МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

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

Рабочая программа дисциплины

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Код УМК 69467

Утверждено
Протокол №6
от «26» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Криптографические протоколы

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.01** Компьютерная безопасность

специализация Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

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

10.05.01 Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

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

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

ПК.13 способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей

ПК.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения

ПК.15 Способность оценивать эффективность системы защиты информации в компьютерных системах

ПК.18 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы

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

ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

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

ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности

4. Объем и содержание дисциплины

Направления подготовки	10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	12
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение лекционных занятий	28
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (2)
Формы промежуточной аттестации	Экзамен (12 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Криптографические протоколы.Первый семестр

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

Основные понятия криптографических протоколов

Понятия криптографии, криптосистем. Основные закономерности построения криптосистем. Многоуровневая структура криптосистем.
Классическая криптография. Доказательная (редукционистская) криптография.
Криптографические примитивы. Криптографические функции. Криптографические схемы.
Криптографические протоколы, свойства криптографических протоколов.
Классификация основных видов атак на криптографические протоколы: атака по известным ключам, атака методом повтора сеанса, атака методом деперсонификации, словарная атака, атака методом опережающего поиска, атака методом включения в канал

Интерактивные системы доказательства

Интерактивная система доказательства. Пример интерактивной системы доказательства, основанной на задаче теории чисел. Пример интерактивной системы доказательства, основанной на задаче теории графов.

Доказательства с нулевым разглашением

Доказательства с нулевым разглашением. Структура протоколов доказательства с нулевым разглашением знания. Протокол доказательства изоморфизма графов. Протокол доказательства знания дискретного логарифма. Протокол доказательства знания представления числа в базисе. Протокол доказательства знания множества чисел в соответствующих базисах. Протокол доказательства знания мультипликативной связи депонирования величин.

Протоколы обмена ключами

Понятие криптографического ключа. Жизненный цикл криптографических ключей. Модели управления ключами: децентрализованное управление ключами, централизованное (трехстороннее) управление ключами. Центр распределения ключей, центр трансляции ключей.
Структура ключевой системы симметричных криптосхем. Принципы функционального разделения ключей. Принципы временного разделения ключей.
Методы распространения открытых ключей. Метод сертификации открытых ключей. Инфраструктура открытых ключей.
Протоколы распределения ключей, свойства протоколов распределения ключей. Классификация протоколов распределения ключей.
Протоколы распределения ключей, основанные на симметричных криптосхемах: простой однопроходный протокол обновления сеансового ключа, простой двухпроходный протокол обновления сеансового ключа, протокол транспортировки ключа методом "запрос-ответ", протокол транспортировки ключа построенный на базе "протокола рукопожатия", однопроходный протокол выработки производного ключа, протокол AKEP2, трехэтапный протокол Шамира, протокол Нидхема-Шредера, протокол Kerberos, протокол Отвея-Риса.
Протоколы распределения ключей, основанные на асимметричных криптосхемах: протокол Нидхема-Шредера с открытыми ключами, протокол SSL, протокол Beller-Yacobi, протокол открытого распределения ключей Диффи-Хеллмана, протокол MTI (Matsumoto-Takashima-Imai), протокол STS (station-to-station).
Конференц-связь, протокол распределения ключей конференц-связи. Протокол

Ингемарссона-Танга-Вонга. Протокол Бурместера-Десмедта.

Протоколы аутентификации

Понятие протокола аутентификации. Требования к протоколу аутентификации.
Парольная аутентификация. Основные угрозы протоколам парольной аутентификации. Протоколы с фиксированными и с одноразовыми паролями. Протокол Лампорта аутентификации по одноразовым паролям.
Аутентификация методом "запрос-ответ". Протоколы "запрос-ответ" с использованием симметричных криптосхем: протокол односторонней аутентификации с меткой времени, протокол односторонней аутентификации с использованием случайных чисел, протокол взаимной аутентификации с использованием случайных чисел, протокол взаимной аутентификации с использованием случайных чисел (вариант с хеш-функцией). Протоколы "запрос-ответ" с использованием асимметричных криптосхем: протокол односторонней аутентификации с использованием схемы цифровой подписи (варианты с меткой времени и случайными числами), протокол взаимной аутентификации с использованием схем цифровой подписи, протокол односторонней аутентификации с использованием схем открытого шифрования, протокол взаимной аутентификации с использованием схем открытого шифрования.
Аутентификация, основанная на доказательствах с нулевым разглашением знания. Протокол аутентификации Фиата-Шамира. Протокол аутентификации Файге-Фиата-Шамира. Протокол аутентификации Гиллу-Кискатра. Протокол аутентификации Шнорра. Протокол аутентификации Брикелла-Мак-Карли.

Электронная коммерция

Основные задачи защиты информации в электронной коммерции. Классификация задач электронной коммерции. Архитектура SEMPER.
Защищенные каналы передачи данных. Протокол IPSec: заголовок AH, заголовок ESP, протокол обмена ключами IKE. Протокол SSL.
Честный обмен цифровыми подписями и его приложения. Протокол доказательства для схемы проверяемого депонирования. Схема честного обмена цифровыми подписями Asokan - Slioup - Waidner. Основной протокол схемы одновременного подписания контракта.

