МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

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

Рабочая программа дисциплины

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Код УМК 69467

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

Пермь, 2022

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)

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

Индикаторы

ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации

ОПК.9.2 Анализирует возможности криптографических средств защиты информации

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

4. Объем и содержание дисциплины

Специальность	10.05.01 Компьютерная безопасность (специализация: 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:учебное пособие для вузов/С. В. Запечников.-Москва: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 // Цифровой образовательный ресурс IPR SMART : [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 специальности 510200 "Прикладная математика и информатика"/О. Р. Лапонина ; ред. В. А. Сухомлин.-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

ОПК.9

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

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

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

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

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

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : 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
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	Доказательства с нулевым разглашением **Письменное контрольное мероприятие**	Письменная контрольная работа, проверяющая знание протоколов доказательства с нулевым разглашением
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	Протоколы обмена ключами **Письменное контрольное мероприятие**	Письменная контрольная работа, проверяющая знание протоколов обмена ключами.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.3** Применяет методы и средства криптографической защиты информации для решения профессиональных задач **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	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	5

симметричных криптосхем.	
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