

МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

Авторы-составители: **Мустакимова Яна Романовна
Шкарапута Александр Петрович
Черников Арсений Викторович**

Рабочая программа дисциплины

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 94116

Утверждено
Протокол №6
от «26» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Криптографические методы защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную 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	10,11
Объем дисциплины (з.е.)	6
Объем дисциплины (ак.час.)	216
Контактная работа с преподавателем (ак.час.), в том числе:	84
Проведение лекционных занятий	28
Проведение лабораторных работ, занятий по иностранному языку	56
Самостоятельная работа (ак.час.)	132
Формы текущего контроля	Защищаемое контрольное мероприятие (5) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (10 триместр) Экзамен (11 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

1 триместр

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"

2 триместр

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.

Алгоритм 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.

Атаки, связанные с особенностями реализации криптосистем

Пассивные и активные атаки. Атаки только зашифрованным текстом. Известная атака открытого текста. Выбранная атака открытым текстом. Атака по словарю. Атака грубой силы. Атака "человек посередине". Атаки по времени.

Итоговое контрольное мероприятие

Итоговое контрольное мероприятие по всем пройденным темам курса

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. Романьков, В. А. Алгебраическая криптография : монография / В. А. Романьков. — Омск : Омский государственный университет им. Ф.М. Достоевского, 2013. — 136 с. — ISBN 978-5-7779-1600-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/24868>
2. Сонг Й. Ян Криптоанализ RSA/Сонг Й. Ян:Институт компьютерных исследований,2011, ISBN 978-5-93972-873-7.-Библиогр.: с. 259-280 (337 назв.). - Предм. указ.: с. 281-285

Дополнительная:

1. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/102017.html>
2. 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 с. — 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

<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-образовательную среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:

- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader 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 компьютерами 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.
Индикаторы и критерии их оценивания**

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>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</p>	<p>Знать основные требования информационной безопасности. Уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры. Владеть навыками решения профессиональных задач с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p>	<p style="text-align: center;">Неудовлетворител Не способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.</p> <p style="text-align: center;">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.</p> <p style="text-align: center;">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.</p> <p style="text-align: center;">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.</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично безопасности.

ПК.7

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

Компетенция (индикатор)	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.	<p>Неудовлетворител Не способен проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем.</p> <p>Удовлетворительн Способен со значительными затруднениями проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем.</p> <p>Хорошо Способен с незначительными затруднениями проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем.</p> <p>Отлично Способен без затруднений проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p>

ПК.6

способность проводить анализ рисков информационной безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.6 способность проводить	Знать потенциальные уязвимости	<p>Неудовлетворител Не способен проводить анализ рисков</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
анализ рисков информационной безопасности автоматизированной системы	автоматизированных систем. Уметь проводить анализ рисков информационной безопасности автоматизированной системы. Владеть методами анализа рисков информационной безопасности автоматизированной системы.	Неудовлетворител 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 безопасности автоматизированной системы. Отлично Способен без затруднений проводить анализ рисков информационной безопасности автоматизированной системы.

ПК.18

способность проводить инструментальный мониторинг защищенности автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
------------------------------------	--	---

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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 программноаппаратных, криптографических и технических средств защиты информации Владеть методами оценки эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.	<p>Неудовлетворител Не способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Удовлетворительн Способен со значительными затруднениями проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Хорошо Способен с незначительными затруднениями проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</p> <p>Отлично Способен без затруднений проводить контрольные проверки работоспособности и эффективности применяемых программноаппаратных, криптографических и технических средств защиты информации.</p>

ПК.9

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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	<p>Неудовлетворител Не способен проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем.</p> <p>Удовлетворительн Способен со значительными затруднениями проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем.</p> <p>Хорошо Способен с незначительными затруднениями</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Хорошо проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем.</p> <p>Отлично Способен без затруднений проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем.</p>

ПК.5

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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.	<p>Неудовлетворител Не способен разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.</p> <p>Удовлетворительн Способен со значительными затруднениями разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.</p> <p>Хорошо Способен с незначительными затруднениями разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.</p> <p>Отлично Способен без затруднений разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.</p>

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.23 способность разрабатывать проекты	Знать основные требования по обеспечению информационной безопасности	<p>Неудовлетворител Не способен разрабатывать проекты нормативных и методических материалов,</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>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</p>	<p>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.</p>	<p>Неудовлетворител регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности.</p> <p>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.</p> <p>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.</p> <p>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.</p>

ПК.13

способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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 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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Хорошо защищенности автоматизированной системы.</p> <p>Отлично Способен без затруднений участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы.</p>