Электронное голосование

Задача электронного голосования. Виды систем электронного голосования. Риски электронного голосования.
Схема традиционного ("бумажного") голосования. Протокол двух агентств Нурми-Саломаа-Сантин. Протокол двух агентств Фудзиока-Окамото-Охта. Протокол Sensus. Протокол голосования с одной Центральной комиссией на базе протокола ANDOS. Протокол голосования с одной Центральной комиссией на базе "слепой" подписи.

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. Запечников С. В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности:учеб. пособие для вузов/С. В. Запечников.-М.:Горячая линия-Телеком,2007, ISBN 978-5-93517-318-2.-320.-Библиогр.: с. 296-305

2. 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 c. — ISBN 978-5-4497-0684-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/97571

Дополнительная:

1. Гаврилов, Л. П. Электронная коммерция : учебник и практикум для вузов / Л. П. Гаврилов. — 3-е изд., доп. — Москва : Издательство Юрайт, 2019. — 477 с. — (Высшее образование). — ISBN 978-5-534-11785-1. — Текст : электронный // ЭБС Юрайт [сайт]. https://www.urait.ru/bcode/446579

2. Лапонина О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия:курс. лекций: учеб пособие для студентов вузов, обучающихся по спец. 510200 "Прикл. математика и информатика"/под. ред. В. А. Сухомлина.-Москва:Интернет-Университет информационных технологий,2005, ISBN 5-9556-0020-5.-608.-Библиогр.: с. 604-605

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

crypto-class.org Cryptography I
http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

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

Образовательный процесс по дисциплине **Криптографические протоколы** предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «AdobeAcrobatReader DC»;
- офисный пакет приложений «LibreOffice».

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для лабораторных работ требуется аудитория Лаборатории Информационной безопасности: аппаратные и программные средства определены паспортом лаборатории.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Криптографические протоколы

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

ПК.13

способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.13 способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей	Знать потенциальные уязвимости компьютерных систем. Уметь проводить экспериментальные исследования компьютерных систем. Владеть навыками проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей	**Неудовлетворител** Не умеет проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей **Удовлетворительн** Знает базовые принципы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей **Хорошо** Знает базовые принципы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей и умеет применять их на практике **Отлично** Умеет проводить экспериментальные исследования компьютерных систем с целью выявления уязвимостей с помощью различных средств и методов

ПК.14

способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.14 способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные	Знать базовые модели решения профессиональной задачи. Уметь обосновывать правильность выбранной модели решения профессиональной задачи. Владеть навыками обработки результатов проведенного эксперимента	**Неудовлетворител** Не может обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения **Удовлетворительн** Умеет работать с базовыми моделями решения профессиональной задачи

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
данные и теоретические решения		**Хорошо** Умеет работать с базовыми моделями решения профессиональной задачи, анализировать полученные результаты **Отлично** Умеет работать с различными моделями решения профессиональной задачи, самостоятельно выбирать их для решения задачи и анализировать полученные результаты

ПК.23

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Знать технические и программные средства защиты данных. Уметь организовать защиту информации техническими и программными средствами. Владеть приемами антивирусной защиты при работе с компьютерными системами	**Неудовлетворител** Не может организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами **Удовлетворительн** Умеет работать с базовыми средствами организации защиты информации техническими и программными средствами **Хорошо** Умеет работать с различными средствами организации защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами **Отлично** Умеет работать с различными средствами организации защиты информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами, анализировать их эффективность, самостоятельно выбирать оптимальное в указанных условиях

ПК.5

Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций	Знать существующие источники информации для аналитических обзоров по вопросам обеспечения информационной безопасности компьютерных систем Уметь осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций Владеть навыками обработки полученной информации.	**Неудовлетворител** Не способен осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций **Удовлетворительн** Умеет на базовом уровне осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем **Хорошо** Умеет использовать различные источники информации для аналитических обзоров по вопросам обеспечения информационной безопасности компьютерных систем и обобщать полученную информацию **Отлично** Умеет осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

ПК.11

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи	Знать механизмы обеспечения безопасности. Уметь выбирать механизмы обеспечения безопасности для решения поставленной задачи. Владеть методами оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи	**Неудовлетворител** Не способен оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **Удовлетворительн** Знает базовые методы оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Знает базовые методы оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи и умеет применять их на практике **Отлично** Знает различные сложные методы оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи и умеет применять их на практике

ПК.15

Способность оценивать эффективность системы защиты информации в компьютерных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.15 Способность оценивать эффективность системы защиты информации в компьютерных системах	Знать компоненты системы защиты информации. Уметь оценивать эффективность системы защиты информации в компьютерных системах. Владеть методами оценки эффективности системы защиты информации в компьютерных системах.	**Неудовлетворител** Не умеет оценивать эффективность системы защиты информации в компьютерных системах **Удовлетворительн** Владеет базовыми приемами оценки эффективность системы защиты информации в компьютерных системах **Хорошо** Владеет различными приемами оценки эффективность системы защиты информации в компьютерных системах **Отлично** Владеет различными приемами оценки эффективность системы защиты информации в компьютерных системах, может выбрать оптимальный

