МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

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

Рабочая программа дисциплины

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 73104

Утверждено
Протокол №6
от «06» мая 2022 г.

Пермь, 2022

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.9 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Индикаторы

ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации

ОПК.9.2 Анализирует возможности криптографических средств защиты информации

ОПК.9.3 Применяет методы и средства криптографической защиты информации для решения профессиональных задач

4. Объем и содержание дисциплины

Специальность	10.05.03 Информационная безопасность автоматизированных систем (специализация: Безопасность открытых информационных систем)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	7,8
Объем дисциплины (з.е.)	8
Объем дисциплины (ак.час.)	288
Контактная работа с преподавателем (ак.час.), в том числе:	144
Проведение лекционных занятий	72
Проведение практических занятий, семинаров	72
Самостоятельная работа (ак.час.)	144
Формы текущего контроля	Защищаемое контрольное мероприятие (5) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (7 семестр) Экзамен (8 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

Криптографические методы защиты информации. Первый семестр

В рамках первого семестра курса «Криптографические методы защиты информации» студент должен научиться основным принципам построения математических преобразований информации, обеспечивающих конфиденциальность, аутентичность или контроль целостности информации.

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 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.

ГОСТ Р 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"

Криптографические методы защиты информации. Второй семестр

В рамках второго семестра курса «Криптографические методы защиты информации» студент должен научиться основным принципам построения математических преобразований информации, обеспечивающих конфиденциальность, аутентичность или контроль целостности информации.

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.

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

2. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. — Москва : СОЛОН-Пресс, 2016. — 256 c. — ISBN 5-98003-002-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/90248

Дополнительная:

1. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си/Ред. пед. П. В. Семьянов.-М.:Триумф,2003, ISBN 5-89392-055-4.-816.-Библиогр.: с. 741-797

2. 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

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
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 «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 проведения практических занятий - 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

ОПК.9

Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации	Знать основные методы и средства криптографической защиты информации. Уметь находить информацию о существующих методах и средствах криптографической защиты информации. Владеть навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации.	**Неудовлетворител** Не знает основные методы и средства криптографической защиты информации. Не умеет находить информацию о существующих методах и средствах криптографической защиты информации. Не владеет навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации. **Удовлетворительн** Знает основные методы и средства криптографической защиты информации. Умеет находить информацию о существующих методах и средствах криптографической защиты информации. Не владеет навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации. **Хорошо** Знает основные методы и средства криптографической защиты информации. Умеет находить информацию о существующих методах и средствах криптографической защиты информации. Не владеет в полной мере навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации. **Отлично** Знает основные методы и средства криптографической защиты информации. Умеет находить информацию о существующих методах и средствах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично криптографической защиты информации. Владеет в полной мере навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации.
ОПК.9.2 Анализирует возможности криптографических средств защиты информации	Знать существующие криптографические средства защиты информации. Уметь анализировать возможности криптографических средств защиты информации. Владеть навыками анализа при выборе криптографических средств защиты информации при решении практических заданий.	**Неудовлетворител** Не знает существующие криптографические средства защиты информации. Не умеет анализировать возможности криптографических средств защиты информации. Не владеет навыками анализа при выборе криптографических средств защиты информации при решении практических заданий. **Удовлетворительн** Знает существующие криптографические средства защиты информации. Не умеет анализировать возможности криптографических средств защиты информации. Не владеет навыками анализа при выборе криптографических средств защиты информации при решении практических заданий. **Хорошо** Знает существующие криптографические средства защиты информации. Умеет анализировать возможности криптографических средств защиты информации. Не владеет в полной мере навыками анализа при выборе криптографических средств защиты информации при решении практических заданий. **Отлично** Знает существующие криптографические средства защиты информации. Умеет анализировать возможности криптографических средств защиты информации. Владеет в полной мере навыками анализа при выборе криптографических средств защиты информации при решении

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично практических заданий.
ОПК.9.3 Применяет методы и средства криптографической защиты информации для решения профессиональных задач	Знать существующие средства криптографической защиты информации. Уметь делать выбор средств криптографической защиты информации в соответствии с целями профессиональных задач, и обосновывать его. Владеть навыками применения методов и средств криптографической защиты информации для решения профессиональных задач.	**Неудовлетворител** Не знает существующие средства криптографической защиты информации. Не умеет делать выбор средств криптографической защиты информации в соответствии с целями профессиональных задач, и обосновывать его. Не владеет навыками применения методов и средств криптографической защиты информации для решения профессиональных задач. **Удовлетворительн** Знает существующие средства криптографической защиты информации. Умеет с ошибками делать выбор средств криптографической защиты информации в соответствии с целями профессиональных задач, и обосновывать его. Не владеет навыками применения методов и средств криптографической защиты информации для решения профессиональных задач. **Хорошо** Знает существующие средства криптографической защиты информации. Умеет правильно делать выбор средств криптографической защиты информации в соответствии с целями профессиональных задач, и обосновывать его. Не владеет в полной мере навыками применения методов и средств криптографической защиты информации для решения профессиональных задач. **Отлично** Знает существующие средства криптографической защиты информации. Умеет правильно делать выбор средств криптографической защиты информации в соответствии с целями профессиональных задач, и обосновывать его. Владеет в полной мере навыками применения методов и средств криптографической защиты информации для

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично решения профессиональных задач.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : ИКНИТ

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 50 до 60
«неудовлетворительно» / «незачтено» менее 50 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	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
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	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
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	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: **20**

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: **15**

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: **15**

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 50 до 60
«неудовлетворительно» / «незачтено» менее 50 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	Алгоритм RSA **Защищаемое контрольное мероприятие**	Знание алгоритма RSA, реализация алгоритма RSA на одном из языков программирования
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	Атаки, связанные с особенностями реализации криптосистем **Защищаемое контрольное мероприятие**	Знание основных атак на криптосистемы.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	Итоговый контроль **Итоговое контрольное мероприятие**	Итоговая контрольная работа по всем пройденным темам курса

Спецификация мероприятий текущего контроля

Алгоритм RSA

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **10**

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

Атаки, связанные с особенностями реализации криптосистем

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **20**

Показатели оценивания	Баллы
Знание атак только зашифрованным текстом	10
Знание атаки "человек посередине"	10
Знание атаки по словарю и атаки грубой силы	10
Знание атак открытым текстом	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: **20**

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