрим сложение по модулю 2^n.

В этом методе осуществляется обычное сложение, а результатом (КС) являются n младших битов. Как правило n равно длине слова в битах: 16, 32, 256, 512 или другая длина.

Рассмотрим сложение четырех чисел, имеющих 4-х битное представление. Эти числа: 14, 15, 11, 13, сумма этих чисел равна 53. В двоичном представлении это будет: 11 0101.

Проведем сложение по модулю 2^4 в двоичном виде:

1110+1111=1 1101+1011=1 1000+1101=1 0101.

Таким образом, КС=0101.

1. Три аспекта безопасности информации.
2. Что такое конфиденциальность информации.
3. Что такое целостность информации.
4. Что понимается под случайным воздействием на информацию.
5. Опишите технологию контроля информации при случайных воздействиях.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 2. «Поточное шифрование».»

Цель работы – освоить технологию создания ключа для поточного шифрования на основе регистра сдвига с линейной обратной связью.

В современных системах симметричного шифрования информации широкое применение находят системы поточного шифрования.

Необходимо различать процедуру создания поточного ключа и процедуру поточного шифрования (хотя эти процедуры очень связаны и могут выполняться совместно). В связи с этим разделим поточное шифрование на две процедуры:

а) само поточное шифрование;

б) создание ключа для поточного шифрования.

Современные поточные системы при шифровании используют побитное сложение по модулю 2 (операцию *XOR*). Мы ее уже не однократно использовали, например, при контроле целостности информации, когда рассматривали контроль целостности при случайных воздействиях.

Пусть m – исходное электронное сообщение, конфиденциальность которого необходимо обеспечить; c – зашифрованное сообщение, полученное из исходного; K – секретный поточный ключ. Тогда при зашифровании используется следующая операция

$$c_i=m_i(+)K_i, \quad i=1,2,\ldots,I,$$

где m_i – i-й бит исходного сообщения; K_i – i-й бит поточного ключа; c_i – i-й бит зашифрованного сообщения; I – число битов в сообщениях и в ключе; (+) – операция сложения по модулю 2.

При расшифровании используется та же операция

$$m_i=c_i(+)K_i, \quad i=1,2,\ldots,I.$$

Убедимся, что

$$c_i(+)K_i =(m_i(+)K_i)(+)K_i)= m_i(+)(K_i(+)K_i)= m_i.$$

Для поточного шифрования справедливо равенство, которое вытекает из свойства операции сложения по модулю 2

$$K_i=m_i(+)c_i, \quad i=1,2,\ldots,I.$$

Заметим, что в российских национальных стандартах поточное шифрование называют гаммированием, а поточный ключ – гаммой.

1. Способы формирования ключей для поточного шифрования.
2. Какой аспект безопасности обеспечивает шифрование.
3. Что такое отводная последовательность.
4. Как работает РСЛОС.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 3. «Обмен Диффи-Хеллмана».»

Цель работы – ознакомиться с протоколом «Диффи-Хеллмана», как одним из вариантов создания общего секретного ключа при симметричном шифровании.

В двухключевых (несимметричных, асимметричных, с открытым ключом) криптосистемах адресатом, которому необходим закрытый (секретный) ключ, создаются два ключа (e, d), связанные между собой математической зависимостью (он их может также заказать). При этом один ключ генерируется, а другой вычисляется (это обеспечивается за счет математической связи между ключами).

Один ключ (e) объявляется открытым (публичным), а другой (d) – закрытым (приватным или секретным). Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Закрытый ключ сохраняется в тайне и находится у его создателя (владельца). В дальнейшем закрытый ключ будет называться секретным или закрытым в зависимости от ситуации.

Обозначение открытого ключа (e) условно, при использовании эллиптических функций открытый ключ – это точка на эллиптической кривой с двумя координатами (x и y).

Ключи всегда создает (заказывает) тот, кому нужен закрытый ключ, поэтому этот ключ никуда не передается в отличие от секретного ключа симметричной криптосистемы. Это важное преимущество двухключевых криптосистем.

При выполнении этой лабораторной работы проверяются знания по разделу «Криптография – шифрование электронных сообщений». Ниже приведены вопросы для тестирования.

