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**
Черников Арсений Викторович
Мустакимова Яна Романовна

Рабочая программа дисциплины

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 31625

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: **10.05.01** Компьютерная безопасность

специализация Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

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

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

ПК.19 Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем

ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами

ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности

ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

ПСК.5 способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах

4. Объем и содержание дисциплины

Направления подготовки	10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	10,11
Объем дисциплины (з.е.)	7
Объем дисциплины (ак.час.)	252
Контактная работа с преподавателем (ак.час.), в том числе:	98
Проведение лекционных занятий	42
Проведение лабораторных работ, занятий по иностранному языку	56
Самостоятельная работа (ак.час.)	154
Формы текущего контроля	Защищаемое контрольное мероприятие (5) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (10 триместр) Экзамен (11 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Криптографические методы защиты информации.Первый триместр

Основные понятия криптографии

Предмет и задачи криптографии. Основные понятия криптографии: шифр, алфавит, ключ, система шифрования, криптостойкость, криптографическая система защиты информации, атака, криптографический протокол. Требования к криптографическим системам защиты информации.

Симметричные алгоритмы шифрования

Блочные и потоковые симметричные алгоритмы шифрования. Общая схема. Виды симметричных шифров.

ГОСТ 34.12-2018

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.

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.

ГОСТ Р 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.

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.

Алгоритмы электронной подписи

Понятие электронной подписи. Простая электронная подпись, усиленная неквалифицированная электронная подпись, усиленная квалифицированная электронная подпись. Использование электронной подписи. Основные криптопримитивы и протоколы, с помощью которых формируется электронная подпись.

ГОСТ Р 34.10-2018

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.

-

-

-

Криптографические методы защиты информации. Второй триместр

Криптосистема 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.

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. — М.: Интернет-Университет Информационных Технологий, БИНОМ. Лаборатория знаний, 2010. — 784 с. : ил., табл. — (Основы информационных технологий). — ISBN 978-5-9963-0242-0. — Текст : электронный // Электронно-библиотечная система БиблиоТех : [сайт]. https://psu.bibliotech.ru/Reader/Book/8789

Дополнительная:

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. Основы криптографии:учеб. пособие для студентов вузов, обучающихся по группе спец. в обл. информ. безопасности/А. П. Алферов [и др.].-3-е изд., испр. и доп..-М.:Гелиос АРВ,2005, ISBN 5-85438-137-0.-480.-Библиогр.: с. 469-475

3. Бабаш А. В.История криптографии Ч. 1/А. В. Бабаш, Г. П. Шанкин.-М.:Гелиос АРВ,2002, ISBN 5-85438-043-9.-240.-Библиогр.: с. 237-239

4. Росошек С. К.Специальные главы математики (Математические основы криптографии).учеб. пособие Ч. 1/М-во образования РФ, Томск. гос. ун-т систем управления радиоэлектроники,2004.-93

5. Осипян В. О.,Осипян К. В. Криптография в задачах и упражнениях/В. О. Осипян, К. В. Осипян.-М.:Гелиос АРВ,2004, ISBN 5-85438-009-9.-144.-Библиогр.: с. 139

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://eprint.iacr.org/ Электронные публикации международной ассоциации криптологов
http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

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 проведения лабораторных работ - аудитория Лаборатории Информационной безопасности: аппаратные и программные средства определены паспортом лаборатории.
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.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

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. Индикаторы и критерии их оценивания

ПК.3

Способность к анализу и формализации поставленных задач в области информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности	Знать методы анализа и формализации поставленных задач в области информационной безопасности. Уметь анализировать и формализировать поставленные задачи в области информационной безопасности. Владеть методами анализа и формализации поставленных задач в области информационной безопасности.	**Неудовлетворител** Не способен к анализу и формализации поставленных задач в области информационной безопасности **Удовлетворительн** Способен со значительными затруднениями к анализу и формализации поставленных задач в области информационной безопасности **Хорошо** Способен с незначительными затруднениями к анализу и формализации поставленных задач в области информационной безопасности **Отлично** Способен без затруднений к анализу и формализации поставленных задач в области информационной безопасности

