

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное 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 2020 г.

Пермь, 2020

1. Наименование дисциплины

Криптографические протоколы и стандарты

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в вариативную 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.5 Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности

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	9
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 (9 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. ОTR. Симметричные / асимметричные 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. ОTR. Симметричные / асимметричные 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

использованием мультипликативной группы целых чисел по модулю p :

$A \rightarrow B: KA = gx \pmod p$ (x – случайное секретное число)

$B \rightarrow A: KB = gy \pmod p$ (y – случайное секретное число)

$A: K = (KB)^x \pmod p$

$B: K = (KA)^y \pmod p$

p – большое простое число, g – первообразный корень по модулю p .

Переписать протокол Диффи-Хеллмана с использованием эллиптических кривых вида $y^2 = x^3 + ax + b \pmod{p}$ 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 аудиторские 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 // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/97571>

Дополнительная:

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.html>
2. 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>
3. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; перевод В. А. Хорев ; под редакцией С. М. Молякко. — 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

<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-образовательную 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 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 протоколы и стандарты**

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p>	<p>Знания принципов, методик и технологий построения автоматизированных систем. Умение анализировать АС и выбирать решение соответствующее требуемому уровню эффективности применения АС. Обладания навыками анализа АС, выбора решений среди существующих, аргументации выбора.</p>	<p align="center">Неудовлетворител Отсутствие каких либо знаний принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков</p> <p align="center">Удовлетворительн Частично сформированы общие знания принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков. Не полностью сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией.</p> <p align="center">Хорошо Сформированные систематические знания принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков, 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.</p> <p align="center">Отлично Полностью сформированные знания принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков. Сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.6 способность проводить анализ рисков информационной безопасности автоматизированной системы</p>	<p>Знания принципов, методик и технологий анализа автоматизированных систем. Умение анализировать АС и выбирать решение соответствующее требуемому уровню эффективности применения АС. Обладания навыками анализа АС, выбора решений среди существующих, аргументации выбора.</p>	<p>Отлично владение терминологией.</p> <p>Неудовлетворител Отсутствие каких либо знаний принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков</p> <p>Удовлетворительн Частично сформированы общие знания принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков. Не полностью сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией.</p> <p>Хорошо Сформированные систематические знания принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков, 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.</p> <p>Отлично Полностью сформированные систематические знания принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков. Сформировано умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Свободное владение терминологией.</p>
<p>ПК.18 способность проводить инструментальный мониторинг защищенности</p>	<p>Знание инструментов, методик и техник для мониторинга защищенности АС. Умение использовать различные инструменты для</p>	<p>Неудовлетворител Отсутствие каких либо знаний инструментов, методик и техник для мониторинга защищенности АС</p> <p>Удовлетворительн</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
автоматизированных систем	<p>мониторинга защищенности автоматизированных систем</p> <p>Навык использования различных инструментов для мониторинга защищенности автоматизированных систем</p>	<p>Удовлетворительн</p> <p>Сформированы общие, но не систематические знания инструментов, методик и техник для мониторинга защищенности АС, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p>Хорошо</p> <p>Сформированы систематические знания инструментов, методик и техник для мониторинга защищенности АС, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p>Отлично</p> <p>Полностью сформированы знания инструментов, методик и техник для мониторинга защищенности АС.</p>
<p>ПК.15</p> <p>способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p>	<p>Знание методик и техник проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Умение проведения проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</p> <p>Навык работы с техническими средствами контроля.</p>	<p>Неудовлетворител</p> <p>Отсутствие каких либо знаний, навыков, умений при проведении контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>Удовлетворительн</p> <p>Частично сформированы знания методик и техник проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации, не влияющие на общий уровень профессиональной подготовки.</p> <p>Хорошо</p> <p>Сформированные систематические знания методик и техник проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации, не влияющие на общий уровень профессиональной подготовки.</p> <p>Отлично</p> <p>Полностью сформированные знания методик и техник проведения контрольных</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p align="center">Отлично</p> <p>проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.</p>
<p>ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p>	<p>Знание методик и техник для проведения синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем. Умение проводить анализа проектных решений по обеспечению безопасности автоматизированных систем. Навык работы с программной и технической базой для проведения синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем</p>	<p align="center">Неудовлетворител</p> <p>Отсутствие каких либо знаний методик и техник для проведения синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем</p> <p align="center">Удовлетворительн</p> <p>Сформированы общие, но не систематические знания методик и техник для проведения синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем.</p> <p align="center">Хорошо</p> <p>Сформированные систематические знания методик и техник для проведения синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p align="center">Отлично</p> <p>Сформированные систематические знания методик и техник для проведения синтеза и анализа проектных решений по обеспечению безопасности автоматизированных систем.</p>
