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.В.ДВ.04.02 Криптографические протоколы

рабочая программа дисциплины

Специальность/направление подготовки – 10.04.01 Информационная безопасность
Специализация/профиль – Безопасность информационных систем и технологий
Квалификация выпускника – Магистр
Форма и срок обучения – очная форма 2 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 3
Часов по учебному плану (УП) – 108
В том числе в форме практической подготовки (ПП) – 10
(очная)

Формы промежуточной аттестации
очная форма обучения:
экзамен 3 семестр

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

Семестр	3	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	51/10	**51/10**
– лекции	17	**17**
– практические (семинарские)	17/10	**17/10**
– лабораторные	17	**17**
Самостоятельная работа	21	**21**
Экзамен	36	**36**
Итого	108/10	**108/10**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 26.11.2020 № 1455.

Программу составил(и):
к.ф.-м.н., доцент, А.А. Бутин

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 ЗАДАЧА ДИСЦИПЛИНЫ	
1.1 Цель дисциплины	
1	изучение криптографических протоколов
1.2 Задача дисциплины	
1	освоение методов анализа криптопротоколов, основных сфер практического применения и особенностей реализации

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
Блок/часть ОПОП	Блок 1. Дисциплины / Часть, формируемая участниками образовательных отношений
2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины	
1	Б1.В.ДВ.01.01 Проектирование информационных систем
2	Б1.В.ДВ.02.01 Инструментарий анализа информационных рисков
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б2.В.01(П) Производственная - организационно-управленческая практика
2	Б2.В.02(Пд) Производственная - преддипломная практика
3	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
4	Б3.02(Д) Защита 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
ПК-2 Способен организовать работы по выявлению недостатков в функционировании системы защиты	ПК-2.2 Исследует архитектуру системы защиты информации для оценки функциональных возможностей добавочных программно-аппаратных средств защиты информации	Знать: виды атак на криптопротоколы; способы анализа криптографических протоколов
		Уметь: производить обоснованный выбор средств защиты информации на основе криптографических протоколов
		Владеть: навыками анализа российских и международных стандартов по идентификации и аутентификации субъектов; навыками анализа уязвимостей криптографических протоколов
ПК-3 Способен проектировать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной безопасности	ПК-3.2 Выполняет работы по установке, настройке и обслуживанию программных, программно-аппаратных средств защиты информации	Знать: основные классы криптографических протоколов
		Уметь: оценивать функциональные возможности криптопротоколов
		Владеть: навыками администрирования продуктов на базе криптографических протоколов

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. Понятие криптографического протокола. Классификация криптографических протоколов. Формальные методы анализа протоколов обеспечения безопасности**						
1.1	Тема 1. Основные определения. Функции -сервисы безопасности	3	3				ПК-2.2 ПК-3.2
1.2	Тема 2. Примитивные и прикладные протоколы. Основные атаки на безопасность протоколов. Слабости в известных протоколах	3	4			4	ПК-2.2 ПК-3.2
1.3	Лабораторная работа № 1. Протоколы на основе алгоритма RSA	3			2		ПК-2.2 ПК-3.2
2.0	**Раздел 2. Протоколы идентификации и аутентификации. Протоколы, использую-щие технику доказательства знания. Протоколы передачи**						

