ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.Б.1.23 Криптографические методы защиты информации

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем
Квалификация выпускника – специалист по защите информации
Форма обучения – очная
Нормативный срок обучения – 5 лет
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 6
Часов по учебному плану – 216

Формы промежуточной аттестации в семестрах:
экзамен (7), курсовая работа

Распределение часов дисциплины по семестрам

Семестр	7	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**90**	**90**
– лекции	36	36
– практические (семинарские)	36	36
– лабораторные	18	18
Самостоятельная работа	**90**	**90**
Экзамен	**36**	**36**
Итого	**216**	**216**

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	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологии профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.Б.1.13 Информатика
2	Б1.Б.1.09 «Дискретная математика»
3	Б1.Б.1.10 «Теория вероятностей и математическая статистика»
4	Б1.Б.1.11 «Математическая логика и теория алгоритмов»
5	Б1.Б.1.12 «Теория информации»
6	Б1.В.04 «Теоретические основы компьютерной безопасности»
7	Б1.Б.1.16 «Языки программирования»
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.Б.1.ДС.02 Криптографические протоколы и стандарты
2	Б1.Б.1.ДС.03 Информационная безопасность открытых систем
3	Б1.Б.1.ДС.04 Виртуальные частные сети
5	Б1.Б.1.28 Программно-аппаратные средства обеспечения информационной безопасности
7	Б1.Б.1.29 Разработка и эксплуатация защищенных автоматизированных систем
8	Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта
9	Б1.В.ДВ.04.01 Защита электронного документооборота
10	Б1.В.ДВ.04.02 Защита и обработка конфиденциальных документов
11	Б2.Б.03(П) Производственная - эксплуатационная
12	Б2.Б.05(П) Производственная - технологическая
13	Б2.Б.06(Пд) Производственная - преддипломная

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-14: способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации
Минимальный уровень освоения компетенции

Знать	методики проведения проверки эффективности работы средства криптографической защиты информации (СКЗИ);
Уметь	организовать проверки эффективности работы СКЗИ;
Владеть	навыками тестирования работоспособности СКЗИ;
Базовый уровень освоения компетенции	
Знать	способы устранения нештатных ситуаций в процессе функционирования СКЗИ;
Уметь	проводить проверки эффективности работы СКЗИ;
Владеть	навыками анализа работы СКЗИ и выявления наличия нештатных ситуаций;
Высокий уровень освоения компетенции	
Знать	методики проведения проверки эффективности работы и способы устранения нештатных ситуаций;
Уметь	проводить проверки эффективности работы СКЗИ и устранять нештатные ситуации;
Владеть	навыками тестирования работоспособности СКЗИ и анализа его результатов.

ПК-23: способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
Минимальный уровень освоения компетенции	
Знать	основные требования к шифрам;
Уметь	оценить необходимость применения СКЗИ;
Владеть	навыками программирования простейших шифров;
Базовый уровень освоения компетенции	
Знать	основные классы шифров и свойства их представителей;
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 выбора метода/средства для криптографической защиты информации ограниченного доступа.

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 средства криптографической защиты информации (СКЗИ).
Владеть	
1	терминологией в области криптографической защиты информации;
2	навыками использования типовых криптографических алгоритмов;
3	способами применения криптографических средств.

