МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра информационной безопасности и систем связи

Авторы-составители: **Айдаров Юрий Рафаэлевич**
Шкарапута Александр Петрович
Мустакимова Яна Романовна

Рабочая программа дисциплины

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 68668

Утверждено
Протокол №1
от «31» августа 2020 г.

Пермь, 2020

1. Наименование дисциплины

Криптографические методы защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в базовую часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.03** Информационная безопасность автоматизированных систем специализация Безопасность открытых информационных систем

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Криптографические методы защиты информации** у обучающегося должны быть сформированы следующие компетенции:

10.05.03 Информационная безопасность автоматизированных систем (специализация : Безопасность открытых информационных систем)

ОПК.3 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности

ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы

ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем

ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности

ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы

ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем

ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем

4. Объем и содержание дисциплины

Направления подготовки	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	10
Объем дисциплины (з.е.)	7
Объем дисциплины (ак.час.)	252
Контактная работа с преподавателем (ак.час.), в том числе:	112
Проведение лекционных занятий	56
Проведение лабораторных работ, занятий по иностранному языку	56
Самостоятельная работа (ак.час.)	140
Формы текущего контроля	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (3)
Формы промежуточной аттестации	Экзамен (10 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Криптографические алгоритмы

ГОСТ 34.12-2018

Понятие блочного шифра. ГОСТ Р 34.12-2018 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры». Область применения, основные термины и определения. Алгоритм блочного шифрования с длиной блока 64 бит. Алгоритм блочного шифрования с длиной блока 128 бит.

ГОСТ 34.11-2018

Понятие хеш-функции. Применение хеш-функций. ГОСТ Р 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хеширования». Область применения, основные термины и определения. Процедура вычисления хеш-функции.

ГОСТ 34.10-2018

Понятие электронной подписи. Простая электронная подпись, усиленная неквалифицированная электронная подпись, усиленная квалифицированная электронная подпись. Использование электронной подписи. ГОСТ 34.10-2018 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Область применения, основные термины и определения. Генерация ключей. Формирование подписи. Проверка подписи.

Криптографически стойкие генераторы псевдослучайных чисел

Генератор псевдослучайных чисел. Критерии, которым должен удовлетворять генератор псевдослучайных чисел. Криптографически стойкий генератор псевдослучайных чисел. Требования к криптографически стойкому генератору псевдослучайных чисел. Классы реализации криптографически стойкого генератора псевдослучайных чисел: на основе криптографических алгоритмов, на основе вычислительно сложных математических задач, специальные реализации.

Парадокс дней рождения и его применение в криптографии

Парадокс дней рождения. Применение парадокса дней рождения для создания хеш-функций. Атака "дней рождения"

Криптографически стойкие хеш-функции

Криптографические хеш-функции. Принципы построения: итеративная последовательная схема, сжимающая функция на основе симметричного блочного алгоритма. Требования к криптогрфически стойким хеш-функциям. Понятие идеальной криптографической хеш-функции

Блочные шифры

Определение блочных шифров. Построение блочного шифра: итеративные блочные шифры, сеть Фейстеля. Режимы работы блочных шифров: шифрование независимыми блоками, шифрование, зависящее от предыдущих блоков, дополнение до целого блока. Криптоанализ блочных шифров. Атаки на блочные шифры.

MAC

Понятие имитовставки. Имитовставка по ГОСТ 34.13-2018 "Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров"

Криптосистема RSA

Факторизация целых чисел

Понятие факторизации натуральных чисел. Методы факторизации натуральных чисел: экспоненциальные алгоритмы и субэкспоненциальные алгоритмы. Примеры факторизации натуральных чисел. Перебор делителей. Алгоритм факторизации Ферма. Метод Полларда.

RSA

Алгоритм RSA. Генерация ключей RSA. Алгоритмы шифрования и дешифрования. Взаимная обратность отображений шифрования и дешифрования. Выбор параметров. Основные виды атак: атаки на основе алгоритмов разложения на множители, атаки на основе алгоритмов вычисления дискретного логарифма, атака Винера, атака на подпись RSA в схеме с нотариусом

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Фороузан Б. А. Криптография и безопасность сетей:учебное пособие [для вузов]/Б. А. Фороузан ; пер. с англ. А. Н. Берлина.-Москва:Интернет-Университет информационных технологий,2010, ISBN 978-5-9963-0242-0.-784.