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
	ключей. Протокол TLS/SSL						
2.1	Тема 3. Виды и примеры протоколов идентификации и аутентификации. Протоколы идентификации, использующие технику «запрос—ответ»	3	4			4	ПК-2.2 ПК-3.2
2.2	Тема 4. Генерация и передача ключей	3	3			5	ПК-2.2 ПК-3.2
2.3	Тема 5. Алгоритм Диффи-Хеллмана-Меркле	3	3			4	ПК-2.2 ПК-3.2
2.4	Тема 6. Интерактивное доказательство. Протоколы Фиата-Шамира, Шнорра, Окамото. Протокол привязки к биту. Протокол подписания контракта	3		6/3			ПК-2.2 ПК-3.2
2.5	Тема 7. Криптографические операции. HMAC и псевдослучайная функция. Протокол записи	3		4/3			ПК-2.2 ПК-3.2
2.6	Тема 8. Протокол TLS/SSL	3		3/2		4	ПК-2.2 ПК-3.2
2.7	Тема 9. Общий анализ стандартов по идентификации и аутентификации при доступе субъектов к информации	3		4/2			ПК-2.2 ПК-3.2
2.8	Лабораторная работа № 2. Схема Клауса-Шнорра	3			3		ПК-2.2 ПК-3.2
2.9	Лабораторная работа № 3.. Схема аутентификации Фейге-Фиата-Шамира	3			4		ПК-2.2 ПК-3.2
2.10	Лабораторная работа № 4. Схема разбиения секрета с использованием гаммированияОбщий анализ стандартов по идентификации и аутентификации при доступе субъектов к информации	3			4		ПК-2.2 ПК-3.2
2.11	Лабораторная работа № 5. Протокол тайных многосторонних вычислений и разделения секрета	3			4		ПК-2.2 ПК-3.2
	Форма промежуточной аттестации – экзамен	3	36				
	Итого часов (без учёта часов на промежуточную аттестацию)		17	17/10	17	21	

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	Каширская, Е. Н. Криптографический анализ и методы защиты информации : учебное пособие / Е. Н. Каширская. — Москва : РТУ МИРЭА, 2020. — 91 с. — URL: https://e.lanbook.com/book/163861 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.1.2	Корниенко, А.А. Криптографические протоколы / рец.: В. Н. Кустов, С. В. Диасамидзе. — Санкт-Петербург : ПГУПС, 2020. — 74 с. — URL: https://umczdt.ru/books/1283/260440/ (дата обращения: 26.04.2024). — 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:	Онлайн

	18.04.2024). — Текст : электронный.	
6.1.1.4	Косолапов, Ю. В. Криптографические протоколы на основе линейных кодов : учебное пособие / Ю. В. Косолапов ; Южный федеральный университет. — Ростов-на-Дону, Таганрог : Южный федеральный университет, 2020. — 100 с. — URL: https://biblioclub.ru/index.php?page=book&id=598671 (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	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. — Самара : ПГУТИ, 2019. — 68 с. — URL: https://e.lanbook.com/book/223319 (дата обращения: 15.04.2024). — Текст : электронный.	Онлайн
6.1.2.2	Рацеев, С. М. Криптографические протоколы. Схемы разделения секрета : учебное пособие для вузов / С. М. Рацеев. — Санкт-Петербург : Лань, 2024. — 336 с. — URL: https://e.lanbook.com/book/367457 (дата обращения: 15.04.2024). — 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	Бутин, А.А. Методические указания по изучению дисциплины Б1.В.ДВ.04.02 Криптографические протоколы по направлению подготовки 10.04.01 Информационная безопасность, профиль Безопасность информационных систем и технологий / А.А. Бутин; ИрГУПС. – Иркутск: ИрГУПС, 2023. – 12 с - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_47492_1506_2024_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.2.2	Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте «ЭБ УМЦ ЖДТ» — https://umczdt.ru/books/	
6.2.3	Электронно-библиотечная система «Университетская библиотека онлайн», https://biblioclub.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.	
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	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
3	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)
4	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507; – 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» 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» участвует в формировании компетенций:

ПК-2. Способен организовать работы по выявлению недостатков в функционировании системы защиты

ПК-3. Способен проектировать и эксплуатировать автоматизированные системы, используя программно-аппаратные средства обеспечения информационной безопасности