<p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p>	<p>Знание законодательной базы, методик, рекомендаций, необходимых для разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы Умение создавать модели угроз и модели нарушителя информационной безопасности автоматизированной системы Навык работы с документами.</p>	<p align="center">Неудовлетворител</p> <p>Отсутствие каких либо знаний законодательной базы, методик, рекомендаций, необходимых для разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p align="center">Удовлетворительн</p> <p>Сформированы общие, но не систематические знания законодательной базы, методик, рекомендаций, необходимых для разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p align="center">Хорошо</p> <p>Сформированные систематические знания</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо</p> <p>законодательной базы, методик, рекомендаций, необходимых для разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p style="text-align: center;">Отлично</p> <p>Полностью сформированные систематические знания законодательной базы, методик, рекомендаций, необходимых для разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы</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>Знание законодательной базы, методик, позволяющих 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>Умение искать и понимать профессиональную литературу, а так же законы и нормативные акты, относящиеся к профессиональной деятельности.</p> <p>Навык работы с документами.</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Отсутствие каких либо знаний методик, положений позволяющих разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности АС</p> <p style="text-align: center;">Удовлетворительн</p> <p>Сформированы общие знания законодательной базы, методик, позволяющих обеспечивать профессиональную деятельность в рамках составления проектов нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов.</p> <p style="text-align: center;">Хорошо</p> <p>Сформированные систематические знания законодательной базы, методик, позволяющих обеспечивать профессиональную деятельность в рамках составления проектов нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо</p> <p>положений, инструкций и других организационно-распорядительных документов, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p style="text-align: center;">Отлично</p> <p>Полностью сформированные знания законодательной базы, методик, позволяющих обеспечивать профессиональную деятельность в рамках составления проектов нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов.</p>
<p>ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы</p>	<p>Знания принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС. Умение анализировать АС и разрабатывать системы управления ИБАС Обладания навыками анализа АС, разработки системы управления ИБАС.</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Отсутствие каких либо знаний принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС.</p> <p style="text-align: center;">Удовлетворительн</p> <p>Сформированы общие знания принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС.</p> <p style="text-align: center;">Хорошо</p> <p>Сформированные систематически знания принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p style="text-align: center;">Отлично</p> <p>Сформированные систематически знания принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС. Умение анализировать АС и разрабатывать системы управления ИБАС Владение навыками анализа АС, разработки системы управления ИБАС.</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы</p>	<p>Знание схем, решений, методик и техник проектирования средств защиты информации и средств контроля защищенности автоматизированной системы Умение проектировать, анализировать и синтезировать средства защиты информации и средств контроля защищенности автоматизированной системы Навыки проектирования средств защиты информации и средств контроля защищенности автоматизированной системы</p>	<p>Неудовлетворител Отсутствие каких либо знаний методик и техник проектирования средств защиты информации и средств контроля защищенности автоматизированной системы</p> <p>Удовлетворительн Сформированы общие, но не систематические знание схем, решений, методик и техник проектирования средств защиты информации и средств контроля защищенности автоматизированной системы</p> <p>Хорошо Сформированные систематические знание схем, решений, методик и техник проектирования средств защиты информации и средств контроля защищенности автоматизированной системы, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p>Отлично Сформированные систематические знание схем, решений, методик и техник проектирования средств защиты информации и средств контроля защищенности автоматизированной системы. Умение проектировать, анализировать и синтезировать средства защиты информации и средств контроля защищенности автоматизированной системы Владение навыкам проектирования средств защиты информации и средств контроля защищенности автоматизированной системы</p>
<p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p>	<p>Знание схем, методик, техник построения защищенных АС. Умение использовать готовые схемы, методики и техники для анализа и синтеза прототипа, а так же построения защищенной АС. Навык командной работы, навык комплексного анализа АС на каждом этапе разработки.</p>	<p>Неудовлетворител Отсутствие каких либо знаний, методик, техник построения защищенных АС, умений и навыков их построения</p> <p>Удовлетворительн Частично сформированы общие знания схем, методик, техник построения защищенных АС, умений и навыков их построения</p> <p>Хорошо Сформированные систематически знания</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Хорошо</p> <p>схем, методик, техник построения защищенных АС, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p style="text-align: center;">Отлично</p> <p>Полностью сформированные систематически знания схем, методик, техник построения защищенных АС.</p> <p>Умение использовать готовые схемы, методики и техники для анализа и синтеза прототипа, а так же построения защищенной АС.</p> <p>Уверенное владение навыками командной работы, комплексного анализа АС на каждом этапе разработки.</p>
<p>ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности</p>	<p>Знание стандартов разработки компонентов защищенных АС. Умение использовать стандартные схемы и методики для анализа и синтеза защищенных АС. Навык командной работы на каждом этапе разработки компонентов защищенных АС.</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Отсутствие каких либо знаний стандартов разработки компонентов защищенных АС.</p> <p style="text-align: center;">Удовлетворительн</p> <p>Сформированы общие но не систематические знания схем, методик, техник построения защищенных АС.</p> <p style="text-align: center;">Хорошо</p> <p>Частично сформированные знания схем, методик, техник построения защищенных АС, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p style="text-align: center;">Отлично</p> <p>Полностью сформированные знания схем, методик, техник построения защищенных АС.</p> <p>Умение использовать стандартные схемы и методики для анализа и синтеза защищенных АС.</p> <p>Владение навыками командной работы на каждом этапе разработки компонентов защищенных АС.</p>
<p>ОПК.5 Способность применять языки, системы и инструментальные средства программирования в</p>	<p>Знание приемов объектно-ориентированного проектирования, правил оформления исходного кода программы, средств разработки и отладки прикладных</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Отсутствие каких либо знаний языков, систем и инструментальных средств программирования.</p> <p style="text-align: center;">Удовлетворительн</p> <p>Частично сформированы знания языков,</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>профессиональной деятельности</p>	<p>программ. Умение составлять требования к разрабатываемой программе, принимать обоснованное решение относительно выбора инструментария и технологий для решения поставленных задач, определять оптимальный вариант решения задачи. Владение навыками проектирования архитектуры программного обеспечения, разработки интерфейса пользователя, тестирования прикладных программ.</p>	<p>Удовлетворительн систем и инструментальных средств программирования. Хорошо Сформированные систематически знания языков, систем и инструментальных средств программирования, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки. Отлично Хорошо сформированные знания языков, систем и инструментальных средств программирования. Умение составлять требования к разрабатываемой программе, самостоятельно принимать обоснованное решение относительно выбора инструментария и технологий для решения поставленных задач, определять оптимальный вариант решения задачи. Уверенное владение навыками проектирования архитектуры программного обеспечения, разработки интерфейса пользователя, тестирования прикладных программ.</p>

