

**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 94118**

**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 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 протоколы и стандарты** у обучающегося должны быть сформированы следующие компетенции:

**10.05.03** Информационная безопасность автоматизированных систем (специализация : 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

|   |  |
|---|--|
| <b>Направления подготовки</b>                                       | 10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем) |
| <b>форма обучения</b>   | очная  |
| <b>№№ триместров, выделенных для изучения дисциплины</b>            | 12   |
| <b>Объем дисциплины (з.е.)</b>                                      | 3  |
| <b>Объем дисциплины (ак.час.)</b>                                   | 108  |
| <b>Контактная работа с преподавателем (ак.час.), в том числе:</b>   | 42   |
| <b>Проведение лекционных занятий</b>                                | 14   |
| <b>Проведение лабораторных работ, занятий по иностранному языку</b> | 28   |
| <b>Самостоятельная работа (ак.час.)</b>                             | 66   |
| <b>Формы текущего контроля</b>                                      | Защищаемое контрольное мероприятие (3)<br>Итоговое контрольное мероприятие (1)   |
| <b>Формы промежуточной аттестации</b>                               | Зачет (12 триместр)  |

## 5. Аннотированное описание содержания разделов и тем дисциплины

### Криптографические протоколы и стандарты

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

Итоговое контрольное мероприятие проводится в виде зачета.

Вопросы к зачету:

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  $p$ :

$A \rightarrow B: K_A = g^x \mod p$  ( $x$  – случайное секретное число)

$B \rightarrow A: K_B = g^y \mod p$  ( $y$  – случайное секретное число)

$A: K = (K_B)^x \mod p$

B:  $K = (KA)y \bmod p$

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

Переписать протокол Диффи-Хеллмана с использованием эллиптических кривых вида  $y^2 = x^3 + ax + b \bmod p$  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. Разработка моделей криптографической защиты информации : монография / В. Г. Шубович, В. В. Капитанчук, Н. С. Знаенко, Ю. И. Титаренко. — Ульяновск : Ульяновский государственный педагогический университет имени И.Н. Ульянова, 2013. — 128 с. — ISBN 978-5-86045-640-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/59180.html>
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 с. — ISBN 978-5-9515-0166-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/60851.html>
3. 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>
4. Лапони́на, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапони́на ; 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. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/102017.html>
2. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; перевод В. А. Хорев ; под редакцией С. М. Молявко. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 480 с. — ISBN 978-5-00101-700-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/20709>



## **9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины**

<https://www.lektorium.tv/course/22759> Криптографические протоколы. Николенко

<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 Player";
- программа просмотра интернет контента (браузер) "Google Chrome"

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 компьютерного класса

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.  
Индикаторы и критерии их оценивания**

**ОПК.5**

**Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности**

| <b>Компетенция<br/>(индикатор)</b>  | <b>Планируемые результаты<br/>обучения</b>  | <b>Критерии оценивания результатов<br/>обучения</b>  |
|---|---|--|
| <b>ОПК.5</b><br>Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности | Знание приемов объектно-ориентированного проектирования, правил оформления исходного кода программы, средств разработки и отладки прикладных программ.<br>Умение составлять требования к разрабатываемой программе, принимать обоснованное решение относительно выбора инструментария и технологий для решения поставленных задач, определять оптимальный вариант решения задачи.<br>Владение навыками проектирования архитектуры программного обеспечения, разработки интерфейса пользователя, тестирования прикладных программ. | <b>Неудовлетворител</b><br>Отсутствие каких либо знаний.<br><b>Удовлетворительн</b><br>Сформированы общие но не систематические знания языков, систем и инструментальных средств программирования.<br><b>Хорошо</b><br>Сформированные систематически знания языков, систем и инструментальных средств программирования, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.<br><b>Отлично</b><br>Сформированные систематически знания языков, систем и инструментальных средств программирования |

**ПК.7**

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

| <b>Компетенция<br/>(индикатор)</b>   | <b>Планируемые результаты<br/>обучения</b>  | <b>Критерии оценивания результатов<br/>обучения</b>  |
|--|---|--|
| <b>ПК.7</b><br>способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения | Знания принципов, методик и технологий построения автоматизированных систем.<br>Умение анализировать АС и выбирать решение соответствующее требуемому уровню эффективности применения АС.<br>Обладания навыками анализа | <b>Неудовлетворител</b><br>Отсутствие каких-либо знаний<br><b>Удовлетворительн</b><br>Сформированы общие, но не систематические знания принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков. Не полностью сформировано умение свободно осуществлять мыслительную |

| <b>Компетенция<br/>(индикатор)</b> | <b>Планируемые результаты<br/>обучения</b>                  | <b>Критерии оценивания результатов<br/>обучения</b>  |
|------------------------------------|---|--|
| автоматизированных систем          | АС, выбора решений среди существующих, аргументации выбора. | <p><b>Удовлетворительн</b><br/>деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией.</p> <p><b>Хорошо</b><br/>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><b>Отлично</b><br/>Хорошо 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> |

