ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «31» мая 2024 г. № 425-1

Б1.О.43 Криптографические протоколы и стандарты

рабочая программа дисциплины

Специальность/направление подготовки – 10.05.03 Информационная безопасность автоматизированных систем
Специализация/профиль – Безопасность открытых информационных систем
Квалификация выпускника – Специалист по защите информации
Форма и срок обучения – очная форма 5 лет, 6 месяцев
Кафедра-разработчик программы – Информационные системы и защита информации

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

Формы промежуточной аттестации
очная форма обучения:
зачет 8 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

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

ИРКУТСК

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

Программу составил(и):
преподаватель, А.С. Вергасов

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «21» мая 2024 г. № 11

Зав. кафедрой, к. э. н, доцент Т.К. Кириллова

1 ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ	
1.1 Цель дисциплины	
1	формирование представления о криптографических протоколах и стандартах
1.2 Задачи дисциплины	
1	ознакомление с основными понятиями в области криптографических протоколов и стандартов
2	формирование глубоких и всесторонних знаний по используемым криптографическим протоколам и стандартам
3	формирование навыков применения полученных знаний для решения практических задач по применению криптографических протоколов и стандартов
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
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	
Блок/часть ОПОП	Блок 1. Дисциплины / Обязательная часть
2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины	
1	Б1.О.34 Документоведение
2	Б1.О.36 Сети и системы передачи информации
3	Б1.О.37 Защита информации от утечки по техническим каналам
4	Б1.О.54 Методы и средства криптографической защиты информации
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.О.39 Программно-аппаратные средства защиты информации
2	Б1.О.45 Виртуальные частные сети
3	Б1.О.60 Защита информации от несанкционированного доступа
4	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения
ОПК-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Знает средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Знать: современные подходы к организации сложных криптосистем; основные международные стандарты, регламентирующие применение криптографических методов защиты информации
		Уметь: анализировать текущее состояние ИБ на предприятии с целью разработки требований к средствам криптографической защиты информации (СКЗИ)
		Владеть: навыками решения задач количественной оценки стойкости и производительности криптографических протоколов
	ОПК-10.2 Умеет применять доверенное хранение, защиту каналов связи и электронного документооборота	Знать: нормативно-технические документы, регламентирующие проектирование, разработку и применение СКЗИ в РФ
		Уметь: применять формальные методы анализа криптографических протоколов; оценивать сложность реализации криптографических протоколов

		Владеть: навыками организации защищенного электронного документооборота, защищенных каналов связи и доверенного хранения
	ОПК-10.3 Имеет навыки работы с алгоритмами криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и для защиты информации от несанкционированного доступа при ее обработке и хранении	Знать: принципы анализа стойкости криптографических протоколов; принципы выявления уязвимостей СКЗИ
		Уметь: грамотно выбирать и корректно реализовывать криптографические методы защиты информации при создании средств и систем комплексной защиты информации
		Владеть: навыками разработки элементов технических заданий на создание СКЗИ

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
1.0	**Раздел 1. Криптографические протоколы и сервисы идентификации и аутентификации абонентов и объектов сети.**						
1.1	Введение. Определения, цели, задачи дисциплины. Основные термины и определения	8	4			6	ОПК-10.1
1.2	Аутенфикация на основе паролей	8	4			6	ОПК-10.1
1.3	Аутентификация Kerberos	8	4			6	ОПК-10.1
1.4	Изучение механизмов аутенфикации, использующих криптографические протоколы	8	2	12		4	ОПК-10.1
1.5	Механизмы одноразовой аутенфикации	8	2			4	ОПК-10.1
1.6	Программная реализация алгоритма DES	8			7		ОПК-10.1 ОПК-10.2 ОПК-10.3
2.0	**Раздел 2. Инфраструктура открытых ключей. Национальные криптографические стандарты.**						
2.1	Криптографическая система с открытым ключом	8	2			4	ОПК-10.1
2.2	Программная реализация алгоритма RSA	8			10		ОПК-10.1 ОПК-10.2 ОПК-10.3
2.3	Основные компоненты PKI	8	2			4	ОПК-10.1
2.4	Базовые криптографические механизмы сервисов безопасности PKI	8	6			13	ОПК-10.1
2.5	Национальные криптографические стандарты	8	4			6	ОПК-10.1
2.6	Нормативная база по использованию ЭП в РФ	8	4			6	ОПК-10.1
2.7	Анализ политик безопасности удостоверяющих центров	8		10			ОПК-10.1
2.8	Требования ГОСТ к криптографическим протоколам	8		12			ОПК-10.1
	Форма промежуточной аттестации – зачет	8					
	Итого часов (без учёта часов на промежуточную аттестацию)		34	34	17	59	