2. Сонг Й. Ян Криптоанализ RSA:научное издание/Сонг Й. Ян:Институт компьютерных исследований,2011, ISBN 978-5-93972-873-7.-2851.-Библиогр.: с. 259-280 (337 назв.). - Предм. указ.: с. 281-285

3. Бабенко Л. К.,Ищуков С. С.,Макаревич О. Б. Защита информации с использованием смарт-карт и электронных брелоков/Л. К. Бабенко, С. С. Ищуков, О. Б. Макаревич.-М.:Гелиос АРВ,2003, ISBN 5-85438-093-5.-352.-Библиогр.: с. 348-349

Дополнительная:

1. Криптография и безопасность цифровых систем : учебное пособие / В. Г. Грибунин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко ; под редакцией А. И. Астайкин. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2011. — 411 c. — ISBN 978-5-9515-0166-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/60851.html

2. Романьков, В. А. Алгебраическая криптография : монография / В. А. Романьков. — Омск : Омский государственный университет им. Ф.М. Достоевского, 2013. — 136 c. — ISBN 978-5-7779-1600-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/24868

3. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; перевод В. А. Хорев ; под редакцией С. М. Молявко. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 480 c. — ISBN 978-5-00101-700-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/20709

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

crypto-class.org Cryptography I
http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
https://intuit.ru/studies/courses/691/547/info Основы криптографии
https://intuit.ru/studies/courses/552/408/lecture/9371?page=1 Криптографическая система RSA

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Криптографические методы защиты информации** предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «AdobeAcrobatReader DC»;
- офисный пакет приложений «LibreOffice».

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для лабораторных работ требуется компьютерный класс. Состав оборудования определен в Паспорте компьютерного класса.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными

компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Криптографические методы защиты информации

Планируемые результаты обучения по дисциплине для формирования компетенции и критерии их оценивания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	Знать этапы принятия решений при решении профессиональных задач. Уметь проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем. Владеть методами анализа и оценки уровня эффективности автоматизированных систем.	**Неудовлетворител** Не способен проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем. **Удовлетворительн** Способен со значительными затруднениями проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем. **Хорошо** Способен с незначительными затруднениями проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем. **Отлично** Способен без затруднений проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем.
ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы	Знать потенциальные уязвимости автоматизированных систем. Уметь проводить анализ рисков информационной безопасности автоматизированной системы. Владеть методами анализа рисков информационной безопасности автоматизированной системы.	**Неудовлетворител** Не способен проводить анализ рисков информационной безопасности автоматизированной системы. **Удовлетворительн** Способен со значительными затруднениями проводить анализ рисков информационной безопасности автоматизированной системы. **Хорошо** Способен с незначительными затруднениями проводить анализ рисков информационной

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо безопасности автоматизированной системы. **Отлично** Способен без затруднений проводить анализ рисков информационной безопасности автоматизированной системы.
ПК.18 способность проводить инструментальный мониторинг защищенности автоматизированных систем	Знать инструменты для мониторинга защищенности автоматизированных систем. Уметь проводить инструментальный мониторинг защищенности автоматизированных систем. Владеть навыками установки и настройки инструментов для мониторинга защищенности автоматизированных систем.	**Неудовлетворител** Не способен проводить инструментальный мониторинг защищенности автоматизированных систем. **Удовлетворительн** Способен со значительными затруднениями проводить инструментальный мониторинг защищенности автоматизированных систем. **Хорошо** Способен с незначительными затруднениями проводить инструментальный мониторинг защищенности автоматизированных систем. **Отлично** Способен без затруднений проводить инструментальный мониторинг защищенности автоматизированных систем.
ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать программно-аппаратные, криптографические и технические средства защиты информации. Уметь проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации Владеть методами оценки эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.	**Неудовлетворител** Не способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации. **Удовлетворительн** Способен со значительными затруднениями проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации. **Хорошо** Способен с незначительными затруднениями проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации. **Отлично** Способен без затруднений проводить контрольные проверки работоспособности и

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.
ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем	Знать основные требования безопасности автоматизированных систем. Уметь проводить синтез проектных решений по обеспечению безопасности автоматизированных систем. Владеть методами анализа проектных решений по обеспечению безопасности автоматизированных систем.	**Неудовлетворител** Не способен проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем. **Удовлетворительн** Способен со значительными затруднениями проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем. **Хорошо** Способен с незначительными затруднениями проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем. **Отлично** Способен без затруднений проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем.
ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать содержание модели угроз и модели нарушителя информационной безопасности. Уметь разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы. Владеть навыками разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы на практике.	**Неудовлетворител** Не способен разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы. **Удовлетворительн** Способен со значительными затруднениями разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы. **Хорошо** Способен с незначительными затруднениями разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы. **Отлично** Способен без затруднений разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.
ПК.23 способность разрабатывать проекты	Знать основные требования по обеспечению информационной безопасности	**Неудовлетворител** Не способен разрабатывать проекты нормативных и методических материалов,

