ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

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

Б1.Б.1.ДС.02 Криптографические протоколы и стандарты

рабочая программа дисциплины

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

Общая трудоемкость в з.е. – 3
Часов по учебному плану – 108

Формы промежуточной аттестации в семестрах:
зачет 8

Распределение часов дисциплины по семестрам

Семестр	9	**Итого**
Число недель в семестре	15	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**54**	**54**
– лекции	18	18
– практические (семинарские)	18	18
– лабораторные работы	18	18
Самостоятельная работа	**54**	**54**
Итого	**108**	**108**

ИРКУТСК

Электронный документ выгружен из ЕИС ФГБОУ ВО ИрГУПС и соответствует оригиналу
Подписант ФГБОУ ВО ИрГУПС Трофимов Ю.А.
00a73c5b7b623a969ccad43a81ab346d50 с 08.12.2022 14:32 по 02.03.2024 14:32 GMT+03:00
Подпись соответствует файлу документа

1 ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цели освоения дисциплины	
1	- формирование представления о криптографических протоколах и стандартах.
1.2 Задачи освоения 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

Научно-образовательное воспитание обучающихся

Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.

Цель достигается по мере решения в единстве следующих задач:
– формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности;
– создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками;
– популяризация научных знаний среди обучающихся;
– содействие повышению привлекательности науки, поддержка научно-технического творчества;
– создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества;
– совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.Б.1.23 «Криптографические методы защиты информации»;
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
2	Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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

ПК-9**:** способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

Минимальный уровень освоения компетенции	
Знать	Нормативные документы по разработке защищенных автоматизированных систем в сфере профессиональной деятельности
Уметь	Применять на практике нормативные документы по разработке защищенных автоматизированных систем в сфере профессиональной деятельности
Владеть	Навыками безопасного использования технических средств автоматизации
Базовый уровень освоения компетенции	
Знать	Уровни защищенности АС
Уметь	Оценивать эффективность и надежность автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов
Владеть	Навыками применения криптопротоколов и стандартов для построения защищенных систем
Высокий уровень освоения компетенции	
Знать	Методики оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов
Уметь	Применять на практике методики оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов
Владеть	Навыками документирования оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов
ПСК-4.1**:** способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных	
Минимальный уровень освоения компетенции	
Знать	Принципы эксплуатации систем и средств обеспечения информационной безопасности
Уметь	формулировать принципы эксплуатации систем и средств обеспечения информационной безопасности
Владеть	Способностью формулировать принципы эксплуатации систем и средств обеспечения информационной безопасности
Базовый уровень освоения компетенции	
Знать	Перечень работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности
Уметь	Составлять перечень работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности
Владеть	Навыками ввода в эксплуатацию систем и средств обеспечения информационной безопасности
Высокий уровень освоения компетенции	
Знать	Организацию работ по вводу в эксплуатацию систем и средств обеспечения информационной
Уметь	Организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности
Владеть	Методами организации выполнения работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности

ПСК-4.5**:** способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем	
Минимальный уровень освоения компетенции	
Знать	Основные протоколы и сервисы идентификации и аутентификации абонентов и объектов сети;
Уметь	Моделировать работу криптографических протоколов;
Владеть	Навыками практического применения криптографических протоколов и стандартов
Базовый уровень освоения компетенции	
Знать	Российские и международные стандарты, описывающие криптографические функции;
Уметь	Определять перечень нормативных актов и руководящих документов по использованию криптографических протоколов;
Владеть	Специальной терминологией;
Высокий уровень освоения компетенции	
Знать	Стандартные криптопротоколы протоколы
Уметь	Применять криптопротоколы и стандарты на практике
Владеть	Навыками подбора программных и аппаратных средств, использующих криптопротоколы и стандарты

В результате освоения дисциплины обучающийся должен

Знать

1. Российские и международные стандарты, описывающие криптографические функции;

2. Основные протоколы и сервисы идентификации и аутентификации абонентов и объектов сети

Уметь

1. Определять перечень нормативных актов и руководящих документов по использованию криптографических протоколов;
2. Моделировать работу криптографических протоколов;

Владеть

1. Специальной терминологией;
2. Навыками практического применения криптографических протоколов и стандартов.