## ПК.6

**способность проводить анализ рисков информационной безопасности автоматизированной системы**

| <b>Компетенция<br/>(индикатор)</b>  | <b>Планируемые результаты<br/>обучения</b>   | <b>Критерии оценивания результатов<br/>обучения</b>   |
|---|--|---|
| <b>ПК.6</b><br>способность проводить анализ рисков информационной безопасности автоматизированной системы | 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 | <p><b>Неудовлетворител</b><br/>Отсутствие знаний принципов, методик и технологий построения автоматизированных систем уязвимостей и рисков</p> <p><b>Удовлетворительн</b><br/>Частично сформированы общие, но не систематические знания принципов, методик и технологий построения автоматизированных систем, уязвимостей и рисков. Не полностью сформировано</p> |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения | Критерии оценивания результатов<br>обучения  |
|----------------------------|------------------------------------|--|
|                            | выбора.                            | <p><b>Удовлетворительн</b><br/>умение свободно осуществлять мыслительную деятельность, ставить цели, и успешно достигать их в процессе профессиональной деятельности. Затрудненное владение терминологией</p> <p><b>Хорошо</b><br/>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><b>Отлично</b><br/>Хорошо 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 владение терминологией.</p> |

## ПК.18

### способность проводить инструментальный мониторинг защищенности автоматизированных систем

| Компетенция<br>(индикатор)  | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения   |
|---|--|---|
| ПК.18<br>способность проводить инструментальный мониторинг защищенности автоматизированных систем | <p>Знание инструментов, методик и техник для мониторинга защищенности АС.</p> <p>Умение использовать различные инструменты для мониторинга защищенности автоматизированных систем</p> <p>Навык использования различных инструментов для мониторинга защищенности автоматизированных систем</p> | <p><b>Неудовлетворител</b><br/>Нет общих знаний инструментов, методик и техник для мониторинга защищенности АС</p> <p><b>Удовлетворительн</b><br/>Не совсем сформированы общие знания инструментов, методик и техник для мониторинга защищенности АС, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки</p> <p><b>Хорошо</b></p> |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения | Критерии оценивания результатов<br>обучения   |
|----------------------------|------------------------------------|---|
|                            |                                    | <p><b>Хорошо</b><br/>Сформированы систематические знания инструментов, методик и техник для мониторинга защищенности АС, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.</p> <p><b>Отлично</b><br/>Хорошо сформированы систематические знания инструментов, методик и техник для мониторинга защищенности АС.</p> |

### ПК.15

**способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации**

| Компетенция<br>(индикатор)  | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения   |
|---|--|---|
| <p><b>ПК.15</b><br/>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><b>Неудовлетворител</b><br/>Отсутствие общих знаний методик и техник проведения контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p><b>Удовлетворительн</b><br/>Частично сформированы общие 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><b>Хорошо</b><br/>Сформированные 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><b>Отлично</b><br/>Хорошо сформированные знания методик и техник проведения контрольных проверок</p> |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения | Критерии оценивания результатов<br>обучения  |
|----------------------------|------------------------------------|--|
|                            |                                    | <b>Отлично</b><br>работоспособности и эффективности<br>применяемых программно-аппаратных,<br>криптографических и технических средств<br>защиты информации. |

### ПК.9

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

| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения  | Критерии оценивания результатов<br>обучения  |
|--|---|--|
| <b>ПК.9</b><br>способность проводить<br>синтез и анализ<br>проектных решений по<br>обеспечению<br>безопасности<br>автоматизированных<br>систем | Знание методик и техник для<br>проведения синтеза и анализа<br>проектных решений по<br>обеспечению безопасности<br>автоматизированных систем.<br>Умение проводить анализа<br>проектных решений по<br>обеспечению безопасности<br>автоматизированных систем.<br>Навык работы с программной и<br>технической базой для<br>проведения синтеза и анализа<br>проектных решений по<br>обеспечению безопасности<br>автоматизированных систем | <b>Неудовлетворител</b><br>Отсутствие знания методик и техник для<br>проведения синтеза и анализа проектных<br>решений по обеспечению безопасности<br>автоматизированных систем.<br><b>Удовлетворительн</b><br>Частично сформированы общие знания<br>методик и техник для проведения синтеза и<br>анализа проектных решений по обеспечению<br>безопасности автоматизированных систем.<br><b>Хорошо</b><br>Сформированные систематические знания<br>методик и техник для проведения синтеза и<br>анализа проектных решений по обеспечению<br>безопасности автоматизированных систем,<br>содержащие отдельные пробелы, не<br>влияющие на общий уровень<br>профессиональной подготовки.<br><b>Отлично</b><br>Хорошо сформированные знания методик и<br>техник для проведения синтеза и анализа<br>проектных решений по обеспечению<br>безопасности автоматизированных систем. |