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

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Корниенко, А. А. Криптографические протоколы : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2020. — 74 с. — URL: https://e.lanbook.com/book/191009 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Пугин, В. В. Криптографические протоколы : методические указания к выполнению лабораторных работ / В. В. Пугин, С. А. Лабада. — Самара : ПГУТИ, 2018. — 51 с. — URL: https://e.lanbook.com/book/182303 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.3	Ищукова, Е. А. Криптографические протоколы и стандарты : учебное пособие / Е. А. Ищукова, Е. А. Лобова ; Южный федеральный университет. — Таганрог : Южный федеральный университет, 2016. — 80 с. — URL: https://biblioclub.ru/index.php?page=book&id=493059 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.2 Дополнительная литература		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Лапонина, О. Р. Криптографические основы безопасности : учебное пособие / О. Р. Лапонина. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. — 244 с. — URL: https://biblioclub.ru/index.php?page=book&id=429092 (дата обращения: 18.04.2024). — Текст : электронный.	Онлайн
6.1.2.2	Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Юрайт, 2024. — 349 с. — URL: https://urait.ru/bcode/536902 (дата обращения: 22.04.2024). — Текст : электронный.	Онлайн
6.1.2.3	Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд. — Москва : Юрайт, 2024. — 473 с. — URL: https://urait.ru/bcode/536132 (дата обращения: 22.04.2024). — Текст : электронный.	Онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	А.С. Вергасов. Методические указания по изучению дисциплины Б1.О.43 Криптографические протоколы и стандарты по специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Безопасность открытых информационных систем / А.С. Вергасов; ИрГУПС. – Иркутск: ИрГУПС, 2023. – 14 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47635_1529_2024_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.ru/	
6.2.2	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.2.3	Электронно-библиотечная система «Образовательная платформа ЮРАЙТ», https://urait.ru/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	MathCAD_student 15.0 Academic_License, Customer Number 434692, контракт от 03.12.2012 № 0334100010012000148-0000756-01	

6.3.2.2	Python 3.9, свободно распространяемое программное обеспечение https://docs.python.org/3/license.html
6.3.2.3	Dev-C++, свободная интегрированная среда разработки приложений для языков программирования C/C++, https://code-live.ru/post/dev-cpp-free-cpp-ide-for-windows/
6.3.2.4	MatLab Classroom, R2015a, R2015b, контракт от 09.07.2014 № 0334100010014000028-0000756-01.
6.3.2.5	MatLab Classroom, R2010a, R2010b, лицензия от 16.03.2011 № 689810, ГК № 0334100010011000032-00000756-01. прогр.средство защиты от НСД Secret Net4.0, клиент серв.безоп.Secret Net 4.0, сервер безопасности С Secret Net4.0, система разгр.доступа Dallas Lock 7.0
6.3.3 Информационные справочные системы	
6.3.3.1	Не предусмотрены
6.4 Правовые и нормативные документы	
6.4.1	Не предусмотрены

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

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Учебная аудитория Д-521 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
4	Лаборатория Д-523 «Моделирование и разработка программных систем и защита информации».«Безопасность программно-аппаратных средств защиты информации» для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор (переносной), экран (переносной), компьютер измеритель шумов и вибрации 003-МЗ
5	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место