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-23	Л1.1 Л1.3 Л2.1 Л2.3 Э3

1.2	Исторический обзор. Открытые сообщения и их характеристики /Пр/	7	2	ПК-23	Л1.1 Л1.3 Л2.4 Э2 Э3
1.3	Программная реализация шифра подстановки (квадрат Полибия) /Лаб/	7	2	ПК-23	Л1.3 Л2.3 Э3
1.4	Программная реализация шифра многоалфавитной замены /Лаб/	7	2	ПК-23	Л1.3 Л2.3 Э3
1.5	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	7	10	ПК-23	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-23	Л1.1 Л1.3 Л2.1 Л2.3 Э3
2.2	Программная реализация шифрования методом постолбцовой транспозиции /Лаб/	7	2	ПК-23	Л1.1 Л1.3 Э3
2.3	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	7	8	ПК-23	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-23	Л1.2 Л2.4 Э3
3.2	Оценка криптостойкости различных алгоритмов: простых и многомерных подстановок, гаммирования по ключу /Пр/	7	2	ПК-23	Л1.2 Л2.4 Э3
3.3	Способы увеличения имитостойкости и помехоустойчивости шифров /Пр/	7	2	ПК-23	Л1.2 Л2.4 Э3
3.4	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	7	8	ПК-23	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-14, ПК-23	Л1.1 Л1.3 Л2.1 Л2.3 Э2 Э3
4.2	Алгоритмы с параллельным шифрованием и задержкой. Алгоритмы с «автоключом» /Пр/	7	2	ПК-23	Л1.1 Л1.3 Л2.1 Э3
4.3	Алгоритмы с обратной связью по тексту. Алгоритмы с «бегущим ключом». Шифрование с коммутацией /Пр/	7	2	ПК-23	Л1.1 Л1.3 Л2.1 Л2.3 Э3
4.4	Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел. Алгоритм Берлекемпа-Месси /Пр/	7	2	ПК-23	Л1.1 Л1.3 Л2.1 Л2.3 Э3
4.5	Линейка СКЗИ Криптон /Пр/	7	4	ПК-14	Э4
4.6	СКЗИ КриптоАРМ /Пр/	7	4	ПК-14	Э4
4.7	Программная реализация алгоритма получения псевдослучайной последовательности на основе конгруэнтного оператора /Лаб/	7	2	ПК-23	Л2.3 Л4.1 Э3

4.8	Программная реализация метода XOR - кодирования (схема С.Вернама) /Лаб/	7	2	ПК-14, ПК-23	Л2.3 Э3
4.9	Эксплуатация СКЗИ КриптоАРМ /Лаб/	7	3	ПК-14	Л2.3
4.10	Эксплуатация СКЗИ Криптон-10 /Лаб/	7	5	ПК-14	Э3 Э4
4.11	Проработка лекционного материала, подготовка к семинарским занятиям и лабораторным работам /Ср/	7	23	ПК-14, ПК-23	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. Криптосистема на основе задачи об “укладке рюкзака”/Лек/	7	6	ПК-23	Л1.1 Л1.3 Л2.1 Л2.2 Л2.3 Э3
5.2	Практические аспекты использования криптосистем с открытым ключом /Пр/	7	4	ПК-23	Л1.1 Л1.3 Л2.1 Л2.2 Л2.3 Э3
5.3	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	7	15	ПК-23	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-23	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-23	Л1.1 - Л1.3 Л2.3 - Л2.5 Л4.1 Э3
6.3	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	7	8	ПК-23	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-23	Л1.1 Л1.3 Л2.1 Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
7.2	Конструкции систем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC/Пр/	7	2	ПК-23	Л1.1 Л1.3 Л2.1 Л2.1 Л2.2 Л2.3 Э1 Э2 Э3
7.3	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	7	10	ПК-23	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.	7	4	ПК-23	Л1.1 Л1.3 Л2.1 Л2.2 Л2.3 Э2 Э3 Э4

	Инфраструктура открытых ключей /Лек/				
8.2	Конструкции MAC на основе симметричного шифрования /Пр/	7	2	ПК-23	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	4	ПК-23	Л1.3 Л2.1 Л2.3 Э3
8.4	Протоколы аутентификации Эль Гамаля, RSA, Диффи-Хэллмана, с использованием временных меток /Пр/	7	2	ПК-23	Л1.3 Л1.3 Л2.1 Л2.3 Э3
8.5	Проработка лекционного материала, подготовка к семинарским занятиям /Ср/	7	8	ПК-23	Л1.3 Л1.3 Л2.1 Л2.3 Э3
	Раздел 9 Аттестация				
9.1	Подготовка к экзамену /Экзамен/		36	ПК-14, ПК-23	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 по дисциплине
Б1.Б.1.23 Безопасность операционных систем

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине
Б1.Б.1.23 «Криптографические методы защиты информации»

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

Дисциплина «**Криптографические методы защиты информации**» участвует в формировании компетенций:

ПК-14: способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
ПК-23: способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа.

