Минобрнауки России

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «ВГУ»)**

**УТВЕРЖДАЮ**

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

23.04.2024

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.46 Криптографические протоколы

## 1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

## 2. Профиль подготовки/специализация:

Разработка защищенного программного обеспечения

## 3. Квалификация (степень) выпускника:

Специалист

## 4. Форма обучения:

Очная

## 5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

## 6. Составители программы:

Дрюченко Михаил Анатольевич, к.т.н., доцент

## 7. Рекомендована:

протокол №5 от 05.03.2024

## 8. Учебный год:

2027-2028

## 9. Цели и задачи учебной дисциплины:

Изучение основных понятий и методов современной теории криптографических протоколов, ознакомление студентов с математическими основами криптографической защиты информации и криптографических протоколов, изучение основных прикладных криптографических протоколов (распределения ключей, аутентификации (идентификации), электронной цифровой подписи, контроля целостности, электронных платежей, голосования, доказательства с нулевым разглашением и т.д.), типовых криптографических протоколов, используемых в сетях связи, получение профессиональных компетенций в области современных технологий защиты информации.

Основные задачи дисциплины:
- обучение студентов математическим основам криптографической защиты информации и криптографических протоколов;
- ознакомление студентов с примитивными и основными прикладными криптографическими протоколами;

- ознакомление студентов с методами выбора, оценки качества и анализа безопасности криптографических протоколов;
- овладение практическими навыками применения теории криптографических протоколов для защиты конфиденциальности, контроля целостности, решения задач идентификации и аутентификации.

## 10. Место учебной дисциплины в структуре ООП:

базовый блок дисциплины в обще-профессиональной части. Для успешного освоения дисциплины необходимы входные знания в области информатики, теории информации, криптографии, математической статистики, цифровой обработки сигналов, навыки программирования.

## 11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

| Код | Название компетенции | Код(ы) | Индикаторы(ы) | Планируемые результаты обучения |
|---|---|---|---|---|
| ОПК-10 | Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности | ОПК-10.7 | Знает типовые криптопротоколы, используемые в сетях связи | Знает типовые криптографические протоколы, используемые в сетях связи (SSL, TLS). |
| | | ОПК-10.8 | Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем | Знает основные типы примитивных и прикладных криптографических протоколов, а также их математические основы и принципы построения. |
| | | ОПК-10.9 | Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач | Знает принципы работы асимметричных криптографических систем, компоненты и механизмы функционирования инфраструктуры открытых ключей.<br>Умеет разворачивать инфраструктуру открытых ключей для решения прикладных криптографических задач. |
| | | ОПК-10.10 | Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств | Знает математические основы криптографических протоколов.<br>Умеет применять на практике математические методы для анализа криптографических протоколов, корректно использовать специализированное и разрабатывать собственное программное обеспечение, позволяющее автоматизировать процедуру анализа безопасности криптографических протоколов. |

| Код | Название компетенции | Код(ы) | Индикаторы(ы) | Планируемые результаты обучения |
|---|---|---|---|---|
| ОПК-10 | Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности | ОПК-10.11 | Владеет подходами к разработке и анализу безопасности криптографических протоколов | Знает математические основы симметричных и асимметричных криптографических систем, математические основы криптографических протоколов.<br>Владеет методами выбора, разработки и анализа безопасности криптографических протоколов.<br>Умеет применять на практике математические методы при исследовании безопасности криптографических протоколов. |
| | | ОПК-10.20 | Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач | Знает задачи системы информационной безопасности, которые решает инфраструктура открытых ключей, основные компоненты PKI.<br>Умеет разворачивать инфраструктуру открытых ключей для решения прикладных криптографических задач.<br>Владеет практическими навыками применения современных криптографических алгоритмов и протоколов, практическими навыками работы с известными криптографическими библиотеками. |

## 12. Объем дисциплины в зачетных единицах/час:

4/144

## Форма промежуточной аттестации:

Экзамен

## 13. Трудоемкость по видам учебной работы

| Вид учебной работы | Семестр 8 | Всего |
|---|---|---|
| Аудиторные занятия | 56 | 56 |
| Лекционные занятия | 28 | 28 |
| Практические занятия | 0 | 0 |
| Лабораторные занятия | 28 | 28 |
| Самостоятельная работа | 52 | 52 |
| Курсовая работа | | 0 |
| Промежуточная аттестация | 0 | 0 |
| Часы на контроль | 36 | 36 |
| Всего | 144 | 144 |