### ПК.5

**способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы**

| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения  |
|--|--|--|
| <b>ПК.5</b><br>способность<br>разрабатывать модели<br>угроз и модели<br>нарушителя | Знание законодательной базы,<br>методик, рекомендаций,<br>необходимых для разработки<br>модели угроз и модели<br>нарушителя информационной | <b>Неудовлетворител</b><br>Отсутствие знаний законодательной базы,<br>методик, рекомендаций, необходимых для<br>разработки модели угроз и модели<br>нарушителя информационной безопасности |

| <b>Компетенция<br/>(индикатор)</b>                     | <b>Планируемые результаты<br/>обучения</b>   | <b>Критерии оценивания результатов<br/>обучения</b>   |
|--|--|---|
| информационной безопасности автоматизированной системы | безопасности автоматизированной системы<br>Умение создавать модели угроз и модели нарушителя информационной безопасности автоматизированной системы<br>Навык работы с документами. | <b>Неудовлетворител</b><br>автоматизированной системы<br><b>Удовлетворительн</b><br>Частично сформированы общие знания законодательной базы, методик, рекомендаций, необходимых для разработки модели угроз и модели нарушителя информационной безопасности автоматизированной системы<br><b>Хорошо</b><br>Сформированные знания 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.<br><b>Отлично</b><br>Хорошо сформированные систематические знания законодательной базы, методик, рекомендаций, необходимых для разработки 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**

| <b>Компетенция<br/>(индикатор)</b>   | <b>Планируемые результаты<br/>обучения</b>   | <b>Критерии оценивания результатов<br/>обучения</b>  |
|--|--|--|
| <b>ПК.23</b><br>способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций | 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 | <b>Неудовлетворител</b><br>Отсутствие знаний 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<br><b>Удовлетворительн</b> |



| Компетенция<br>(индикатор)  | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения  |
|---|--|--|
| и других<br>организационно-<br>распорядительных<br>документов в сфере<br>профессиональной<br>деятельности | Умение искать и понимать<br>профессиональную литературу,<br>а так же законы и нормативные<br>акты, относящиеся к<br>профессиональной<br>деятельности.<br>Навык работы с документами. | <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Частично сформированы общие знания<br/>законодательной базы, методик,<br/>позволяющих обеспечивать<br/>профессиональную деятельность в рамках<br/>составления проектов нормативных и<br/>методических материалов,<br/>регламентирующих работу по обеспечению<br/>информационной безопасности<br/>автоматизированных систем, а также<br/>положений, инструкций и других<br/>организационно-распорядительных<br/>документов</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные систематические знания<br/>законодательной базы, методик,<br/>позволяющих обеспечивать<br/>профессиональную деятельность в рамках<br/>составления проектов нормативных и<br/>методических материалов,<br/>регламентирующих работу по обеспечению<br/>информационной безопасности<br/>автоматизированных систем, а также<br/>положений, инструкций и других<br/>организационно-распорядительных<br/>документов, содержащие отдельные<br/>пробелы, не влияющие на общий уровень<br/>профессиональной подготовки.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Хорошо сформированные знания<br/>законодательной базы, методик,<br/>позволяющих обеспечивать<br/>профессиональную деятельность в рамках<br/>составления проектов нормативных и<br/>методических материалов,<br/>регламентирующих работу по обеспечению<br/>информационной безопасности<br/>автоматизированных систем, а также<br/>положений, инструкций и других<br/>организационно-распорядительных<br/>документов</p> |

### ПК.13

**способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы**

| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения  |
|--|--|--|
| <b>ПК.13</b><br>способность<br>участвовать в<br>проектировании<br>системы управления<br>информационной<br>безопасностью<br>автоматизированной<br>системы | Знания принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС.<br>Умение анализировать АС и разрабатывать системы управления ИБАС<br>Обладания навыками анализа АС, разработки системы управления ИБАС. | <b>Неудовлетворител</b><br>Отсутствие знаний принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС.<br><b>Удовлетворительн</b><br>Частично сформированы общие, но не систематические знания принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС.<br><b>Хорошо</b><br>Сформированные систематически знания принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС, содержащие отдельные пробелы, не влияющие на общий уровень профессиональной подготовки.<br><b>Отлично</b><br>Хорошо сформированные систематически знания принципов, методик и технологий построения автоматизированных систем и систем управления ИБАС. |