1) Первый стандарт шифрования данных США имеет наименование:

А) AES

Б) IDEA

В) DES

Г) SEAL

2) Размер блока и размер ключа в первом стандарте шифрования данных США имеют следующие значения в битах:

А) 64 и 64

Б) 64 и 256

В) 64 и 48

Г) 64 и 56

3) Режим имитовставки это:

А) Поточный режим шифрования данных

Б) Метод контроля целостности данных средствами симметричной криптосистемы

В) Метод контроля целостности данных средствами несимметричной криптосистемы

Г) Блочный режим шифрования данных

4) Российский алгоритм ГОСТ 28147-89 позволяет:

А) Блочное шифрование данных

Б) Поточное шифрование данных

В) Формировать электронно-цифровую подпись

Г) Осуществлять контроль целостности информации

5) Укажите блочные криптосистемы с длиной блока 64 бита:

А) RSA

Б) AES

В) DES

Г) ГОСТ 28147-89

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 4. «Шифрование сообщений криптосистемой RSA».»

Цель работы – ознакомиться с технологией асимметричного шифрования на примере алгоритма RSA.

В 1976 году произошло важное событие, существенно изменившее приложения прикладной криптографии. Этим событием является статья У. Диффи и М. Хеллмана «Новые направления в криптографии», которая заложила основы двухключевой (асимметричной, несимметричной) криптографии. В этом классе методов криптографии один ключ является открытым (не секретным), а другой закрытым (секретным). Эти ключи связаны математической зависимостью и создаются одновременно: один из ключей генерируется (выбирается), а другой после этого вычисляется.

Закрытый ключ всегда находится у той стороны, кому он нужен (эта сторона и создает пару ключей), поэтому отсутствует проблема передачи секретного ключа. Открытый ключ передается другой стороне по открытому каналу.

Помимо шифрования (обеспечение конфиденциальности информации) этот класс криптоалгоритмов успешно используется:

а) при создании электронно-цифровой подписи (ЭЦП),

б) в задачах аутентификации, как партнеров, так и сообщений,

в) при контроле целостности данных отдельного сообщения или потока сообщений,

г) при доказательстве принадлежности в случае отказа от переданного или принятого сообщения.

Одной из первых асимметричных криптосистем является система *RSA* (1977 год), получившая название по начальным буквам фамилий ее создателей (*Rivest, Shamir, Adleman*).

Односторонняя функция алгоритма *RSA* имеет вид

$$n=p\cdot q,$$

где n – модуль (открытая информация); p и q – большие простые числа (секретная информация).

При выполнении этой лабораторной работы проверяются знания по разделу «Криптография – двухключевые криптосистемы и их применение». Ниже приведены вопросы для тестирования.

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) Размер хэш-кода по российскому стандарту (ГОСТ-94) равен:

А) 256 бит или 512 бит
Б) 256 бит
В) 160 бит
Г) 320 бит

5) Размер ЭЦП по российскому стандарту (ГОСТ-2001) равен:

А) 256 бит 512 бит
Б) 512 бит
В) 1024 бит
Г) 320 бит

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 5. «Технология электронной подписи».»

Целью работы является обучение пользователей компонентам этапов в технологии электронной подписи (ЭП), последовательности этапов, а также функциям ЭП.

Основные компоненты технологии:

- исходное сообщение (mA);
- уведомление (mB);
- ключ электронной подписи (dA или dB), предназначенный для создания ЭП;
- ключ проверки электронной подписи (eA или eB);
- электронная подпись (ZmA или ZmB). В российском стандарте по ГОСТ Р 34.10-2012 ЭП состоит из двух чисел равной длины (r, s), длина ЭП равна 512 или 1024 битов;
- результат хэширования (YmA или YmB), для хэширования используется хэш-функция. В российском стандарте по ГОСТ Р 34.11-2012 длина хэш-образа равна 256 или 512 битов;
- отправитель (A), который либо подписывает исходное сообщение (mA), тем самым создает ЭП ZmA, или проверяет подлинность ЭП получателя ZmB;
- получатель (B), который либо проверяет подлинность ЭП отправителя ZmA, либо подписывает уведомление (mB), тем самым создает ЭП ZmB;
- сертификат, электронный документ, содержащий ключ проверки ЭП и другую служебную информацию;
- удостоверяющий центр (УЦ), который создает ключи (dA, eA и dB, eB), а также сертификаты (SeA, SeB). Затем сертификаты УЦ отправляет пользователям.

Описание работы

При запуске программы высвечивается основное окно, содержащее кнопку «Теория» и 5 кнопок практики с названиями этапов.

Внизу имеется поле с выходными результатами:

Время начала и окончания работы;

Сколько этапов Вы выполнили;

Сколько раз Вы обращались к кнопке «Теория»;

Сколько ошибок Вы допустили.

Вы должны в правильной последовательности пройти все 5 этапов.