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
3 семестр				
1.0	**Раздел 1. Понятие криптографического протокола. Классификация криптографических протоколов. Формальные методы анализа протоколов обеспечения безопасности**			
1.1	Текущий контроль	Тема 1. Основные определения. Функции -сервисы безопасности	ПК-2.2 ПК-3.2	Тестирование (компьютерные технологии)
1.2	Текущий контроль	Тема 2. Примитивные и прикладные протоколы. Основные атаки на безопасность протоколов. Слабости в известных протоколах	ПК-2.2 ПК-3.2	Тестирование (компьютерные технологии)
1.3	Текущий контроль	Лабораторная работа № 1. Протоколы на основе алгоритма RSA	ПК-2.2 ПК-3.2	Лабораторная работа (письменно/устно)
2.0	**Раздел 2. Протоколы идентификации и аутентификации. Протоколы, использую-щие технику доказательства знания. Протоколы передачи ключей. Протокол TLS/SSL**			
2.1	Текущий контроль	Тема 3. Виды и примеры протоколов идентификации и аутентификации. Протоколы идентификации, использующие технику «запрос—ответ»	ПК-2.2 ПК-3.2	Тестирование (компьютерные технологии)
2.2	Текущий контроль	Тема 4. Генерация и передача ключей	ПК-2.2 ПК-3.2	Тестирование (компьютерные технологии)
2.3	Текущий контроль	Тема 5. Алгоритм Диффи-Хеллмана-Меркле	ПК-2.2 ПК-3.2	Тестирование (компьютерные технологии)
2.4	Текущий контроль	Тема 6. Интерактивное доказательство. Протоколы Фиата-Шамира, Шнорра, Окамото. Протокол привязки к биту. Протокол подписания контракта	ПК-2.2 ПК-3.2	Доклад (устно) В рамках ПП**: Лабораторная работа (письменно/устно)
2.5	Текущий контроль	Тема 7. Криптографические операции. HMAC и псевдослучайная функция. Протокол записи	ПК-2.2 ПК-3.2	Доклад (устно) В рамках ПП**: Лабораторная работа (письменно/устно)
2.6	Текущий контроль	Тема 8. Протокол TLS/SSL	ПК-2.2 ПК-3.2	Доклад (устно) В рамках ПП**: Лабораторная работа (письменно/устно)
2.7	Текущий контроль	Тема 9. Общий анализ стандартов по идентификации и аутентификации при доступе субъектов к информации	ПК-2.2 ПК-3.2	Доклад (устно) В рамках ПП**: Лабораторная работа (письменно/устно)

2.8	Текущий контроль	Лабораторная работа № 2. Схема Клауса-Шнорра	ПК-2.2 ПК-3.2	Лабораторная работа (письменно/устно)
2.9	Текущий контроль	Лабораторная работа № 3.. Схема аутентификации Фейге-Фиата-Шамира	ПК-2.2 ПК-3.2	Лабораторная работа (письменно/устно)
2.10	Текущий контроль	Лабораторная работа № 4. Схема разбиения секрета с использованием гаммированияОбщий анализ стандартов по идентификации и аутентификации при доступе субъектов к информации	ПК-2.2 ПК-3.2	Лабораторная работа (письменно/устно)
2.11	Текущий контроль	Лабораторная работа № 5. Протокол тайных многосторонних вычислений и разделения секрета	ПК-2.2 ПК-3.2	Лабораторная работа (письменно/устно)
	Промежуточная аттестация	Все разделы		Экзамен (собеседование) Экзамен - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.
**ПП – практическая подготовка

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	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
2	Тестирование (компьютерные технологии)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
3	Лабораторная работа	Средство, позволяющее оценить умение обучающегося	Образец задания

		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	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	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (образец экзаменационного билета) к экзамену
2	Тест – промежуточная аттестация в форме экзамена	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

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

Шкала оценивания	Критерии оценивания	Уровень освоения компетенции
«отлично»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«неудовлетворительно»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенция не сформирована

Тест – промежуточная аттестация в форме экзамена

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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Доклад

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

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 темы для написания докладов

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

Ниже приведен образец типовых вариантов тем для написания докладов.

Образец тем докладов

1. Интерактивное доказательство;
2. Протоколы Фиата-Шамира, Шнорра, Окамото;
3. Протокол привязки к биту;
4. Протокол подписания контракта;
5. Криптографические операции;
6. HMAC и псевдослучайная функция;
7. Протокол записи;
8. Протокол TLS/SSL;
9. Общий анализ стандартов по идентификации и аутентификации при доступе субъектов к информации.