ПК.7

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.7 Способность провести обоснование и выбор	Знать методы и технологии обеспечения информационной безопасности компьютерных	**Неудовлетворител** Не может провести обоснование и выбор рационального решения по уровню

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	систем. Уметь провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований. Владеть навыками выбора рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований.	**Неудовлетворител** обеспечения информационной безопасности компьютерных систем с учетом заданных требований **Удовлетворительн** Может со значительными затруднениями провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **Хорошо** Может выбрать из широкого набора средств рационально решение по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **Отлично** Может выбрать оптимальное решение по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований из широкого набора средств и обосновать его

ПК.18

способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.18 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Знать компоненты системы управления информационной безопасностью компьютерной системы Уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы. Владеть методами оценки эффективности системы управления информационной безопасностью компьютерной системы.	**Неудовлетворител** Не умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы **Удовлетворительн** Может сформулировать основные предложения по совершенствованию системы управления информационной безопасностью компьютерной системы **Хорошо** Может сформулировать четкие и понятные предложения по совершенствованию системы управления информационной безопасностью компьютерной системы **Отлично**

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Может сформулировать четкие и понятные предложения по совершенствованию системы управления информационной безопасностью компьютерной системы, обосновать их

ПК.10

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	Знать составляющие системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, формальные модели политик безопасности, политик управления доступом и информационными потоками. Уметь принимать участие в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	**Неудовлетворител** Не может участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **Удовлетворительн** Знает основные требования к разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы **Хорошо** Знает основные требования к разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, умеет разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **Отлично** Знает различные, в т.ч. международные, требования к разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, умеет разрабатывать формальные модели политик безопасности, политик управления доступом и

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично информационными потоками в компьютерных системах

ПСК.6

Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	Знать языки, системы и инструментальные средства программирования. Уметь работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	**Неудовлетворител** Не умеет применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности **Удовлетворительн** Умеет использовать основные языки, системы и инструментальные средства программирования **Хорошо** Умеет использовать различные языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности **Отлично** Умеет использовать различные языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности, выбирает наилучшие в указанных условиях

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

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

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 50 до 60
«неудовлетворительно» / «незачтено» менее 50 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.5 Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций **ПК.14** способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения	Доказательства с нулевым разглашением **Письменное контрольное мероприятие**	Письменная контрольная работа, проверяющая знание протоколов доказательства с нулевым разглашением

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.10 Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **ПК.13** способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей **ПК.15** Способность оценивать эффективность системы защиты информации в компьютерных системах **ПК.18** способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы	Протоколы обмена ключами **Письменное контрольное мероприятие**	Письменная контрольная работа, проверяющая знание протоколов обмена ключами.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности **ПК.7** Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **ПК.11** способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи **ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Электронное голосование **Итоговое контрольное мероприятие**	Письменная контрольная работа, проверяющая знание протоколов электронного голосования.

Спецификация мероприятий текущего контроля

Доказательства с нулевым разглашением

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **15**

Показатели оценивания	Баллы
Знание протокола доказательства знания представления числа в базисе и протокола доказательства знания множества чисел в соответствующих базисах.	10
Знание протокола доказательства знания дискретного логарифма.	8
Знание протокола доказательства изоморфизма графов.	

	7
Знание структуры протоколов доказательства с нулевым разглашением знания.	5

Протоколы обмена ключами

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **15**

Показатели оценивания	Баллы
Знание протоколов распределения ключей, основанных на симметричных криптосхемах (протокол AKEP2, трехэтапный протокол Шамира, протокол Нидхема-Шредера, протокол Kerberos, протокол Отвея-Риса)	10
Знание протоколов распределения ключей, основанных на асимметричных криптосхемах (протокол Нидхема-Шредера с открытыми ключами, протокол SSL, протокол Beller-Yacobi, протокол открытого распределения ключей Диффи-Хеллмана, протокол MTI (Matsumoto-Takashima-Imai), протокол STS (station-to-station))	10
Знание жизненного цикла криптографических ключей и структуры ключевой системы симметричных криптосхем.	5
Знание протоколов распределения ключей, свойств протоколов распределения ключей. Знание классификации протоколов распределения ключей.	5

Электронное голосование

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **20**

Показатели оценивания	Баллы
Знание видов систем электронного голосования	10
Знание протокола голосования с одной Центральной комиссией на базе протокола ANDOS и протокола голосования с одной Центральной комиссией на базе "слепой" подписи.	10
Знание протокола двух агентств Фудзиока-Окамото-Охта и протокола Sensus.	10
Знание протокола двух агентств Нурми-Саломаа-Сантин.	10