ПК.10

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p>	<p>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</p>	<p>Неудовлетворител Не способен участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p>Удовлетворительн Способен со значительными затруднениями участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности.</p> <p>Хорошо Способен с незначительными затруднениями участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности.</p> <p>Отлично Способен без затруднений участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p>

ПК.11

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.11 способность участвовать в</p>	<p>Знать компоненты автоматизированных систем в сфере профессиональной</p>	<p>Неудовлетворител Не способен участвовать в разработке компонентов автоматизированных систем в</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
разработке компонентов автоматизированных систем в сфере профессиональной деятельности	<p>деятельности. Уметь принимать участие в разработке компонентов автоматизированных систем в сфере профессиональной деятельности. Владеть навыками разработки компонентов автоматизированных систем в сфере профессиональной деятельности.</p>	<p>Неудовлетворител сфере профессиональной деятельности.</p> <p>Удовлетворительн Способен со значительными затруднениями участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности.</p> <p>Хорошо Способен с незначительными затруднениями участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности.</p> <p>Отлично Способен без затруднений участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности.</p>

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Зачет

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 43 до 60

«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы 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	ГОСТ 34.12-2018 Защищаемое контрольное мероприятие	Знание основных положений ГОСТ 34.12-2018. Реализация алгоритмов блочного шифрования в соответствии с ГОСТ 34.12-2018

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>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</p> <p>ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p>	<p>ГОСТ 34.11-2018</p> <p>Защищаемое контрольное мероприятие</p>	<p>Знание понятия хеш-функция. Знание основных положений ГОСТ Р 34.11-2018. Реализация хеш-функции в соответствии с ГОСТ Р 34.11-2018.</p>
<p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p>	<p>ГОСТ 34.10-2018</p> <p>Защищаемое контрольное мероприятие</p>	<p>Знание понятия электронной подписи. Знание основных положений ГОСТ 34.10-2018. Реализация формирования и проверки электронной подписи в соответствии с ГОСТ 34.10-2018.</p>

Спецификация мероприятий текущего контроля

ГОСТ 34.12-2018

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

Показатели оценивания	Баллы
Реализация алгоритма блочного шифрования с длиной блока 64 бит.	15
Реализация алгоритма блочного шифрования с длиной блока 128 бит.	15
Знание основных положений ГОСТ 34.12-2018.	10

ГОСТ 34.11-2018

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

Показатели оценивания	Баллы
Реализация хеш-функции в соответствии с ГОСТ Р 34.11-2018.	20
Знание понятия хеш-функция. Знание основных положений ГОСТ Р 34.11-2018.	10

ГОСТ 34.10-2018

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

Показатели оценивания	Баллы
Реализация формирования и проверки электронной подписи в соответствии с ГОСТ 34.10-2018.	20
Знание понятия электронной подписи. Знание основных положений ГОСТ 34.10-2018	10

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 43 до 60

«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
----------------------------	----------------------------------	---

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p>ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности</p>	<p>Алгоритм RSA</p> <p>Защищаемое контрольное мероприятие</p>	<p>Знание алгоритма RSA, реализация алгоритма RSA на одном из языков программирования</p>
<p>ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы</p> <p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы</p> <p>ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы</p>	<p>Атаки, связанные с особенностями реализации криптосистем</p> <p>Защищаемое контрольное мероприятие</p>	<p>Знание основных атак на криптосистемы.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>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</p> <p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p>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</p>	<p>Итоговое контрольное мероприятие</p> <p>Итоговое контрольное мероприятие</p>	<p>Итоговая контрольная работа по проверке: знаний основных положений ГОСТ 34.12-2018, реализации алгоритмов блочного шифрования в соответствии с ГОСТ 34.12-2018; знаний понятия хеш-функций, основных положений ГОСТ Р 34.11-2018, реализации хеш-функции в соответствии с ГОСТ Р 34.11-2018; знаний понятия электронной подписи, основных положений ГОСТ 34.10-2018, реализации формирования и проверки электронной подписи в соответствии с ГОСТ 34.10-2018; знаний алгоритма RSA и его реализации на одном из языков программирования; знаний основных атак на криптосистемы.</p>

Спецификация мероприятий текущего контроля

Алгоритм RSA

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

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

Атаки, связанные с особенностями реализации криптосистем

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

Показатели оценивания	Баллы
Знание атаки "человек посередине"	10
Знание атак открытым текстом	10
Знание атак только зашифрованным текстом	10

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

Показатели оценивания	Баллы
Знание основных положений ГОСТ по криптографической защите информации	15
Знание алгоритма RSA, основных видов атак на RSA	15
Знание основных понятий и определений	10