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	Раздел 1. Криптографические протоколы и сервисы идентификации и аутентификации абонентов и объектов сети				
1.1	Введение. Определения, цели, задачи дисциплины. Основные термины и определения /Лек/	9	2	ПСК-4.1	Л1.1, Л1.2, Л2.1, Э2
1.2	Аутенфикация на основе паролей /Лек/	9	2	ПСК-4.1	Л1.1, Л1.2, Л2.1,
1.3	Аутентификация Kerberos/Лек/	9	2	ПСК-4.1	Л1.1, Л1.2, Э1, Э2
1.4	Изучение механизмов аутенфикации, использующих криптографические протоколы /Ср/	9	12	ПСК-4.1	Л1.3, Л2.1, Э1, Э2
1.5	Программная реализация алгоритма DES /Лр/	9	9	ПК-9, ПСК-4.1	Л1.2, Л2.2, Э1, Э2
1.6	Механизмы одноразовой аутенфикации /См/	9	6	ПСК-4.1	Л1.2, Л2.2, Э2
1.7	Подготовка к текущему контролю (защита лабораторной работы)/Ср/	9	4	ПК-9, ПСК-4.1	Л1.1, Л1.2, Л2.1, Л2.3, Э1,
	Раздел 2. Инфраструктура открытых ключей				
2.1	Криптографическая система с открытым ключом /Лек/	9	2	ПСК-4.5	Л1.1, Л2.2, Э1, Э2
2.2	Программная реализация алгоритма RSA /Лр/	9	9	ПСК-4.5	Л1.1, Л1.2, Э1, Э2
2.3	Подготовка к текущему контролю (защита лабораторной работы) /Ср/	9	4	ПСК-4.5	Л1.1, Л2.2, Э1, Э2
2.4	Основные компоненты PKI /Лек/	9	2	ПСК-4.5	Л1.2, Л2.2, Э2
2.5	Базовые криптографические механизмы сервисов безопасности PKI /Лек/	9	4	ПСК-4.5	Л1.2, Л2.2, Э2
	Раздел 3. Национальные криптографические стандарты				
3.1	Национальные криптографические стандарты /Лек/	9	2	ПСК-4.5	Л1.1, Л1.2, Л2.2, Л2.3, Э1, Э2
3.2	Нормативная база по использованию ЭП в РФ /Лек/	9	2	ПСК-4.5	
3.3	Анализ политик безопасности удостоверяющих центров /Ср/	9	12	ПСК-4.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1, Э2
3.4	Требования ГОСТ к криптографическим протоколам /См/	9	6	ПСК-4.5	Л1.1, Л1.2, Л2.1, Л2.2, Э1
3.5	Решения для построения удостоверяющих центров/См/	9	6	ПСК-4.5	Л1.2, Л2.2, Э2
3.6	Подготовка к текущему контролю (защита лабораторной работы)/Ср/	9	4	ПК-9, ПСК-4.1, ПСК-4.5	Л1.1, Л1.2, Л2.1, Э1, Э2

3.7	Подготовка к зачету /Ср/	9	18		
	Зачет по дисциплине	9		ПК-9, ПСК-4.1, ПСК-4.5	Л1.1, Л1.2, Л2.1, Л2.2, , Э1, Э2

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

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

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

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л1.1	Лапонина О.Р.	Криптографические основы безопасности / О.Р. Лапонина. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. : ил. - (Основы информационных технологий). - Библиогр. в кн. - ISBN 5-9556-00020-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429092 (13.09.2017).	М.: НОУ «ИНТУИТ», 2016	100 % онлайн
Л1.2	Трипкош В.А.	Электронная цифровая подпись в деятельности предприятий и организаций : учебное пособие / В.А. Трипкош, А.Г. Матвеев ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2012. - 172 с. : схем., ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=270314 (13.09.2017).	Оренбург : ОГУ, 2012	100 % онлайн