### ПК.14

**способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы**

| Компетенция<br>(индикатор)  | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения  |
|---|--|--|
| <b>ПК.14</b><br>способность<br>участвовать в<br>проектировании<br>средств защиты<br>информации и средств<br>контроля<br>защищенности<br>автоматизированной<br>системы | Знание схем, решений, методик и техник проектирования средств защиты информации и средств контроля защищенности автоматизированной системы<br>Умение проектировать, анализировать и синтезировать средства защиты информации и средств контроля защищенности автоматизированной системы<br>Навыки проектирования средств защиты информации и | <b>Неудовлетворител</b><br>Отсутствие знания схем, решений, методик и техник проектирования средств защиты информации и средств контроля защищенности автоматизированной системы<br><b>Удовлетворительн</b><br>Частично сформированы общие знания схем, решений, методик и техник проектирования средств защиты информации и средств контроля защищенности автоматизированной системы<br><b>Хорошо</b><br>Сформированные знания схем, решений, методик и техник проектирования средств |

| Компетенция<br>(индикатор) | Планируемые результаты<br>обучения                             | Критерии оценивания результатов<br>обучения   |
|----------------------------|--|---|
|                            | средств контроля<br>защищенности<br>автоматизированной системы | <p><b>Хорошо</b><br/>защиты информации и средств контроля<br/>защищенности автоматизированной<br/>системы, содержащие отдельные пробелы,<br/>не влияющие на общий уровень<br/>профессиональной подготовки.</p> <p><b>Отлично</b><br/>Хорошо сформированные знания схем,<br/>решений, методик и техник проектирования<br/>средств защиты информации и средств<br/>контроля защищенности<br/>автоматизированной системы</p> |

### ПК.10

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

| Компетенция<br>(индикатор)   | Планируемые результаты<br>обучения   | Критерии оценивания результатов<br>обучения   |
|--|--|---|
| <b>ПК.10</b><br>способность<br>участвовать в<br>разработке<br>защищенных<br>автоматизированных<br>систем по профилю<br>своей<br>профессиональной<br>деятельности | Знание схем, методик, техник<br>построения защищенных АС.<br>Умение использовать готовые<br>схемы, методики и техники для<br>анализа и синтеза прототипа, а<br>так же построения защищенной<br>АС.<br>Навык командной работы,<br>навык комплексного анализа<br>АС на каждом этапе разработки | <p><b>Неудовлетворител</b><br/>Отсутствие знания схем, методик, техник<br/>построения защищенных АС</p> <p><b>Удовлетворительн</b><br/>Частично сформированы общие но не<br/>систематические знания схем, методик,<br/>техник построения защищенных АС.</p> <p><b>Хорошо</b><br/>Сформированные систематически знания<br/>схем, методик, техник построения<br/>защищенных АС, содержащие отдельные<br/>пробелы, не влияющие на общий уровень<br/>профессиональной подготовки.</p> <p><b>Отлично</b><br/>Хорошо сформированные систематически<br/>знания схем, методик, техник построения<br/>защищенных АС.</p> |

### ПК.11

**способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности**

| Компетенция<br>(индикатор)                                 | Планируемые результаты<br>обучения  | Критерии оценивания результатов<br>обучения   |
|--|---|---|
| <b>ПК.11</b><br>способность<br>участвовать в<br>разработке | Знание стандартов разработки<br>компонентов защищенных АС.<br>Умение использовать<br>стандартные схемы и методики | <p><b>Неудовлетворител</b><br/>Отсутствие знания схем, методик, техник<br/>построения защищенных АС.</p> <p><b>Удовлетворительн</b></p> |

| Компетенция<br>(индикатор)  | Планируемые результаты<br>обучения  | Критерии оценивания результатов<br>обучения  |
|---|---|--|
| компонентов<br>автоматизированных<br>систем в сфере<br>профессиональной<br>деятельности | для анализа и синтеза<br>защищенных АС.<br>Навык командной работы на<br>каждом этапе разработки<br>компонентов защищенных АС. | <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Частично сформированы общие знания<br/>схем, методик, техник построения<br/>защищенных АС.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированные систематические знания<br/>схем, методик, техник построения<br/>защищенных АС, содержащие отдельные<br/>пробелы, не влияющие на общий уровень<br/>профессиональной подготовки.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Хорошо сформированные систематические<br/>знания схем, методик, техник построения<br/>защищенных АС.</p> |