3.2 Типовые контрольные задания для проведения тестирования

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

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ

ПК-2.2 ПК-3.2	Тема 1. Основные определения. Функции -сервисы безопасности	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ПК-2.2 ПК-3.2	Тема 2. Примитивные и прикладные протоколы. Основные атаки на безопасность протоколов. Слабости в известных протоколах	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ПК-2.2 ПК-3.2	Тема 3. Виды и примеры протоколов идентификации и аутентификации. Протоколы идентификации, использующие технику «запрос—ответ»	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ПК-2.2 ПК-3.2	Тема 4. Генерация и передача ключей	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
ПК-2.2 ПК-3.2	Тема 5. Алгоритм Диффи-Хеллмана-Меркле	Знание	1 – ОТЗ 1 – ЗТЗ
		Умение	1 – ОТЗ 1 – ЗТЗ
		Навык	1 – ОТЗ 1 – ЗТЗ
		Итого	30 – ОТЗ 30 – 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. Приведите правильный ответ: «RSA - это»:

А) криптографический алгоритм с открытым ключом;
Б) криптографический алгоритм с закрытым ключом, но без открытого ключа;
В) протокол шифрования с гаммированием.

2. Цели управлениями ключами:

А) компрометация конфиденциальности закрытых ключей;
Б) распределение ключей;
В) компрометация аутентичности закрытых или открытых ключей.

3. Вставьте слово: «Электронная подпись применяется для подтверждения _____ сообщения»:

Ответ: подлинности/авторства

4. Вставьте слово: «Схема цифровой подписи *Schnorr* Клауса Шнорра является вариантом схемы цифровой _____ Эль-Гамаля»:

Ответ: подписи

5. Вставьте слово: «Протоколы идентификации и аутентификации необходимы для установления _____ соединений»

Ответ: доверенных

6. Приведите правильный ответ: «Функции криптографических протоколов»:
А) формирование ключей;
Б) аутентификация сторон;
В) обеспечение открытости соединения.

7. Вставьте слово: «Протокол Фейга — Фиата — Шамира — протокол идентификации с _____ разглашением»:
Ответ: нулевым

8. Вставьте слово: «Криптографические протоколы можно разделить на две группы: примитивные и _____»:
Ответ: прикладные

9. Приведите правильный ответ: «Дешифрование « - это
А) процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного;
Б) процесс извлечения открытого текста со знанием криптографического ключа на основе известного шифрованного;
В) процесс сокрытия открытого текста без знания криптографического ключа на основе известного шифрованного.

10. Выберите правильный ответ: «Отечественный алгоритм криптографического преобразования»:
А) ГОСТ 28147-89;
Б) ГОСТ 26145-89;
В) ГОСТ 26145-98.

11. Приведите правильный ответ: «Выберите из списка ассиметричные алгоритмы шифрования:
А) AES;
Б) DEA;
В) RSA

12. Приведите правильный ответ: «Выберите из списка симметричные алгоритмы шифрования»:
А) ГОСТ 28147-89;
Б) MD5;
В) Elgamal.

13. Приведите правильный ответ: «Симметричные системы шифрования реализуются в виде следующих схем»:
А) блочные;
Б) поточные;
В) алгоритмичные.

14. Вставьте слово; «Доказательство с_____ разглашением — это интерактивный вероятностный протокол, который позволяет доказать, что доказываемое утверждение верно, и Доказывающий знает это доказательство, в то же время не предоставляя никакой информации о самом доказательстве данного утверждения»:
Ответ: нулевым

15. Вставьте слово: «В криптографии протоколы _____ голосования — это протоколы обмена данными для реализации безопасного тайного электронного голосования через Интернет»:

Ответ: тайного

16. Вставьте слово: «Diffie–Hellman key exchange protocol, DH) — криптографический протокол, позволяющий двум и более сторонам получить общий _____ ключ, используя незащищенный от прослушивания канал связи»:

Ответ: секретный

17. Вставьте слово: «HMAC (Hash-based message authentication code) - это хэш, который вычисляется, основываясь на двух значениях: 'ключ' и '_____'»:

Ответ: сообщение

18. Вставьте слово: «Криптографический протокол (англ. Cryptographic protocol) — это абстрактный или конкретный протокол, включающий набор _____ алгоритмов, часто являющихся последовательностью криптографических примитивов»:

Ответ: криптографических

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

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

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

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

«Лабораторная работа № 1. Протоколы на основе алгоритма RSA»

Задание:

1. Реализовать приложение для шифрования;
2. Реализовать приложение для дешифрования;
3. С помощью реализованных приложений протестировать правильность работы разработанных приложений;
4. Сделать выводы о проделанной работе.