Таблица траекторий формирования у обучающихся компетенций ПК-14, ПК-23 при освоении образовательной программы

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин/ практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-14	способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Б1.Б.1.25 Техническая защита информации	6	1
		Б1.Б.1.23 Криптографические методы защиты информации	7	2
		Б1.Б.1.28 Программно-аппаратные средства обеспечения информационной безопасности	8, 9	3
		Б2.Б.05(П) Производственная - технологическая	А	4
ПК-23	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Б1.Б.1.19 Безопасность операционных систем	5, 6	1
		Б1.Б.1.23 Криптографические методы защиты информации	7	2
		Б1.В.06 Комплексная защита в информационных системах персональных данных	9	3
		Б2.Б.06(Пд) Производственная - преддипломная	А	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	4

Таблица соответствия уровней освоения компетенций ПК-14, ПК-23 **планируемым результатам обучения**

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-14	способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и	Раздел 4. Методы реализации криптографических алгоритмов с секретным ключом.	Минимальный уровень	Знать методики проведения проверки эффективности работы средства криптографической защиты информации (СКЗИ);
				Уметь организовать проверки эффективности работы СКЗИ;
				Владеть навыками тестирования работоспособности СКЗИ
			Базовый уро-	Знать способы устранения не-

	технических средств защиты информации		вень	штатных ситуаций в процессе функционирования СКЗИ;
				Уметь проводить проверки эффективности работы СКЗИ;
				Владеть навыками анализа работы СКЗИ и выявления наличия нештатных ситуаций.
			Высокий уровень	Знать методики проведения проверки эффективности работы и способы устранения нештатных ситуаций;
				Уметь проводить проверки эффективности работы СКЗИ и устранять нештатные ситуации;
				Владеть навыками тестирования работоспособности СКЗИ и анализа его результатов.
ПК-23	способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Раздел 1. История криптографии. Характер криптографической деятельности. Простейшие шифры и их свойства. Раздел 2. Требования к шифрам. Основные классы шифров и их свойства. Раздел 3. Надёжность и криптографическая стойкость шифров. Совершенные шифры. Раздел 4. Методы реализации криптографических алгоритмов с секретным ключом. Раздел 5. Методы реализации криптографических алгоритмов с открытым ключом. Раздел 6. Криптоанализ шифров. Раздел 7. Хеш-функции и их криптографические приложения. Раздел 8. Электронная подпись. Инфраструктура PKI.	Минимальный уровень	Знать основные требования к шифрам;
				Уметь оценить необходимость применения СКЗИ;
				Владеть навыками программирования простейших шифров.
			Базовый уровень	Знать основные классы шифров и свойства их представителей;
				Уметь формировать предложения по составу подсистемы криптографической защиты информации;
				Владеть навыками администрирования СКЗИ.
			Высокий уровень	Знать структуру базовых стандартизированных криптоалгоритмов;
				Уметь оценивать криптостойкость шифров;
				Владеть навыками выбора метода/средства для криптографической защиты информации ограниченного доступа.

Программа контрольно-оценочных мероприятий

за период изучения дисциплины

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
7 семестр					
1	2	Текущий контроль	Программная реализация шифра подстановки (квадрат Полибия)	ПК-14, ПК-23	Защита лабораторной работы
2	4	Текущий контроль	Программная реализация шифра многоалфавитной замены	ПК-14, ПК-23	Защита лабораторной работы
3	6	Текущий контроль	Программная реализация шифрования методом постолбцовой транспозиции	ПК-14, ПК-23	Защита лабораторной работы
4	8	Текущий контроль	Программная реализация алгоритма получения псевдослучайной последовательности на основе конгруэнтного оператора	ПК-14, ПК-23	Защита лабораторной работы
5	10	Текущий контроль	Программная реализация метода XOR - кодирования (схема С.Вернама)	ПК-14, ПК-23	Защита лабораторной работы
6	14	Текущий контроль	Эксплуатация СКЗИ Крипто-АРМ	ПК-14, ПК-23	Защита лабораторной работы
7	18	Текущий контроль	Эксплуатация СКЗИ Криптон-10	ПК-14, ПК-23	Защита лабораторной работы
8	18	Текущий контроль	Защита курсовой работы	ПК-14, ПК-23	Курсовая работа
9	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ПК-14, ПК-23	Сообщение, доклад (устно); наличие презентации
10	18	Тест	Разделы 1 – 8 РПД	ПК-14, ПК-23	Перечень тестовых заданий
11	18	Промежуточная аттестация – экзамен	Разделы 1 – 8 РПД	ПК-14, ПК-23	Собеседование (устно)

