МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Лунегов Игорь Владимирович**
Балтаев Родион Хамзаевич

Рабочая программа дисциплины

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ И СТАНДАРТЫ

Код УМК 68633

Утверждено
Протокол №4
от «24» июня 2021 г.

Пермь, 2021

1. Наименование дисциплины

Криптографические протоколы и стандарты

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
направленность Безопасность открытых информационных систем

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Криптографические протоколы и стандарты** у обучающегося должны быть сформированы следующие компетенции:

10.05.03 Информационная безопасность автоматизированных систем (направленность : 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

ПК.1 Способен использовать языки, системы, инструментальные, программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты

Индикаторы

ПК.1.2 Использует языки, системы, инструментальные, программные и аппаратные средства, методы моделирования для испытаний систем защиты

4. Объем и содержание дисциплины

Специальность	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	12
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (3) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (12 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Криптографические протоколы и стандарты.Первый семестр

Проверка базы знаний по основам науки криптография. Математические основы шифрования. OTP. Симметричные / ассиметричные шифры. Элементарные функции шифрования. Сеть Фейстеля. Блочные шифры. поточные шифры. ЭЦП. Хеш-функции. Другие криптографические примитивы. Вопросы коллизии. Построение систем, использующих криптографические примитивы. Криптографические стандарты. DES/ AES. Стандарт RC4. Стандарты ЭЦП. Стандарты хеш-функций. Стандарты инфраструктуры открытых ключей на примере X.509. Протоколы, использующие криптографические примитивы разных уровней по модели OSI. Классификация криптографических протоколов. Протоколы с реализацией целостности сообщений. Протоколы цифровой подписи, идентификации и аутентификации участников. Протокол конфиденциальной передачи данных. Протоколы распределения, обмена, согласования ключей.

Криптографические примитивы

Проверка базы знаний по основам науки криптография. Математические основы шифрования. OTP. Симметричные / ассиметричные шифры. Элементарные функции шифрования. Сеть Фейстеля. Блочные шифры. поточные шифры. ЭЦП. Хеш-функции. Другие криптографические примитивы. Вопросы коллизии. Построение систем, использующих криптографические примитивы.

Криптографические протоколы и стандарты

Криптографические стандарты. DES/ AES. Стандарт RC4. Стандарты ЭЦП. Стандарты хеш-функций. Стандарты инфраструктуры открытых ключей на примере X.509. Протоколы, использующие криптографические примитивы разных уровней по модели OSI. Классификация криптографических протоколов. Протоколы с реализацией целостности сообщений. Протоколы цифровой подписи, идентификации и аутентификации участников. Протокол конфиденциальной передачи данных. Протоколы распределения, обмена, согласования ключей.

Анализ защищенности информационных систем

Изучение основных приемов и методов взлома информационных систем и сетей. Изучение способов защиты, противодействия, анализ уязвимостей информационной системы.

Итоговое контрольное мероприятие

Принцип Керкгоффса
Понятие хеш-функции и требования к криптографической хеш-функции
Понятие ЭЦП.
Виды ЭЦП и их определение
Понятие симметричного алгоритма шифрования
Понятие асимметричного алгоритма шифрования
Понятие односторонней функции. Пример
Определение криптографического протокола
Параметры (длина ключа, количество раундов, размер блока шифрования) работы алгоритмов «Магма» и «Кузнечик»
Задан протокол Диффи-Хеллмана формирования общего ключа K между сторонами A и B с использование мультипликативной группы целых чисел по модулю p:
A->B: KA=gx mod p (x – случайное секретное число)
B->A: KB=gy mod p (y – случайное секретное число)
A: K= (KB)x mod p
B: K= (KA)y mod p
p – большое простое число, g – первообразный корень по модулю p.

Переписать протокол Диффи-Хеллмана с использованием эллиптических кривых вида y2=x3+ax+b mod p с заданным набором параметров (p, a, b, G, n, h), где p – большое простое число; a и b – параметры кривой; G – генератор или базовая точка циклической подгруппы; n – порядок подгруппы или количество точек в подгруппе порожденной точкой G; h – кофактор.