	для освещения упомянутых вопросов. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Лабораторная работа	Основной целью лабораторных работ является теоретическое обоснование, наглядное и/или экспериментальное подтверждение и/или проверка существенных теоретических положений (законов, закономерностей) анализ существующих методик и методов их реализации и т.д. Они занимают преимущественное место при изучении дисциплин обязательной части и части, формируемой участниками образовательных отношений Блока 1. Исходя из цели, содержанием лабораторных работ могут быть: - экспериментальная проверка формул, методик расчета; - проведение натурных измерений свойств, рабочих параметров, режимов работы при помощи лабораторного оборудования и/или стендов и макетов; - ознакомление, анализ и теоретические выкладки по устройству, принципу действия и способам обслуживания аппаратов, деталей машин, механизмов, процессов, протекающих в них при этом и т.д.; - наглядная графическая интерпретация чертежей, схем, объемных поверхностей и т.д., воспроизводимых с помощью специализированного программного обеспечения; - имитационное моделирование процессов, протекающих в сложных химических, физических, механических, электрических и пр. объектах; - наглядное представление о работе персонала конкретной организации или подразделения ОАО «РЖД» посредством моделирования штатных и внештатных ситуаций в виртуальных специализированных АРМ (автоматизированных рабочих мест); - установление и подтверждение закономерностей (путем сравнения проведенного эксперимента и рассчитанных значений) и т.д.; - ознакомление с методиками проведения экспериментов, наглядным устройством стенд-макетов и пр.; - установление свойств веществ, их качественных и количественных характеристик; - анализ различных характеристик процессов, в том числе производственных и иных процессов; - расчет параметров различных явлений и процессов, смоделировать которые не возможно в реальных условиях (например, чрезвычайные ситуации и пр.); - наблюдение развития явлений, процессов и др. Допускается иное содержание лабораторных работ, если это будет способствовать реализации целей и задач дисциплины и формированию соответствующих компетенций. По характеру выполняемых лабораторных работ возможны: - ознакомительные работы, используемые для закрепления изученного теоретического материалы; - аналитические работы, используемые для получения новой информации на основе формализованных методов; - творческие работы, ориентированные на самостоятельный выбор подходов решения задач. Прежде, чем приступить к лабораторным занятиям, обучающимся необходимо повторить теоретический материал по теме работы. Каждая лабораторная работа оснащена методическими указаниями, разработанными преподавателями, ведущими дисциплину
Самостоятельная работа	Обучение по дисциплине «Криптографические протоколы и стандарты» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая

	учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

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

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

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

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

– самоподготовка и самоконтроль обучающихся в процессе обучения.

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

Для оценки уровня сформированности компетенций используется трехуровневая система:

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

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

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

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

Дисциплина «Криптографические протоколы и стандарты» участвует в формировании компетенций:

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

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
8 семестр				
1.0	**Раздел 1. Криптографические протоколы и сервисы идентификации и аутентификации абонентов и объектов сети**			
1.1	Текущий контроль	Введение. Определения, цели, задачи дисциплины. Основные термины и определения	ОПК-10.1	Тестирование (компьютерные технологии)
1.2	Текущий контроль	Аутенфикация на основе паролей	ОПК-10.1	Тестирование (компьютерные технологии)
1.3	Текущий контроль	Аутентификация Kerberos	ОПК-10.1	Тестирование (компьютерные технологии)
1.4	Текущий контроль	Изучение механизмов аутенфикации, использующих криптографические протоколы	ОПК-10.1	Тестирование (компьютерные технологии)
1.5	Текущий контроль	Механизмы одноразовой аутенфикации	ОПК-10.1	Тестирование (компьютерные технологии)
1.6	Текущий контроль	Программная реализация алгоритма DES	ОПК-10.1 ОПК-10.2 ОПК-10.3	Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Инфраструктура открытых ключей. Национальные криптографические стандарты**			
2.1	Текущий контроль	Криптографическая система с открытым ключом	ОПК-10.1	Тестирование (компьютерные технологии)
2.2	Текущий контроль	Программная реализация алгоритма RSA	ОПК-10.1 ОПК-10.2 ОПК-10.3	Лабораторная работа (письменно/устно)
2.3	Текущий контроль	Основные компоненты PKI	ОПК-10.1	Тестирование (компьютерные технологии)
2.4	Текущий контроль	Базовые криптографические механизмы сервисов безопасности PKI	ОПК-10.1	Тестирование (компьютерные технологии)
2.5	Текущий контроль	Национальные криптографические стандарты	ОПК-10.1	Тестирование (компьютерные технологии)
2.6	Текущий контроль	Нормативная база по использованию ЭП в РФ	ОПК-10.1	Тестирование (компьютерные технологии)
2.7	Текущий контроль	Анализ политик безопасности удостоверяющих центров	ОПК-10.1	Тестирование (компьютерные технологии)
2.8	Текущий контроль	Требования ГОСТ к криптографическим протоколам	ОПК-10.1	Тестирование (компьютерные технологии)
	Промежуточная аттестация	Все темы		Зачет (собеседование)

				Зачет - тестирование (компьютерные технологии)

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

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	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
2	Лабораторная работа	Средство, позволяющее оценить умение обучающегося письменно/устно 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	Образец задания для выполнения лабораторной работы и примерный перечень вопросов для ее защиты

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Зачет	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 к зачету
2	Тест – промежуточная аттестация в форме зачета	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

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

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«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 владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
	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	Компетенция не сформирована