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

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

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания 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 на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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
2	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
3	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
4	Курсовая работа	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. 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	Темы типовых групповых и / или индивидуальных проектов и типовое задание на курсовую работу
5	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к экзамену

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета и экзамена, а также шкала для оценивания уровня освоения компетенций

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенций
«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
	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	Базовый

	владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	
	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
«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригинальность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

Тест (структура теста по компетенциям)

Проверяемый уровень освоения компетенции компетенций (части компетенций, элементов компетенций)	Минимальное количество тестовых заданий на один раздел программы	Рекомендуемые формы тестовых заданий	Количество баллов за одно тестовое задание
Минимальный уровень освоения компетенции	19	Тестовые задания с выбором одного правильного ответа из нескольких	1
		Тестовые задания с выбором нескольких правильных ответов из множества	

		ответов	
		Тестовые задания на установление соответствия	
		Тестовые задания на установление правильной последовательности	
Базовый уровень освоения компетенции	8	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)	4
Высокий уровень освоения компетенции	6	Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы	7

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся при тестировании набрал 86-93 баллов	Высокий
«хорошо»		Обучающийся при тестировании набрал 69-85 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 53-68 баллов	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-52 баллов	Компетенция не сформирована

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. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсового проекта (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. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. 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. Программа не разработана и/или находится в нерабочем состоянии. При защите курсовой работыобучающийся демонстрирует слабое понимание программного материала. Курсовой работы не представлена преподавателю. Обучающийся не явился на защиту курсовой работы.

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,

характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Перечень типовых тем докладов, сообщений

1. Исторический обзор развития криптологии. Открытые сообщения и их характеристики.
2. Оценка криптостойкости различных алгоритмов: простых и многомерных подстановок, гаммирования по ключу.
3. Способы увеличения имитостойкости и помехоустойчивости шифров.
4. Алгоритмы с параллельным шифрованием и задержкой. Алгоритмы с «автоключом».
5. Алгоритмы с обратной связью по тексту. Алгоритмы с «бегущим ключом». Шифрование с коммутацией.
6. Генераторы Фибоначчи.
7. Генераторы, основанные на сложнорешаемых задачах теории чисел.
8. Алгоритм Берлекемпа-Месси.
9. Линейка СКЗИ Криптон.
10. СКЗИ КриптоАРМ.
11. Практические аспекты использования криптосистем с открытым ключом.
12. Частотный анализ шифров.
13. Корреляционный метод анализа поточных шифров.
14. Конструкции систем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC.
15. Конструкции MAC на основе симметричного шифрования.
16. Схемы цифровых подписей на основе традиционных криптографических систем.
17. Схемы цифровых подписей на основе криптосистем с открытым ключом.
18. Протоколы аутентификации Эль Гамаля, RSA, Диффи-Хэллмана, с использованием временных меток.
19. Перспективы развития квантовой криптографии.
20. Программные средства сокрытия информации на базе методов стеганографии.
21. Подходы к оценке надежности шифров. Совершенная секретность по Шеннону.
22. Способы криптоанализа симметричных шифров.
23. Способы криптоанализа шрифтов с открытым ключом.
24. Аппаратные средства шифрования.
25. Генераторы псевдослучайных последовательностей.
26. Назначение и функции центров сертификации ключей (удостоверяющих центров).
27. Технология PGP; уязвимости PGP и OpenPGP.
28. Анализ стойкости блочных криптосистем (ГОСТ 28147-89, ГОСТ Р 34.12-2015, DES, AES).
29. Схемы подписи Рабина, Эль Гамаля, Файге-Фиата-Шамира, Шнорра (2 чел.).
30. Анализ уровня защищенности протоколов TACACS, TACACS+, XTACACS (3 чел.).
31. Правовые основы применения СКЗИ.
32. Оценка криптостойкости алгоритмов BLOWFISH, RC5, IDEA (3 чел.).
33. Организационные основы применения СКЗИ.

3.2. Тест

1. Алгоритм ГОСТ 28147-89 имеет следующие режимы работы (указать все варианты):
   - ○ простой замены;
   - ○ гаммирования;
   - ○ гаммирования по имитовставке.
2. Длина ключа шифрования/расшифрования алгоритма DES составляет:
   - ○ 128 бит;

○ 56 бит;
○ 256 бит.