### 13.1. Содержание дисциплины

| п/п | Наименование раздела дисциплины | Содержание раздела дисциплины | Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК |
|---|---|---|---|
| **1. Лекции** | | | |
| 1.1 | Введение. Теоретические аспекты | Предметная область криптографических протоколов. Основные понятия. Классификация. Математические основы криптографических протоколов. Основные уязвимости криптографических протоколов и подходы к оценке безопасности протоколов. | Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ. |
| 1.2 | Криптографические протоколы передачи сообщений, аутентификации, аутентифицированного ключевого обмена. Протоколы электронных платежных систем | Протоколы передачи сообщений с обеспечением свойств конфиденциальности, целостности и неотказуемости. Протоколы односторонней и двухсторонней аутентификации. Протоколы аутентификации на основе паролей. Протоколы аутентификации на основе систем ассиметричного шифрования. Варианты протокола Нидхема-Шредера. Протоколы генерации и передачи ключей на основе симметричных и асимметричных криптосистем. Варианты протокола распределения ключей Диффи-Хеллмана (классический, на основе эллиптических кривых). Протоколы с участием доверенной третьей стороны. Свойства неотслеживаемости и несвязывемости в протоколах электронных платежных систем. | Создан онлайн электронный курс, размещены материалы к лекции. Размещены индивидуальные задания для выполнения лабораторных работ. |
| 1.3 | Прикладные протоколы | Виды прикладных протоколов. Особенности реализации протокола Kerberos.<br>Протоколы защиты данных в сети Internet. Особенности реализации семейства протоколов IPsec, SSL/TLS. Особенности реализации протоколов OCSP и TSP.<br>Безопасные протоколы голосования VAV, Twin. | Создан онлайн электронный курс, размещены материалы к лекции.<br>Размещены индивидуальные задания для выполнения лабораторных работ. |

| п/п | Наименование раздела дисциплины | Содержание раздела дисциплины | Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК |
|---|---|---|---|
| **2. Лабораторные работы** | | | |
| 2.1 | Введение. Теоретические аспекты | 1. Практическое изучение уязвимостей криптографических протоколов передачи сообщений с обеспечением свойств конфиденциальности, целостности, неотказуемости. | Размещены индивидуальные задания для выполнения лабораторных работ. |
| 2.2 | Криптографические протоколы передачи сообщений, аутентификации, аутентифицированного ключевого обмена. Протоколы электронных платежных систем | 2. Практическое изучение особенностей работы протоколов односторонней и двухсторонней аутентификации, аутентификации на основе паролей. Реализация протокола по выбору.<br>3. Практическое изучение особенностей работы протокола Нидхема-Шредера. Реализация одного из вариантов данного протокола.<br>4. Практическое изучение протоколов генерации и передачи ключей. Реализация протокола Диффи-Хеллмана в классическом варианте или в варианте на эллиптических кривых.<br>5. Практическое изучение особенностей работы протоколов цифровой подписи. Реализация одного из вариантов протокола цифровой подписи. | Размещены индивидуальные задания для выполнения лабораторных работ. |
| 2.3 | Прикладные протоколы | 6. Практическое изучение протоколов защиты данных в сети Internet. | Размещены индивидуальные задания для выполнения лабораторных работ. |

### 13.2. Темы (разделы) дисциплины и виды занятий

| № п/п | Наименование темы (раздела) | Лекционные занятия | Практические занятия | Лабораторные занятия | Самостоятельная работа | Всего |
|---|---|---|---|---|---|---|
| 1 | Введение. Теоретические аспекты | 8 | | 2 | 12 | 22 |
| 2 | Криптографические протоколы передачи сообщений, аутентификации, аутентифицированного ключевого обмена. Протоколы электронных платежных систем | 12 | | 18 | 26 | 56 |
| 3 | Прикладные протоколы | 8 | | 8 | 14 | 30 |
| | | 28 | 0 | 28 | 52 | 108 |

## 14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических работ обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей, вовремя подключаться к online занятиям, ответственно подходить к заданиям для самостоятельной работы.