Вопросы:

1. В чем заключается алгоритм RSA?
2. Для чего и почему используют комбинированные криптоалгоритмы?
3. В чем заключаются достоинства и недостатки асимметричных алгоритмов?
4. В чем заключаются достоинства и недостатки симметричных алгоритмов?

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

«Лабораторная работа № 2. Схема Клауса-Шнорра»

Задание:

1. Реализовать схему Клауса-Шнорра

Вопросы:

1. Какая идея лежит в основе алгоритма?
2. Как выглядит алгоритм?
3. В чем заключаются достоинства и недостатки алгоритма?
4. В чем заключаются достоинства и недостатки алгоритма?

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

«Лабораторная работа № 3. Схема аутентификации Фейге-Фиата-Шамира»

Задание:

1. Реализовать схему аутентификации Фейге-Фиата-Шамира.
   a. Сгенерировать ключи
   b. Произвести аутентификацию

Вопросы:

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».
2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением?
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

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

«Лабораторная работа № 4. Схема разбиения секрета с использованием гаммирования. Общий анализ стандартов по идентификации и аутентификации при доступе субъектов к информации»

Задание:

1. Выберите метод получения гаммы шифра (псевдослучайной последовательности чисел).
2. Реализуйте программный модуль в соответствии с полученным заданием.

Вопросы:

1. В чем особенности метода аналитических преобразований.
2. Отличия метода посимвольного шифрования и шифрования текста биграммами.

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

«Лабораторная работа № 5. Протокол тайных многосторонних вычислений и разделения секрета»

Задание:

1. Изучить теоретическую часть и создать несколько программ по теме лабораторной работы.

Вопросы:

1. Сколько существует принципов решения задач, связанных с разделением секрета?
2. Как они реализуются?
3. Какие ключи шифрования используются в протоколе тайных многосторонних вычислений?

3.4 Перечень теоретических вопросов к экзамену

(для оценки знаний)

1. Основные определения. Функции -сервисы безопасности;
2. Группы требований (целей, свойств) безопасности Internet Engineering Task Force;
3. Формальные описания криптографических протоколов;
4. Примитивные и прикладные протоколы;
5. Основные атаки на безопасность протоколов;
6. Слабости в известных протоколах;
7. Вероятностные протоколы;
8. Формальные системы анализа на основе логик;

9. Формальные системы анализа на основе верификационной техники.
10. Виды и примеры протоколов идентификации и аутентификации;
11. Протоколы идентификации, использующие технику «запрос—ответ»;
12. Интерактивное доказательство;
13. Протокол Фиата-Шамира;
14. Протокол Шнорра;
15. Протокол Окамото;
16. Протоколы односторонней и двусторонней аутентификации. Электронная подпись;
17. Протоколы с доверенной третьей стороной;
18. Электронная подпись;
19. Протоколы голосования и электронной коммерции;
20. Генерация и передача ключей;
21. Алгоритм Диффи-Хеллмана-Меркле;
22. Анализ стандартов по идентификации и аутентификации;
23. HMAC и псевдослучайная функция;
24. Протокол записи.

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
Доклад	Защита докладов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему докладов и требования, предъявляемые к их выполнению и защите
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 экзамена и оценивания результатов обучения

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

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

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

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

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

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

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

Образец экзаменационного билета

<table>
<tr><td>ИРГУПС
20__-20__
учебный год</td><td>Экзаменационный билет № 1
по дисциплине «<u>Криптографические протоколы</u>»</td><td>Утверждаю:
Заведующий кафедрой
«_____» ИрГУПС
_____</td></tr>
<tr><td colspan="3">1. Интерактивное доказательство
2. Основные определения. Функции-сервисы безопасности
3. HMAC и псевдослучайная функция
4. Протоколы с доверенной третьей стороной</td></tr>
</table>