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	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы 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	Криптографические примитивы Входное тестирование	Знание нормативных документов в области информационной безопасности. Знание методов программирования.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<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.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>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>Криптографические примитивы</p> <p>Защищаемое контрольное мероприятие</p>	<p>Умение применять и разбираться в криптографических примитивах.</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ОПК.5 Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</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>ПК.18 способность проводить инструментальный мониторинг защищенности 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>Криптографические протоколы и стандарты</p> <p>Защищаемое контрольное мероприятие</p>	<p>Знание протоколов аутентификации, конфиденциальной передачи информации. Знание российский и зарубежных стандартов шифрования, создания электронной подписи и хеширования.</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ОПК.5 Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</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>ПК.18 способность проводить инструментальный мониторинг защищенности 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>Анализ защищенности информационных систем</p> <p>Защищаемое контрольное мероприятие</p>	<p>Знание основных приемов и методов взлома информационных систем и сетей.</p> <p>Знание способов защиты, противодействия, анализ уязвимостей информационной системы. Умение работать с программной базой для обеспечения анализа структуры, защищенности ИС.</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ОПК.5 Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</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.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности 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>ПК.13 способность участвовать в проектировании системы управления информационной безопасностью</p>	<p>Итоговое контрольное мероприятие</p> <p>Итоговое контрольное мероприятие</p>	<p>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.</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>автоматизированной системы ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности</p> <p>автоматизированной системы ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p>ПК.18 способность проводить инструментальный мониторинг защищенности 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>		

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, выставяемый 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/симметричных шифров.	5

Криптографические протоколы и стандарты

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

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

Максимальный балл, выставяемый 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 хэш-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, выставяемый 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, выставяемый за мероприятие промежуточной аттестации: **40**

Проходной балл: 17

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