## 15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

| № п/п | Источник |
|---|---|
| 1 | Рябко, Борис Яковлевич. Криптография и стеганография в информационных технологиях / Б.Я. Рябко, А.Н. Фионов, Ю.И. Шокин ; Рос. акад. наук, Сиб. отд-ние, Ин-т вычисл. технологий СО РАН .— Новосибирск : Наука, 2015 .— 239 с. : ил. — Библиогр.: с.232-236 .— ISBN 978-5-02-019206-5. |
| 2 | Рябко, Борис Яковлевич. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов .— 2-е изд. — Москва : Горячая линия - Телеком, 2013 .— 232 с. : ил., табл. — Библиогр.: с.225-229. |
| 3 | Корниенко, А.А. Криптографические методы защиты информации : учебное пособие / А.А. Корниенко, М.Л. Глухарев. – Санкт-Петербург : ПГУПС, [б. г.]. – Часть 1 – 2017. – 64 с. – ISBN 978-5-7641-1053-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/111765 (дата обращения: 07.07.2023). – Режим доступа: для авториз. пользователей. |

б) дополнительная литература:

| № п/п | Источник |
|---|---|
| 1 | Круглов И.А. Введение в теоретико-числовые методы криптографии / И.А. Круглов [и др.]. – СПб: Лань, 2011. – 400 с. |
| 2 | Щербаков, Андрей Юрьевич. Современная компьютерная безопасность. Теоретические основы. Практические аспекты : учебное пособие для студ. вузов / А.Ю. Щербаков .— М. : Кн. мир, 2009 .— 351, [1] с. : ил., табл. — (Высшая школа) .— Библиогр.: с.350-351 .— ISBN 978-5-8041-0378-2. |
| 3 | Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. – Самара : ПГУТИ, 2019. – 68 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/223319 (дата обращения: 07.07.2023). – Режим доступа: для авториз. пользователей. |

в) информационные электронно-образовательные ресурсы:

| № п/п | Источник |
|---|---|
| 1 | Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/). |
| 2 | Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/) |
| 3 | ЭБС Лань, Лицензионный договор №3010, (с 01/03/2024 по 28.02.2025) 06/02 24 от 13.02.2024 (с дополнительным соглашением №1 от 14.03.2024) |
| 4 | ЭБС «Университетская библиотека online» (Контракт №3010 06/11 23 от 26.12.2023 (с 26.12.2023 по 25.12.2024) |
| 5 | ЭБС «Консультант студента» – Лицензионный договор №980КС/12-2023 / 3010-06/01-24 от 24.01.2024 с 24.01.2024 по 11. 01.2025) |
| 6 | Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027) |
| 7 | БС BOOK.ru, Договор №3010 15/983 23 от 20.12.2023, (с 01.02.2024 по 31.01.2025) |

## 16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала, работа с учебно-методической литературой, подготовка отчетов по лабораторным работам.
Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован электронный курс, на котором размещены материалы к лекции и задания к лабораторным работам.

## 17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Для реализации учебного процесса используются:

ПО ОС Windows v.7, 8, 10, ОС GNU/Linux (Ubuntu).

При проведении занятий в дистанционном режиме обучения используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ" (https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

## 18. Материально-техническое обеспечение дисциплины:

1) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479

Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19’’, мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

2) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292

Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6’’ FHD Lenovo V155-15API

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

3) 394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380

Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17'', мультимедийный проектор, экран

ПО: ОС Windows v.7, 8, 10, Набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader

## 19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

| № п/п | Разделы дисциплины (модули) | Код компетенции | Код индикатора | Оценочные средства для текущей аттестации |
|---|---|---|---|---|
| 1 | Разделы 1-3 Введение. Теоретические аспекты. Криптографические протоколы передачи сообщений, аутентификации, аутентифицированного ключевого обмена. Протоколы электронных платежных систем. Прикладные протоколы | ОПК-10 | ОПК-10.7, ОПК-10.8, ОПК-10.9, ОПК-10.10, ОПК-10.11, ОПК-10.20 | Контрольная работа по разделам дисциплины. Лабораторные работы 1-6. Тест по соответствующим разделам |