ПК.23

Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Знать способы защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами. Уметь защищать информацию техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными	**Неудовлетворител** Не способен организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами **Удовлетворительн** Способен со значительными затруднениями организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	системами. Владеть навыками организации защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами.	**Удовлетворительн** работе с компьютерными системами **Хорошо** Способен с незначительными затруднениями организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами **Отлично** Способен без затруднений организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами

ПК.11

способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи	Знать методы оценивания степени надежности выбранных механизмов обеспечения безопасности. Уметь применять методы оценивания степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи.	**Неудовлетворител** Не способен оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **Удовлетворительн** Способен со значительными затруднениями оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **Хорошо** Способен с незначительными затруднениями оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **Отлично** Способен без затруднений оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

ПК.19

Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.19 Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем	Знать компоненты системы обеспечения информационной безопасности компьютерных систем. Уметь эксплуатировать системы обеспечения информационной безопасности компьютерных систем. Владеть навыками эксплуатации системы обеспечения информационной безопасности компьютерных систем.	**Неудовлетворител** Не способен принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем **Удовлетворительн** Способен со значительными затруднениями принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем **Хорошо** Способен с незначительными затруднениями принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем **Отлично** Способен без затруднений принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем

ПК.7

Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	Знать уровни обеспечения информационной безопасности компьютерных систем. Уметь выбрать рациональное решение по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований и обосновать его.	**Неудовлетворител** Не способен провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **Удовлетворительн** Способен со значительными затруднениями провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **Хорошо** Способен с незначительными затруднениями

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **Отлично** Способен без затруднений провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

ПК.10

Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	Знать способы разработки системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, способы разработки формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; владеть этими способами и уметь их применять на практике	**Неудовлетворител** Не способен участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **Удовлетворительн** Способен со значительными затруднениями участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **Хорошо** Способен с незначительными затруднениями участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **Отлично** Способен без затруднений участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

ПСК.5

способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПСК.5 способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах	Знать новые образцы программных средств защиты в компьютерных системах. Уметь оценить эффективность новых образцов программных средств защиты в компьютерных системах. Владеть методами оценивания эффективности новых образцов программных средств защиты в компьютерных системах.	**Неудовлетворител** Не способен оценивать эффективность новых образцов программных средств защиты в компьютерных системах **Удовлетворительн** Способен со значительными затруднениями оценивать эффективность новых образцов программных средств защиты в компьютерных системах **Хорошо** Способен с незначительными затруднениями оценивать эффективность новых образцов программных средств защиты в компьютерных системах **Отлично** Способен без затруднений оценивать эффективность новых образцов программных средств защиты в компьютерных системах

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Очная 2019

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 44 до 60
«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности **ПСК.5** способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах **ПК.7** Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	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
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности **ПСК.5** способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах **ПК.7** Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	ГОСТ Р 34.11-2018 **Защищаемое 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 (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности **ПСК.5** способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах **ПК.7** Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	ГОСТ Р 34.10-2018 **Защищаемое 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.

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: **18**

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 Р 34.11-2018

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый 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 Р 34.10-2018

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый 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 45 до 60
«неудовлетворительно» / «незачтено» менее 45 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **ПК.11** способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **ПК.19** Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем	Криптосистема RSA **Защищаемое контрольное мероприятие**	Знание алгоритма RSA, реализация алгоритма RSA на одном из языков программирования

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **ПК.11** способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **ПК.19** Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем	Атаки, связанные с особенностями реализации криптосистем **Защищаемое контрольное мероприятие**	Знание основных атак накриптосистемы.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **ПК.11** способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **ПК.19** Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем	Итоговый контроль **Итоговое контрольное мероприятие**	Итоговая контрольная работа по всем пройденным темам курса

Спецификация мероприятий текущего контроля

Криптосистема RSA

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Реализация алгоритма RSA на одном из языков программирования	10
Знание алгоритма RSA, алгоритмов шифрования и дешифрования	5
Знание основных видов атак на RSA	5

Атаки, связанные с особенностями реализации криптосистем

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **18**

Показатели оценивания	Баллы
Знание атак только зашифрованным текстом	10
Знание атак открытым текстом	10
Знание атаки по словарю и атаки грубой силы	10
Знание атаки "человек посередине"	10

Итоговый контроль

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **18**

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