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности	автоматизированных систем. Уметь разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем. Владеть навыками разработки положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности.	**Неудовлетворител** регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности. **Удовлетворительн** Способен со значительными затруднениями разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности. **Хорошо** Способен с незначительными затруднениями разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности. **Отлично** Способен без затруднений разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности.
ОПК.3 способность решать стандартные задачи профессиональной деятельности на основе	Знать основные требования информационной безопасности. Уметь решать стандартные задачи профессиональной деятельности на основе	**Неудовлетворител** Не способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	информационной и библиографической культуры. Владеть навыками решения профессиональных задач с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**Неудовлетворител** коммуникационных технологий и с учетом основных требований информационной безопасности. **Удовлетворительн** Способен со значительными затруднениями решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Хорошо** Способен с незначительными затруднениями решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **Отлично** Способен без затруднений решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Знать составляющие системы управления информационной безопасностью автоматизированной системы. Уметь принимать участие в проектировании системы управления информационной безопасностью автоматизированной системы. Владеть навыками проектирования системы управления информационной безопасностью автоматизированной системы.	**Неудовлетворител** Не способен участвовать в проектировании системы управления информационной безопасностью автоматизированной системы. **Удовлетворительн** Способен со значительными затруднениями участвовать в проектировании системы управления информационной безопасностью автоматизированной системы. **Хорошо** Способен с незначительными затруднениями участвовать в проектировании системы управления информационной безопасностью

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо автоматизированной системы. **Отлично** Способен без затруднений участвовать в проектировании системы управления информационной безопасностью автоматизированной системы.
ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы	Знать средства защиты информации и средства контроля защищенности автоматизированной системы. Уметь принимать участие в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы. Владеть навыками проектирования средств защиты информации и средств контроля защищенности автоматизированной системы.	**Неудовлетворител** Не способен участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы. **Удовлетворительн** Способен со значительными затруднениями участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы. **Хорошо** Способен с незначительными затруднениями участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы. **Отлично** Способен без затруднений участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы.
ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности	Знать защищенные автоматизированные системы. Уметь принимать участие в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности. Владеть навыками разработки защищенных автоматизированных систем по профилю своей профессиональной деятельности.	**Неудовлетворител** Не способен участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности. **Удовлетворительн** Способен со значительными затруднениями участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности. **Хорошо** Способен с незначительными затруднениями участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Способен без затруднений участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности.
ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности	Знать компоненты автоматизированных систем в сфере профессиональной деятельности. Уметь принимать участие в разработке компонентов автоматизированных систем в сфере профессиональной деятельности. Владеть навыками разработки компонентов автоматизированных систем в сфере профессиональной деятельности.	**Неудовлетворител** Не способен участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности. **Удовлетворительн** Способен со значительными затруднениями участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности. **Хорошо** Способен с незначительными затруднениями участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности. **Отлично** Способен без затруднений участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

Вид мероприятия промежуточной аттестации : Экзамен
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 47 до 60
«неудовлетворительно» / «незачтено» менее 47 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем **ПК.10** способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности **ПК.11** способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности **ПК.18** способность проводить инструментальный мониторинг защищенности автоматизированных систем	ГОСТ 34.12-2018 **Письменное контрольное мероприятие**	Знание основных положений ГОСТ 34.12-2018. Реализация алгоритмов блочного шифрования в соответствии с ГОСТ 34.12-2018

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы **ПК.7** способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем **ПК.9** способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем **ПК.23** способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности	ГОСТ 34.11-2018 **Письменное контрольное мероприятие**	Знание понятия хеш-функция. Знание основных положений ГОСТ Р 34.11-2018. Реализация хеш-функции в соответствии с ГОСТ Р 34.11-2018.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы **ПК.7** способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем **ПК.11** способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности **ПК.13** способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	ГОСТ 34.10-2018 **Письменное контрольное мероприятие**	Знание понятия электронной подписи. Знание основных положений ГОСТ 34.10-2018. Реализация формирования и проверки электронной подписи в соответствии с ГОСТ 34.10-2018.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.3 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **ПК.7** способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем **ПК.14** способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы **ПК.15** способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	RSA **Итоговое контрольное мероприятие**	Знание алгоритма RSA, реализация алгоритма RSA на одном из языков программирования

Спецификация мероприятий текущего контроля

ГОСТ 34.12-2018

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **10**

Показатели оценивания	Баллы
Реализация алгоритма блочного шифрования с длиной блока 128 бит.	8
Реализация алгоритма блочного шифрования с длиной блока 64 бит.	7

Знание основных положений ГОСТ 34.12-2018.	5

ГОСТ 34.11-2018

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **10**

Показатели оценивания	Баллы
Реализация хеш-функции в соответствии с ГОСТ Р 34.11-2018.	15
Знание понятия хеш-функция. Знание основных положений ГОСТ Р 34.11-2018.	5

ГОСТ 34.10-2018

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **10**

Показатели оценивания	Баллы
Реализация формирования и проверки электронной подписи в соответствии с ГОСТ 34.10-2018.	15
Знание понятия электронной подписи. Знание основных положений ГОСТ 34.10-2018.	5

RSA

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Реализация алгоритма RSA на одном из языков программирования	20
Знание алгоритма RSA, алгоритмов шифрования и дешифрования	10
Знание основных видов атак на RSA	10