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

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 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	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ОПК-10.1	Введение. Определения, цели, задачи дисциплины. Основные термины и определения		3 – ОТЗ
			2 – ЗТЗ
ОПК-10.1	Аутенфикация на основе паролей		3 – ОТЗ
			2 – ЗТЗ
ОПК-10.1	Аутентификация Kerberos		3 – ОТЗ
			2 – ЗТЗ
ОПК-10.1			3 – ОТЗ

	Изучение механизмов аутенфикации, использующих криптографические протоколы		2 – ЗТЗ
ОПК-10.1	Механизмы одноразовой аутенфикации		3 – ОТЗ
			2 – ЗТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Программная реализация алгоритма DES		3 – ОТЗ
			2 – ЗТЗ
ОПК-10.1	Криптографическая система с открытым ключом		3 – ОТЗ
			2 – ЗТЗ
ОПК-10.1 ОПК-10.2 ОПК-10.3	Программная реализация алгоритма RSA		2 – ОТЗ
			3 – ЗТЗ
ОПК-10.1	Основные компоненты PKI		2 – ОТЗ
			3 – ЗТЗ
ОПК-10.1	Базовые криптографические механизмы сервисов безопасности PKI		2 – ОТЗ
			3 – ЗТЗ
ОПК-10.1	Национальные криптографические стандарты		2 – ОТЗ
			3 – ЗТЗ
ОПК-10.1	Нормативная база по использованию ЭП в РФ		2 – ОТЗ
			3 – ЗТЗ
ОПК-10.1	Анализ политик безопасности удостоверяющих центров		2 – ОТЗ
			3 – ЗТЗ
ОПК-10.1	Требования ГОСТ к криптографическим протоколам		3 – ОТЗ
			4 – ЗТЗ
		Итого	36 – ОТЗ
			36 – 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.

1. Что в переводе с греческого языка означает слово «криптография»?
   (1) шифр **(2) тайнопись** (3) преобразование (4) расшифровка
2. Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства? (1) шифр Маркова **(2) шифр Цезаря** (3) шифр Энигма (4) шифр Бэбиджа
3. Когда в криптографии стало использоваться асимметричное шифрование? (1) в первой половине XIX; (2) во второй половине XIX; (3) в первой половине XX; **(4) во второй половине XX**
4. Как называется совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты? (1) алгоритм (2) ключ (3) протокол **(4) шифр**

5. Как называется сообщение, полученное после преобразования с использованием любого шифра? **(1) закрытым текстом** (2) имитовставкой (3) ключом (4) открытым текстом
6. Что в криптографии называют открытым текстом? **(1) исходное сообщение (сообщение до шифрования)** (2) открытый ключ шифрования (3) сообщение, получение после преобразования с использованием любого шифра (4) электронную цифровую подпись
7. Гарантирование невозможности несанкционированного изменения информации - это: **(1) обеспечение целостности** (2) обеспечение конфиденциальности (3) обеспечение аутентификации (4) обеспечение шифрования
8. Под конфиденциальностью понимают (выберите продолжение) (1) решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, имеющих права доступа к **ней (2) решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней** (3) решение проблемы защиты информации от ее изменения со стороны лиц, не имеющих права доступа к ней (4) решение проблемы запуска программ со стороны лиц, не имеющих права доступа к ним (5) разрешение пользоваться информацией только одному лицу
9. Под целостностью понимают (выберите продолжение)
10. (1) гарантирование невозможности несанкционированного изменения объема информации **(2) гарантирование невозможности несанкционированного изменения информации** (3) гарантирование невозможности несанкционированного изменения порядка следования информации (4) гарантирование невозможности несанкционированного изменения переносов в текстовой информации
11. ыберите правильное определение термина «криптография» (1) криптография – это наука о преодолении криптографической защиты информации (2) криптография – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи **(3) криптография изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия** (4) криптография изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации
12. Выберите правильное определение термина «криптоанализ» (**1) криптоанализ – это наука о преодолении криптографической защиты информации** (2) криптоанализ – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи (3) криптоанализ изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия (4) криптоанализ изучает способы защиты информации, основанные на попытке скрыть от противника сам факт наличия интересующей его информации
13. Какая наука разрабатывает методы «вскрытия» шифров? (1) **криптография (2) криптоанализ** (3) теория чисел (4) тайнопись (5) линейная алгебра
14. Какие задачи решает криптография? **(1) защита передаваемых сообщений от прочтения (2) защита передаваемых сообщений от модификации** (3) сжатие передаваемых сообщений (4) помехоустойчивое кодирование передаваемых сообщений
15. Какие требования предъявляются в настоящее время к шифрам? (**1) зашифрованное сообщение должно поддаваться чтению только при наличии ключа** (2) знание алгоритма шифрования должно влиять на надежность защиты **(3) любой ключ из множества возможных должен обеспечивать надежную защиту информации** (4) алгоритм шифрования должен допускать только аппаратную реализацию
16. Как называется распределенный алгоритм, определяющий последовательность действий каждой из сторон? (1) процесс шифрования (2) электронная цифровая подпись **(3) протокол** (4) хэш-функция
17. Как называется способ реализации криптографического метода, при котором все процедуры шифрования и расшифрования выполняются специальными электронными