1. Назначение электронной подписи.
2. Что такое неотказуемость.
3. Какой ключ используется при создании ЭП.
4. Какой ключ используется при проверки подлинности ЭП.

Образец заданий для выполнения лабораторных работ и примерный перечень вопросов для их защиты

«Лабораторная работа № 6. «Взаимная аутентификация субъектов на основе ЭП».»

Цель работы – Создать программу, моделирующую технологию взаимной аутентификации субъектов на основе электронной подписи, которая использует криптосистему *RSA*. В лабораторной работе реализуется двухэтапная технология международного стандарта *X*.509.

Аутентификация – процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет.

Необходимый уровень аутентификации определяется требованиями безопасности, которые установлены в организации. Общедоступные *Web*-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать строгой аутентификации.

При защите каналов передачи данных должна выполняться *взаимная аутентификация субъектов*, т. е. взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи.

Разновидности протоколов строгой аутентификации

В зависимости от вида криптографических алгоритмов протоколы строгой аутентификации используют:

- симметричные алгоритмы шифрования;
- однонаправленные хэш-функции;
- асимметричные криптосистемы шифрования;
- алгоритмы электронной подписи.

1. Что осуществляет процедура аутентификации.
2. Что такое взаимная аутентификация.
3. Как осуществляется протокол «запрос-ответ».
4. Какие методы можно отнести к протоколам строгой аутентификации.

3.4 Типовое задание для выполнения курсовой работы

Типовые задания выложено в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец задания для выполнения курсовой работы и примерный перечень вопросов для ее защиты.

Образец типового задания для выполнения курсовой работы

Выполните курсовую работу на тему «Характеристика зарубежных хэш-функций».

1. Назначение хэш-функции и ее свойства.
2. На что влияет размер хэш-кода.
3. Какая сейчас рекомендуемая длина хэш-кода.
4. Приведите примеры национальных хэш-функций США.

3.5 Перечень теоретических вопросов к экзамену

(для оценки знаний)

1. Аспекты безопасности информации.
2. Основные понятия криптографии.
3. Классификация криптосистем.
4. Общая схема шифрования.
5. Способы формирования ключей для поточного шифрования.
6. Вопросы по поточному шифрованию.
7. Что такое угроза и уязвимость.
8. Конфиденциальность информации и методы ее защиты.
9. Стандарт шифрования данных DES.
10. Стандарт криптографической защиты AES.
11. Российский алгоритм криптографического преобразования: режимы шифрования.
12. Российский алгоритм криптографического преобразования: режим имитовставки.
13. Блочный шифр «Магма».
14. Блочный шифр «Кузнечик».
15. Режимы работы блочных шифров (ГОСТ-2018).
16. Несимметричные системы шифрования. Современный протокол шифрования данных.
17. Алгоритм RSA. Сравнение симметричных и несимметричных криптосистем.
18. Определение и назначение хэш-функции, российский стандарт.
19. Электронная подпись: определения, назначение, роль в электронном документообороте.
20. Российский стандарт ЭП: технология создания и проверки.
21. Обмен Диффи-Хеллмана. Назначение мастер-ключа.
22. Характеристика КриптоПро CSP.
23. Инфраструктура управления открытыми ключами.
24. Технологии аутентификации.
25. Технологии строгой аутентификации.

3.6 Перечень типовых простых практических заданий к экзамену

(для оценки умений)

1. Размер хэш-кода по российскому стандарту (ГОСТ-2012) равен:

А) 256 бит или 512 бит

Б) 512 бит или 160 бит

В) 160 бит

Г) 320 бит

2. Современный протокол шифрования данных базируется на совместном применении как симметричной криптосистемы так и асимметричной:

А) ДА

Б) НЕТ

3. Хэш-функция – это криптографическое преобразование информации, переводящее строку битов произвольной длины в строку битов фиксированной длины:

А) ДА

Б) НЕТ

4. В электронном документообороте наилучшим способом контроля целостности данных является:

А) шифрование

Б) электронная цифровая подпись

В) хэширование

3.7 Перечень типовых практических заданий к экзамену

(для оценки навыков и (или) опыта деятельности)

1. Выполните операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

14A7(+)2CA8

2. Найдите контрольную сумму, используя операцию сложения по модулю 2^{16} двух слов, заданных в шестнадцатеричной системе счисления:

4A9F I+I 7FE4

3. Найдите контрольную сумму, используя операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

CA9F(+)DCB9

4. Выполните операцию сложения по модулю 2 двух слов, заданных в шестнадцатеричной системе счисления:

C4A7(+)BCA8

5. Найдите контрольную сумму, используя операцию сложения по модулю 2^{16} двух слов, заданных в шестнадцатеричной системе счисления:

DA9F I+I AFE4

6. 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

7. При создании ЭЦП секретный ключ по длине больше, чем открытый:

А) ДА

Б) НЕТ

8. В современном протоколе шифрования данных при шифровании сообщений используется двухключевая криптосистема:

А) ДА

Б) НЕТ

9. Размер ЭЦП по американскому стандарту *DSS* равен:

А) 256 бит

Б) 512 бит

В) 1024 бит

Г) 320 бит

10. В электронном документообороте наилучшим способом обеспечения конфиденциальности данных является:

А) шифрование

Б) электронная цифровая подпись

В) хэширование

11. 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) $c = m^e \bmod (n-1);$

12. Двухключевую криптосистему называют криптосистемой с открытым ключом, т.к. при шифровании открытый ключ создает отправитель, а секретный – получатель:

А) ДА

Б) НЕТ

13. Пару ключей при шифровании данных криптосистемой с открытым ключом создает отправитель:

А) ДА

Б) НЕТ

14. Владельцем пары ключей при создании ЭЦП является отправитель:

А) ДА

Б) НЕТ

15. Хэширование сообщения при создании ЭЦП осуществляется, чтобы:

А) обеспечить конфиденциальность информации

Б) увеличить время создания ЭЦП

В) стандартизовать время создания ЭЦП и ее размер

16. 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.

17. Коллизия в хэш-функции, это когда разные сообщения имеют одинаковый хэш-образ:

А) ДА

Б) НЕТ

18. В современном протоколе шифрования данных для шифрования секретного ключа симмерично криптосистемы используется двухключевая криптосистема:

А) ДА

Б) НЕТ

19. 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.

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

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

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Собеседование	Собеседование, предусмотренное рабочей программой дисциплины, проводится на практическом занятии. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся тему, вопросы для подготовки к собеседованию. Результаты собеседования преподаватель доводит до обучающихся сразу после завершения собеседования
Тестирование (компьютерные технологии)	Тестирование проводится по результатам освоения тем или разделов дисциплины или по окончанию ее изучения во время практических занятий. Во время проведения тестирования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для практических занятий не разрешено. Преподаватель на практическом занятии, предшествующем занятию проведения теста, доводит до обучающихся: темы, количество заданий в тесте, время выполнения. Результаты тестирования видны обучающемуся на компьютере сразу после прохождения теста
Лабораторная работа	Защита лабораторных работ проводится во время лабораторных занятий. Во время проведения защиты лабораторной работы пользоваться учебниками, справочниками, конспектами лекций, тетрадями не разрешено. Преподаватель на лабораторной работе, предшествующей занятию проведения за-

	щиты лабораторной работы, доводит до обучающихся: номер защищаемой лабораторной работы, время на защиту лабораторной работы. Преподаватель информирует обучающихся о результатах защиты лабораторной работы сразу после ее контрольно-оценочного мероприятия
Курсовая работа	Ход выполнения разделов курсовой работы в рамках текущего контроля оценивается преподавателем исходя из объемов выполненных работ в соответствие со шкалами оценивания. Преподаватель информирует обучающихся о результатах оценивания выполнения курсового проекта сразу после контрольно-оценочного мероприятия. В ходе защиты курсовой работы обучающийся делает доклад протяженностью 5 – 7 минут. Преподаватель ставит окончательную оценку за курсовую работу после завершения защиты, учитывая уровень ее защиты

Для организации и проведения промежуточной аттестации 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 и типовые практические задания разного уровня сложности для проведения промежуточной аттестации обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

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

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам или в форме компьютерного тестирования.

При проведении промежуточной аттестации в форме собеседования билеты составляются таким образом, чтобы каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; два практических задания: одно из них для оценки умений (выбирается из перечня типовых простых практических заданий к экзамену); другое практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике фондов оценочных средств.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.

Образец экзаменационного билета

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «Криптографические методы защиты информации»**	Утверждаю: Заведующий кафедрой «ИСиЗИ» ИрГУПС _____

1. Аспекты безопасности информации.
2. Российский алгоритм криптографического преобразования: режим имитовставки.
3. В электронном документообороте наилучшим способом контроля целостности данных является:
   А) шифрование
   Б) электронная цифровая подпись
   В) хэширование
4. Найдите контрольную сумму, используя операцию сложения по модулю 2^{16} двух слов, заданных в шестнадцатеричной системе счисления:

DA9F I+I AFE4