3. Критерий оценки AES был разделен на следующие основные категории (указать все варианты):
○ Безопасность;
○ Стоимость;
○ Характеристики алгоритма и его реализации.

4. Алгоритм ГОСТ 28147-89 представляет собой
○ модифицированную сеть Фейстеля;
○ классическую сеть Фейстеля;
○ сеть KASLT;
○ сеть URL.

5. Стойкость к атаке «man in the middle» проявил алгоритм
○ двойной DES;
○ тройной DES;

6. Режим выполнения алгоритмов симметричного шифрования CBC рекомендован для
○ безопасной передачи одиночных значений (данных);
○ общей блокоориентированной передачи данных, аутентификации;
○ потокоориентированной передачи данных;
○ потокоориентированной передачи данных по зашумленному каналу.

7. Режим выполнения алгоритмов симметричного шифрования ECB рекомендован для
○ безопасной передачи одиночных значений (данных);
○ общей блокоориентированной передачи данных, аутентификации;
○ потокоориентированной передачи данных;
○ потокоориентированной передачи данных по зашумленному каналу.

8. Режим выполнения алгоритмов симметричного шифрования OFB рекомендован для
○ безопасной передачи одиночных значений (данных);
○ общей блокоориентированной передачи данных, аутентификации;
○ потокоориентированной передачи данных;
○ потокоориентированной передачи данных по зашумленному каналу.

9. Режим выполнения алгоритмов симметричного шифрования CFB рекомендован для
○ безопасной передачи одиночных значений (данных);
○ общей блокоориентированной передачи данных, аутентификации;
○ потокоориентированной передачи данных;
○ потокоориентированной передачи данных по зашумленному каналу.

10. Алгоритм IDEA использует шифрование блока длиной
○ 32 бит;
○ 64 бит;
○ 128 бит.

11. Один из основных элементов алгоритма IDEA, обеспечивающих диффузию, является структура, называемая
○ MA (умножение/сложение);
○ VA (умножение/ сложение);
○ DA (деление/ сложение).

12. Одним из самых сильных генераторов псевдослучайных чисел является алгоритм
○ LSASS 1200;
○ ANSI X9.17;
○ SYS B17.

13. Финалистами конкурса AES являются:
○ Mars;
○ DES;
○ ГОСТ 28147-89;

○ Rijndael;
○ IDEA.

14. Алгоритм ГОСТ 28147-89 имеет следующее количество раундов:
○ 8;
○ 16;
○ 32.

15. Алгоритм ГОСТ 28147-89 имеет следующее количество S-boxes:
○ 4;
○ 8;
○ 16.

16. Алгоритмы шифрования с открытым ключом, в частности, требуют выполнения условия:
○ вычислительно невозможно, зная открытый ключ, определить закрытый ключ;
○ вычислительно невозможно, зная закрытый ключ, определить открытый ключ;
○ вычислительно невозможно, зная открытый ключ и зашифрованное сообщение, восстановить исходное сообщение.

17. Хэш-функцией называется
○ односторонняя функция, предназначенная для получения дайджеста или "отпечатков пальцев" файла, сообщения или некоторого блока данных;
○ односторонняя функция, предназначенная для получения хэш-кода файла, сообщения или некоторого блока данных;
○ односторонняя функция, предназначенная для получения свертки файла, сообщения или некоторого блока данных.

18. Хэш-функция ГОСТ Р 34.11-2012 «Стрибог» формирует хэш-код размером
○ 256 бит;
○ 512 бит;
○ 1024 бит.

19. Хэш-функция ГОСТ Р 34.11-2012 «Стрибог» оперирует блоком исходного сообщения размером
○ 256 бит;
○ 512 бит;
○ 1024 бит.

20. Максимальный размер имитовставки в алгоритме ГОСТ 28147-89 составляет _____ (64) бит;

21. Длина ключа алгоритма IDEA равна _____ (128) бит.

22. Тройной DES может быть реализован с _____ «количество» (2) или _____ «количество» (3) кчами шифрования.

23. Рассеяние статистических особенностей незашифрованного текста в широком диапазоне статистических особенностей зашифрованного текста называется _____ (диффузией).

24.Уничтожение статистической взаимосвязи между зашифрованным текстом и ключом называется _____(конфузией).

25. Конечная задача _____ (дифференциального) криптоанализа: используя свойства алгоритма, в основном свойства S-boxes, определить подключ раунда.