6.1.2 Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/ 100% онлайн
Л2.1	Афанасьев А.А., Веденьев Л.Т., Воронцов А.А.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: для ВПО: Учебное пособие для вузов http://e.lanbook.com/books/element.php?pl1_id=5114	М.: Горячая линия-Телеком, 2012	100 % онлайн
Л2.2	Полянская О.Ю.	Инфраструктуры открытых ключей : учебное пособие / О.Ю. Полянская, В.С. Горбатов. - М. : Интернет-	М. : Интернет-Университет	100% онлайн

		Университет Информационных Технологий, 2007. - 368 с. : табл. - (Основы информационных технологий). - ISBN 978-5-9556-0081-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233206 (13.09.2017).	Информационных Технологий, 2007.	
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л3.1	Калмыков И.А., Науменко Д.О.	Криптографические методы защиты информации : лабораторный практикум / Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет», Министерство образования и науки Российской Федерации ; авт.-сост. И.А. Калмыков, Д.О. Науменко и др. - Ставрополь : СКФУ, 2015. - 109 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458059 (13.09.2017).	Ставрополь : СКФУ, 2015	100 % онлайн
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/ 100% онлайн
Л4.1	Басалова Г.В.	Основы криптографии : курс лекций / Г.В. Басалова ; Национальный Открытый Университет "ИНТУИТ". - М. : Интернет-Университет Информационных Технологий, 2011. - 253 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233689 (13.09.2017).	М. : Интернет-Университет Информационных Технологий, 2011	100 % онлайн
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э.1	pravo.gov.ru			
Э.2	fsb.ru			
6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)				
6.3.1 Перечень базового программного обеспечения				
6.3.1.1	ОС Microsoft Windows XP Professional, количество – 227, лицензия № 44718499; ОС Microsoft Windows 7 Professional, количество – 100, лицензия № 49379844			
6.3.1.2	Офисный пакет Microsoft Office 2010, количество – 155, Лицензия № 48288083; Libre Office v. 5.2, свободно распространяемое ПО, https://ru.libreoffice.org			
6.3.2 Перечень специализированного программного обеспечения				
6.3.2.1	Microsoft PowerPoint Viewer 2007, бесплатно, количество не ограничено.			
6.3.2.2	Borland Delphi 7			
6.3.3 Перечень информационных справочных систем				
6.3.3.1	«Консультант +» http://www.consultant.ru/			
6.3.3.2	ЭБС ИрГУПС http://www.irgups.ru/htb/;			
6.3.3.3	ЭБС издательства «Лань» http://www.e.lanbook.com;			
6.3.3.4	ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru;			

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	
1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л – по адресу г. Иркутск, ул. Лермонтова, д.80.
	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации).
2	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
3	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.
5	Помещение для хранения и профилактического обслуживания учебного оборудования – А-521.

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ	
1	Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых проектов, работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа имеются учебно-наглядные пособия (презентации).
2	Учебные лаборатории Д-523 «Средства и методы защиты информации», Д-525 «Средства и методы защиты информации».
3	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ	
Вид учебной деятельности	*Организация учебной деятельности обучающегося*
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки. Обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии. Уделить внимание следующим понятиям (перечисление понятий) и др.
Реферат	Реферат – краткое письменное изложение материала по определенной теме, выполняется; цель – привить обучающимся навыков самостоятельного поиска и анализа информации, формирования умения подбора и изучения литературных источников, используя при этом дополнительную научную, методическую и периодическую литературу. Реферат – это самостоятельная учебно-исследовательская работа обучающегося, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание материала должно быть логичным,

	изложение материала носит проблемно-поисковый характер. Ознакомиться со структурой и оформление реферата (Положение «Требования к оформлению текстовой и графической документации. Нормоконтроль» № П.420700.05.4.092-2012 в последней редакции).
Домашнее задание (самостоятельная работа студента)	Для успешного выполнения домашних занятий, студенту необходимо обратиться к лекционному материалу, основным и дополнительным источникам литературы, указанным в рабочей программе. Если этого будет не достаточно для выполнения поставленного задания, необходимо в обязательном порядке посетить консультацию преподавателя.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

Приложение 1 к рабочей программе по дисциплине Б1.Б.1.ДС.02 «Криптографические протоколы и стандарты»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.Б.1.ДС.02 «Криптографические протоколы и стандарты»