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. 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 с. — ISBN 978-5-9515-0166-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/60851.html

2. Теоретико-числовые методы в криптографии : учебное пособие / составители Ф. Б. Тебуева, В. О. Антонов. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 107 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/75601.html

3. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. http://www.iprbookshop.ru/97571

Дополнительная:

1. Фомичев, В. М. Криптография – наука о тайнописи : учебное пособие / В. М. Фомичев. — Москва : Прометей, 2020. — 66 с. — ISBN 978-5-00172-040-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. https://www.iprbookshop.ru/125666

2. Ильин, М. Е. Теоретико-числовые методы в криптографии. Ч.1 : учебное пособие / М. Е. Ильин, К. А. Ципоркова. — Рязань : Рязанский государственный радиотехнический университет, 2020. — 112 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. https://www.iprbookshop.ru/121800

3. Калмыков, И. А. Криптографические методы защиты информации : лабораторный практикум / И. А. Калмыков, Д. О. Науменко, Т. А. Гиш. — Ставрополь : Северо-Кавказский федеральный университет, 2015. — 109 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/63099.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://www.lektorium.tv/course/22759 Криптографические протоколы. Николенко
https://ru.bmstu.wiki/ Национальная библиотека им. Н. Э. Баумана
http://www.intuit.ru/studies/courses/691/547/info Лекции ИНТУИТ
https://www.lektorium.tv/course/22759 Криптографические протоколы. Николенко
http://book.uz/2010/10/16/kris-kasperski-knigi-i-stati-sbornik/ Сборник статей Криса Касперски
http://book.uz/2010/10/16/kris-kasperski-knigi-i-stati-sbornik/ Сборник статей Криса Касперски
https://www.lektorium.tv/course/22759 Криптографические протоколы. Николенко

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

Образовательный процесс по дисциплине **Криптографические протоколы и стандарты** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:
- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).
Перечень используемого программного обеспечения:
- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Plaer";
- программа просмотра интернет контента (браузер) "Google Chrome"
- свободная кроссплатформенная среда разработки "Code::Blocks"
- бесплатная интегрированная среда разработки "Visual Studio Community"

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

Лекционные занятия, занятия семинарского типа (семинары, практические занятия), групповые (индивидуальные) консультации, мероприятия текущего контроля и промежуточной аттестации проводятся в аудитории, оснащенной презентационной техникой (проектор, экран для проектора,

компьютер/ноутбук), а также меловой (и) или маркерной доской.

Лабораторные занятия проводятся в компьютерном классе кафедры радиоэлектроники и защиты информации с техническим оснащением, указанным в паспорте

Аудитория для самостоятельной работы: Компьютерный класс кафедры радиоэлектроники и защиты информации и помещения библиотеки с персональными компьютерами с доступом к локальной и глобальной сетям

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 протоколы и стандарты

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.9.2 Анализирует возможности криптографических средств защиты информации	Знания принципов, методик и технологий построения криптографических средств защиты информации. Умение анализировать криптографические средства защиты информации и выбирать криптографические средства защиты информации соответствующее требуемому уровню эффективности.	**Неудовлетворител** Отсутствие каких либо знаний принципов, методик и технологий построения криптографических средств защиты информации. **Удовлетворительн** Частично сформированы общие знания принципов, методик и технологий построения криптографических средств защиты информации. Не полностью сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией. **Хорошо** Сформированные систематические знания принципов, методик и технологий построения криптографических средств защиты информации, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки. В целом успешно сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией за некоторым исключением. **Отлично** Полностью сформированные знания принципов, методик и технологий построения криптографических средств защиты информации. Сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично достигать их в процессе профессиональной деятельности. Свободное владение терминологией.
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации	Знания методов и средств криптографической защиты информации. Умение анализировать и выбирать решение соответствующее требуемому уровню эффективности применения АС.	**Неудовлетворител** Отсутствие каких либо знаний методов и средств криптографической защиты информации. **Удовлетворительн** Частично сформированы общие знания методов и средств криптографической защиты информации. Не полностью сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией. **Хорошо** Сформированные систематические знания методов и средств криптографической защиты информации, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки. В целом успешно сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией за некоторым исключением. **Отлично** Полностью сформированные знания методов и средств криптографической защиты информации. Сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией.
ОПК.9.3 Применяет методы и средства криптографической защиты информации для решения профессиональных	Знания методов и средств криптографической защиты информации. Умение анализировать методы криптографической защиты информации и выбирать решение соответствующее	**Неудовлетворител** Отсутствие каких либо знаний методов и средств криптографической защиты информации. **Удовлетворительн** Частично сформированы общие знания методов и средств криптографической

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
задач	требуемому уровню эффективности применения АС. Обладания навыками анализа АС, выбора решений среди существующих, аргументации выбора.	**Удовлетворительн** защиты информации. Не полностью сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией. **Хорошо** Сформированные систематические знания методов и средств криптографической защиты информации, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки. В целом успешно сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией за некоторым исключением. **Отлично** Полностью сформированные знания методов и средств криптографической защиты информации. Сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией.