26. Операция подстановки алгоритма DES в каждом раунде использует __ (8) S-boxes.

27. Атака "встреча посередине" применима для алгоритма _____ (двойной) DES.

28. Схема раунда ГОСТ 28147-89 в режиме простой замены;

29. Режим работы блочных криптоалгоритмов CBC: схема шифрования;

30. Режим работы блочных криптоалгоритмов CFB: схема шифрования;

31. Режим работы блочных криптоалгоритмов OFB: схема шифрования;

32. Что такое «сильная» хэш-функция?

33. Что такое «коллизия» для хэш-функций?

3.3. Перечень тем курсовых работ (КР)

1-25. Программная реализация протоколов цифровой подписи, аутентификации, распределения ключей (см. методические указания к КР).

3.4. Перечень теоретических вопросов к экзамену

1. История развития криптографии.
2. Основные задачи и понятия криптографии.
3. Требования к криптосистемам.
4. Шифры перестановки.
5. Шифры замены.
6. Поточные шифры.
7. Блочные шифры.
8. Сети Фейстеля.
9. Основы теории К.Шеннона.
10. Вопросы имитозащиты. Помехоустойчивость шифров.
11. Принципы построения криптографических алгоритмов.
12. Алгоритм DES. Усиления DES.
13. Алгоритм IDEA.
14. Алгоритм AES.
15. Алгоритм ГОСТ 28147-89.
16. Режимы выполнения симметричных криптоалгоритмов.
17. Типовые генераторы псевдослучайных последовательностей.
18. Требования к асимметричным криптосистемам.
19. Криптосистема RSA.
20. Криптосистема Эль-Гамаля.
21. Криптосистема на основе задачи об “укладке рюкзака.
22. Подходы к анализу криптографических алгоритмов. Метод перебора.
23. Частотный анализ. Корреляционный метод анализа поточных шифров.
24. Линейный и дифференциальный методы анализа блочных шифров.
25. Целостность данных и аутентификация источника данных.
26. Общие сведения о хеш-функциях.
27. Требования к хэш-функциям. Понятие о стойкости хеш-функции.
28. Ключевые и бесключевые хеш-функции.
29. Итеративные способы построения хеш-функций.
30. Сильные хэш-функции: MD5.
31. Сильные хэш-функции: SHA.
32. Сильные хэш-функции: ГОСТ 3411.
33. Задачи и назначения электронной подписи.
34. Основные требования, прямая и арбитражная цифровая подпись.
35. Классификация электронных подписей.
36. Примеры цифровых подписей на основе алгоритма RSA.
37. Примеры цифровых подписей на основе алгоритма Эль-Гамаля.
38. Стандарты подписи ГОСТ 3410.
39. Стандарты подписи ГОСТ DSS.
40. Инфраструктура открытых ключей.

3.5. Перечень типовых простых практических заданий к экзамену

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

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

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

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Сообщение, доклад	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Защита лабораторной работы	Обучаемый самостоятельно, под руководством преподавателя выполняет лабораторную работу на заданную тему. Тема (задание) предлагается в конкретном виде. Методы и инструменты для ее разработки предлагаются преподавателем. После выполнения задания обучаемый готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования (защиты). Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Курсовая работа	Обучаемый самостоятельно, под руководством преподавателя выполняет курсовую работу на заданную тему. Тема предлагается в общем виде. Конкретные методы и инструменты для ее разработки обучаемый выбирает самостоятельно. Обучаемый подбирает литературу по теме, не менее 3-4 источников, включая самостоятельный поиск в интернет (обязательно), разрабатывает ее, готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования. Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.

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 экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что в каждый из них включал в себя теоретические вопросы и практические задания.

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

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

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

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

Образец экзаменационного билета

ИРГУПС 20__-20__ учебный год	**Экзаменационный билет № 1** **по дисциплине «_____»** **__ ____ семестр**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1. …… 2. …… 3. …….. 4. …….. 5 ……..……. Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм		

В разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы» приведены типовые контрольные задания, для оценки результатов освоения образовательной программы. Задания, по которым проводятся контрольно-оценочные мероприятия, оформляются в соответствии с формами оформления оценочных средств, приведенными ниже, и не выставляются в электронную информационно-образовательную среду ИрГУПС, а хранятся на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.