## **Оценочные средства текущего контроля и промежуточной аттестации**

Схема доставки : Базовая

**Вид мероприятия промежуточной аттестации : Зачет**

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

**Максимальное количество баллов : 100**

### **Конвертация баллов в отметки**

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 44 до 60

«неудовлетворительно» / «незачтено» менее 44 балла

| <b>Компетенция<br/>(индикатор)</b> | <b>Мероприятие<br/>текущего контроля</b> | <b>Контролируемые элементы<br/>результатов обучения</b> |
|------------------------------------|--|---|
|------------------------------------|--|---|

| Компетенция<br>(индикатор)   | Мероприятие<br>текущего контроля  | Контролируемые элементы<br>результатов обучения  |
|--|---|--|
| <p><b>ПК.5</b><br/>способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p><b>ПК.9</b><br/>способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p><b>ПК.10</b><br/>способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p><b>ПК.15</b><br/>способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p><b>ПК.18</b><br/>способность проводить инструментальный мониторинг защищенности автоматизированных систем</p> <p><b>ПК.23</b><br/>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 примитивы</p> <p><b>Защищаемое контрольное мероприятие</b></p> | <p>Знание протоколов аутентификации, конфиденциальной передачи информации. Знание российский и зарубежных стандартов шифрования, создания электронной подписи и хеширования.</p> |

| Компетенция<br>(индикатор)   | Мероприятие<br>текущего контроля  | Контролируемые элементы<br>результатов обучения  |
|--|---|--|
| <p><b>ПК.5</b><br/>способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p><b>ПК.9</b><br/>способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p><b>ПК.10</b><br/>способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p><b>ПК.15</b><br/>способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации</p> <p><b>ПК.18</b><br/>способность проводить инструментальный мониторинг защищенности автоматизированных систем</p> <p><b>ПК.23</b><br/>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><b>Защищаемое контрольное мероприятие</b></p> | <p>Знание протоколов аутентификации, конфиденциальной передачи информации. Знание российский и зарубежных стандартов шифрования, создания электронной подписи и хеширования.</p> |

| Компетенция<br>(индикатор)  | Мероприятие<br>текущего контроля  | Контролируемые элементы<br>результатов обучения   |
|---|---|---|
| <p><b>ПК.5</b><br/>способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p><b>ПК.9</b><br/>способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p><b>ПК.18</b><br/>способность проводить инструментальный мониторинг защищенности автоматизированных систем</p> <p><b>ПК.23</b><br/>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><b>Защищаемое контрольное мероприятие</b></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<br>(индикатор)   | Мероприятие<br>текущего контроля   | Контролируемые элементы<br>результатов обучения   |
|--|--|---|
| <p><b>ПК.5</b><br/>способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p><b>ПК.6</b><br/>способность проводить анализ рисков информационной безопасности автоматизированной системы</p> <p><b>ПК.7</b><br/>способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p><b>ПК.9</b><br/>способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем</p> <p><b>ПК.10</b><br/>способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p><b>ПК.11</b><br/>способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности</p> <p><b>ПК.13</b><br/>способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы</p> <p><b>ПК.14</b><br/>способность участвовать в проектировании средств защиты информации и средств контроля</p> | <p>Итоговое контрольное мероприятие</p> <p><b>Итоговое контрольное мероприятие</b></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<br>(индикатор)  | Мероприятие<br>текущего контроля | Контролируемые элементы<br>результатов обучения |
|---|----------------------------------|---|
| защищенности<br>автоматизированной системы<br><b>ПК.15</b><br>способность проводить<br>контрольные проверки<br>работоспособности и<br>эффективности применяемых<br>программно-аппаратных,<br>криптографических и<br>технических средств защиты<br>информации<br><b>ПК.18</b><br>способность проводить<br>инструментальный мониторинг<br>защищенности<br>автоматизированных систем<br><b>ПК.23</b><br>способность разрабатывать<br>проекты нормативных и<br>методических материалов,<br>регламентирующих работу по<br>обеспечению информационной<br>безопасности<br>автоматизированных систем, а<br>также положений, инструкций и<br>других организационно-<br>распорядительных документов в<br>сфере профессиональной<br>деятельности |                                  |   |

### 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: **20**

Проходной балл: **9**

| 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 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, 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 |
|---|-------|
| Анализ защищенности информационных систем | 15    |
| Криптографические примитивы               | 15    |
| Криптографические протоколы и стандарты   | 15    |