ПК.1

Способен использовать языки, системы, инструментальные, программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.1.2 Использует языки, системы, инструментальные, программные и аппаратные средства, методы моделирования для испытаний систем защиты	Использует языки, системы, инструментальные, программные и аппаратные средства, методы моделирования для испытаний систем защиты. Обладания навыками анализа систем защиты информации, выбора решений среди существующих, аргументации выбора.	**Неудовлетворител** Отсутствие каких либо знаний языков, систем, инструментальных, программных и аппаратных средств, методы моделирования для испытаний систем защиты. **Удовлетворительн** Частично сформированы общие знания языков, систем, инструментальных, программных и аппаратных средств, методы моделирования для испытаний систем защиты. Не полностью сформировано

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией. **Хорошо** Сформированные систематические знания языков, систем, инструментальных, программных и аппаратных средств, методы моделирования для испытаний систем защиты. В целом успешно сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией за некоторым исключением. **Отлично** Полностью сформированные знания языков, систем, инструментальных, программных и аппаратных средств, методы моделирования для испытаний систем защиты. Сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

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

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 43 до 60
«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Криптографические примитивы **Входное тестирование**	Знание нормативных документов в области информационной безопасности. Знание методов программирования.
ОПК.9.2 Анализирует возможности криптографических средств защиты информации	Криптографические примитивы **Защищаемое контрольное мероприятие**	Умение применять и разбираться в криптографических примитивах.
ПК.1.2 Использует языки, системы, инструментальные, программные и аппаратные средства, методы моделирования для испытаний систем защиты	Криптографические протоколы и стандарты **Защищаемое контрольное мероприятие**	Знание протоколов аутентификации, конфиденциальной передачи информации. Знание российский и зарубежных стандартов шифрования, создания электронной подписи и хеширования.
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации	Анализ защищенности информационных систем **Защищаемое контрольное мероприятие**	Знание основных приемов и методов взлома информационных систем и сетей. Знание способов защиты, противодействия, анализ уязвимостей информационной системы. Умение работать с программной базой для обеспечения анализа структуры, защищенности ИС.

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	Итоговое контрольное мероприятие **Итоговое контрольное мероприятие**	Знание основных нормативных документов в области информационной безопасности. Знание методов программирования. Знание протоколов аутентификации, конфиденциальной передачи информации. Знание российский и зарубежных стандартов шифрования, создания электронной подписи и хеширования. Знание основных приемов и методов взлома информационных систем и сетей. Знание способов защиты, противодействия, анализ уязвимостей информационной системы. Умение работать с программной базой для обеспечения анализа структуры, защищенности ИС.

Спецификация мероприятий текущего контроля

Криптографические примитивы

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
При тестировании допущено менее 10% ошибок	81
При тестировании допущено менее 30% ошибок	61
При тестировании допущено менее 50% ошибок	41
При тестировании допущено более 50% ошибок	0

Криптографические примитивы

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **8**

Показатели оценивания	Баллы
Знание ЭЦП / хэш-функций. Коллизии хэш-функций	10
Знание потоковых и блочных шифров.	5
Знание асимметричных/семмитричных шифров.	5

Криптографические протоколы и стандарты

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
Классификация криптографических протоколов. Протоколы с реализацией целостности сообщений. Протоколы цифровой подписи, идентификации и аутентификации участников. Протокол конфиденциальной передачи данных. Протоколы распределения, обмена, согласования ключей.	8
Криптографические стандарты. DES/ AES. Стандарт RC4. Стандарты ЭЦП. Стандарты хеш-функций. Стандарты инфраструктуры открытых ключей на примере X.509.	8
Протоколы, использующие криптографические примитивы разных уровней по модели OSI.	4

Анализ защищенности информационных систем

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
Основные способы и приема взлома сетей и способы противодействия.	10
Основные способы и приема взлома ИС и способы противодействия.	10

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Криптографические протоколы и стандарты	15
Анализ защищенности информационных систем	15
Криптографические примитивы	10