схемами по определенным логическим правилам**?(1) аппаратный** (2) программный (3) ручной (4) электромеханический

18. Что является основным недостатком программной реализации криптографических методов? (1) высокая стоимость разработки **(2) небольшое быстродействие** (3) небольшая разрядность (4) невозможность использования в современных беспроводных сетях

3.2 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

«Программная реализация алгоритма DES»

Реализовать алгоритм DES и 4 режима шифрования. Шифрование реализовать для любой длины сообщения и любой длины ключа до 56 бит включительно. Программа должна предусматривать сохранение зашифрованного и расшифрованного файла на диск, а также вывод на экран скорости и времени шифрования. Каждый файл шифровать с 3 парами ключей. Посчитать время зашифрования/расшифрования и среднюю скорость шифрования/расшифрования для каждой пары ключей и каждого файла.

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

«Программная реализация алгоритма RSA»

Реализовать алгоритм RSA. Сгенерировать 3 пары открытый/закрытый ключей. Брать файлы размером 20 Кб, 50 Кб, 100 Кб, 500 Кб, 1 МБ. . Программа должна предусматривать сохранение зашифрованного и расшифрованного файла на диск, а также вывод на экран скорости и времени шифрования. Каждый файл шифровать с 3 парами ключей. Посчитать время зашифрования/расшифрования и среднюю скорость шифрования/расшифрования для каждой пары ключей и каждого файла.

3.3 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Понятие криптографического протокола.
2. Роль криптографических протоколов в системах защиты информации.
3. Понятие криптографического протокола.
4. Свойства протоколов, характеризующие их безопасность.
5. Основные виды уязвимостей. Подходы к классификации криптографических протоколов.
6. Подходы к моделированию криптографических протоколов.
7. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры.
8. Основные подходы к автоматизации анализа протоколов.
9. Схемы цифровой подписи.
10. Схемы цифровой подписи на основе симметричных и асимметричных шифрсистем.
11. Схемы Эль-Гамаля, Фиата-Фейга-Шамира и Шнорра, их свойства Семейство схем типа Эль-Гамаля.
12. Стандарты США и России электронной цифровой подписи.
13. Одноразовые подписи.
14. Схемы конфиденциальной цифровой подписи и подписи вслепую.
15. Подписи с обнаружением подделки.
16. Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования.

17. Понятие протоколов интерактивного доказательства и доказательства знания.
18. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.
Аттестационная контрольна
19. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото.
20. Связь между протоколами цифровой подписи и протоколами идентификации.
21. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов.
22. Управление открытыми ключами.
23. Основы организации и основные компоненты инфраструктуры открытых ключей.
24. Сертификат открытого ключа.
25. Стандарт X.509.
26. Сервисы инфраструктуры открытых ключей.
27. Удостоверяющий центр. Центр регистрации.
28. Репозиторий.
29. Архив сертификатов. Конечные субъекты.
30. Архитектуры инфраструктуры открытых ключей.
31. Проверка и отзыв сертификата открытого ключа.
32. Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.
33. Двух и трех сторонние протоколы передачи и распределения ключей.
34. Функции доверенной третьей стороны и выполняемые ею роли.
35. Схемы предварительного распределения ключей.

3.4 Перечень типовых простых практических заданий к зачету

(для оценки умений)

1. Построение протоколов ЦП с использованием актуальных механизмов формирования
2. Построение протокола с нулевым разглашением с алгоритмом Рабина.
3. Построение протокола взаимной уптентификации

3.5 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

1. Построение протоколов открытого шифрования Эль-Гамаля
2. Построение протокола открытого шифрования по Рабину.
3. Построение протокола ЭЦП Эль-Гамаля

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
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 защиты 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

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 зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

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

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Шкала оценивания
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то

промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

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.