1 Перечень компетенций с указанием этапов их формирования

в процессе освоения образовательной программы

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

ПК-9: способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности

ПСК-4.1: способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем

ПСК-4.5: способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем

Таблица траекторий формирования у обучающихся компетенций ПК-9, ПСК-4.1, ПСК-4.5

при освоении образовательной программы

Код компе-тенции	Наименование компетенции	Индекс и наименование дисциплин (модулей)/ практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Б1.Б.1.ДС.01 Открытые информационные системы	7	7
		Б1.Б.1.ДС.02 Криптографические протоколы и стандарты	8	8
		Б2.Б.05(П) Производственная - технологическая	10	10
ПСК-4.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных	Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	10	10
		Б1.Б.1.ДС.02 Криптографические протоколы и стандарты	8	8
		Б1.Б.1.27 Организационное и правовое обеспечение информационной безопасности	8	8
		Б1.Б.1.ДС.05 Аудит информационных технологий и систем обеспечения информационной безопасности	9	9
		Б2.Б.06(Пд) Производственная - преддипломная	10	10
ПСК-4.5	способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические	Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	10	10
		Б1.Б.1.ДС.01 Открытые информационные системы	7	7
		Б1.Б.1.ДС.02 Криптографические протоколы и стандарты	8	8
		Б1.В.ДВ.04.02 Защита и обработка	9	9

	приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем	конфиденциальных документов		
		Б1.Б.1.ДС.03 Информационная безопасность открытых систем	9	9
		Б1.Б.1.ДС.04 Виртуальные частные сети	9	9
		Б1.В.ДВ.04.01 Защита электронного документооборота	9	9
		Б2.Б.06(Пд) Производственная - преддипломная	10	10
		Б2.Б.05(П) Производственная - технологическая	10	10

Таблица соответствия уровней освоения компетенций ПК-9, ПСК-4.1, ПСК-4.5 планируемым результатам обучения

Код компе-тенции	Наименование компетенции	Наименования разделов дисциплины (модуля)/практики	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-9	способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	Криптографические протоколы и сервисы идентификации и аутентификации абонентов и объектов сети Национальные криптографические стандарты	Минимальный уровень освоения компетенции	Знать Нормативные документы по разработке защищенных автоматизированных систем в сфере профессиональной деятельности Уметь Применять на практике нормативные документы по разработке защищенных автоматизированных систем в сфере профессиональной деятельности Владеть Навыками безопасного использования технических средств автоматизации
			Базовый уровень освоения компетенции	Знать Уровни защищенности АС Уметь Оценивать эффективность и надежность автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов Владеть Навыками применения криптопротоколов и стандартов для построения защищенных систем
			Высокий уровень освоения компетенции	Знать Методики оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов Уметь

				Применять на практике методики оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов Владеть Навыками документирования оценки защищенности автоматизированных систем на соответствие требованиям государственных или корпоративных нормативных документов
ПСК-4.1	способностью выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-)	Соединение локальных сетей	Минимальный уровень освоения компетенции	Знать Принципы эксплуатации систем и средств обеспечения информационной безопасности Уметь формулировать принципы эксплуатации систем и средств обеспечения информационной безопасности Владеть Способностью формулировать принципы эксплуатации систем и средств обеспечения информационной безопасности
			Базовый уровень освоения компетенции	Знать Перечень работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности Уметь Составлять перечень работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности Владеть Навыками ввода в эксплуатацию систем и средств обеспечения информационной безопасности
			Высокий уровень освоения компетенции	Знать Основные протоколы и сервисы идентификации и аутентификации абонентов и объектов сети Уметь Моделировать работу криптографических протоколов Владеть Навыками практического применения криптографических протоколов и стандартов
ПСК-4.5	способностью формировать и эффективно применять комплекс мер (правила, процедуры,		Минимальный уровень освоения компетенции	Знать Основные протоколы и сервисы идентификации и аутентификации абонентов и объектов сети Уметь Моделировать работу криптографических протоколов Владеть Навыками практического применения

	практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем			криптографических протоколов и стандартов
			Базовый уровень освоения компетенции	Знать Российские и международные стандарты, описывающие криптографические функции Уметь Определять перечень нормативных актов и руководящих документов по использованию криптографических протоколов Владеть Специальной терминологией
			Высокий уровень освоения компетенции	Знать Стандартные криптопротоколы протоколы Уметь Применять криптопротоколы и стандарты на практике Владеть Навыками подбора программных и аппаратных средств, использующих криптопротоколы и стандарты

Программа контрольно-оценочных мероприятий
за период изучения дисциплины

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
6 семестр					
1	28	Текущий контроль	Механизмы одноразовой аутенфикации /См/	ПСК-4.1	Сообщение, доклад
2	32	Текущий контроль	Программная реализация алгоритма DES /Лр/	ПК-9, ПСК-4.1	Защита ЛР (отчет, устный ответ на вопросы)
3	38	Текущий контроль	Программная реализация алгоритма RSA /Лр/	ПСК–4.5	Защита ЛР (отчет, устный ответ на вопросы)
4	40	Промежуточная аттестация – зачет	Разделы 1, 2, 3	ПК-9, ПСК-4.1 ПСК–4.5	Зачет

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

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

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

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

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
2	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите
3	Зачет (дифференцированный 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 (билетов) к зачету

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

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенций
«отлично»	«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
«хорошо»		Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
«удовлетворительно»		Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С	Минимальный

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

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Доклад, сообщение

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

Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»	Лабораторная работа выполнена с задержкой, письменный отчет с недочетами.

	Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.7 Перечень теоретических вопросов к зачету

1. Криптографическая система с открытым ключом
2. Инфраструктура открытых ключей
3. Схема цифровой подписи
4. Основные компоненты PKI
5. Взаимодействие компонентов PKI
6. Удостоверяющий центр
7. Регистрационный центр
8. Репозиторий сертификатов
9. Архив сертификатов
10. Серверные компоненты PKI
11. Сервисы PKI
12. Криптографические сервисы
13. Сервисы управления сертификатами
14. Вспомогательные сервисы
15. Сервисы, базирующиеся на PKI
16. Сервисы безопасности PKI
17. Идентификация и аутентификация
18. Целостность
19. Конфиденциальность
20. Виды ЭП
21. Обеспечение информационной безопасности УЦ
22. Симметричные алгоритмы шифрования
23. Асимметричные алгоритмы шифрования
24. Алгоритмы хэширования
25. Аутентификация на основе паролей
26. Механизмы одноразовой аутентификации
27. Аутентификация с использованием хэш-функции
28. S/Key One-Time Password System
29. Аутентификация Kerberos
30. Аутентификация при помощи сертификатов
31. Понятие криптографического протоколаОсновные атаки на безопасность протоколов
32. Свойства безопасности протоколов

3.8 Перечень типовых практических заданий к зачету

1. Перечислить число параметров в криптографической системе RSA.
2. Перечислить секретные параметры системы RSA.
3. Перечислить открытые параметры системы RSA.
4. Опишите схему шифрования текста с использованием алгоритма RSA.
5. Опишите схему дешифрования текста с использованием алгоритма RSA.
6. Опишите схему формирование цифровой подписи с применение алгоритма RSA.
7. Указать длину начального ключа в алгоритме DES.
8. Перечислить основные этапы формирование ключей в алгоритме DES.
9. Указать длину ключа при шифровании текста в алгоритме DES.
10. Сколько S-функций определено в алгоритме DES?
11. Какая арифметическая операции используется при преобразованиях в алгоритме DES. Укажите длину шифруемого блока в алгоритме DES.

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

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

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

Для организации и проведения промежуточной аттестации (в форме зачета/экзамена) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

– перечень теоретических вопросов к зачету/экзамену для оценки знаний;

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

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету/экзамену обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

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

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

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

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

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация в форме зачета проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач (не более двух теоретических и двух практических). Промежуточная аттестация в форме зачета с проведением аттестационного испытания в форме собеседования проходит на последнем занятии по дисциплине.

Темы эссе (рефератов, докладов, сообщений)

Перечень компетенций (части компетенции, элементов компетенции), проверяемых оценочным средством: ПСК-4.1

1. Механизмы одноразовой аутенфикации (сообщения готовятся по 4 различным алгоритмам одноразовой аутенфикации по выбору докладчика).