Промежуточная аттестация
Форма контроля – Экзамен
Оценочные средства для промежуточной аттестации
Перечень вопросов, практическое задание

## 20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

### 20.1 Текущий контроль успеваемости

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Устный опрос на практических занятиях
Контрольная работа по теоретической части курса
Лабораторные работы

### Примерный перечень применяемых оценочных средств

| № п/п | Наименование оценочного средства | Представление оценочного средства в фонде | Критерии оценки |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 1 | Устный опрос | Вопросы по темам/разделам дисциплины | Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено |
| 2 | Контрольная работа по разделам дисциплины | Теоретические вопросы по темам/разделам дисциплины | Шкала оценивания соответствует таблице, приведенной ниже |

| № п/п | Наименование оценочного средства | Представление оценочного средства в фонде | Критерии оценки |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 3 | Лабораторная работа | Содержит 6 заданий | При успешном выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену. |
| 4 | КИМ промежуточной аттестации | Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 заданий вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. | Шкала оценивания приведена ниже |

**Пример задания для выполнения лабораторной работы**

**Лабораторная работа № 4**

**«Протоколы генерации и передачи ключей»**

**Цель работы**

Практическое изучение протоколов генерации и безопасного обмена криптографическими ключами по общедоступному каналу. Практическое изучение принципов работы криптографических алгоритмов на основе эллиптических кривых.

**Форма контроля**

Опрос в устной форме по исходному коду и результатам работы реализованной программы

**Количество отведённых аудиторных часов -** 2

**Содержание работы**

Реализовать протокол Диффи-Хеллмана на эллиптических кривых (ECDH). В результате работы протокола для двух абонентов д.б. выработан общий секретный ключ. Предусмотреть возможность задания начальных параметров, включающих вид кривой и координаты точки, принадлежащей данной кривой. Провести тестирование реализованного протокола при различных значениях параметров. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

**Примеры контрольных вопросов:**

1. Сформулируйте задачу дискретного логарифмирования на эллиптической кривой.
2. Перечислите состав согласуемого на начальном этапе работы протокола набора параметров.

**Пример заданий теста по разделам дисциплины**

| | | |
|---|---|---|
| 1 | Протокол Диффи-Хеллмана основан на следующей математической задаче<br>*а) факторизации числа б) нахождения простых чисел в) дискретного логарифмирования* | |
| 2 | Задачей дискретного логарифмирования является<br>*а) нахождение степени, в которую следует возвести простое число для получения заданного целого числа*<br>*б) нахождение степени, в которую следует возвести целое число для получения заданного целого числа*<br>*в) разложение числа на простые сомножители* | |
| 3 | Установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем<br>*а) идентификация б) авторизация в) аутентификация г) контроль целостности* | |
| 4 | Протокол Диффи-Хеллмана дает возможность<br>*а) безопасно обменяться общим секретом при условии аутентификации сторон*<br>*б) безопасно обменяться общим секретом*<br>*в) зашифровать сообщение г) подписать сообщение* | |
| ... | ... | |

**Приведённые ниже задания рекомендуется использовать при проведении диагностических работ для оценки остаточных знаний по дисциплине.**

Задания закрытого типа

***1. Протокол является криптографическим, если он решает по крайней мере одну из трех задач криптографии (выберите данные задачи):***

а) обеспечение конфиденциальности;
б) обеспечение доступности;
в) обеспечение целостности;
г) обеспечение неотслеживаемости;
д) обеспечение робастности

***2. Назначение криптографических протоколов состоит в***

а) максимизации объема доверия, необходимого для взаимодействия участников;
б) минимизации объема доверия, необходимого для взаимодействия участников;

***3. Для создания подписи следует использовать***

а) свой закрытый ключ;
б) свой открытый ключ;
в) закрытый ключ получателя;
г) открытый ключ получателя

***4. Протокол Диффи-Хеллмана основан на следующей математической задаче***

а) факторизации числа;
б) нахождения простых чисел;
в) дискретного логарифмирования

***5. Целостность – это***

а) невозможность несанкционированного просмотра информации;
б) невозможность несанкционированного доступа к информации;
в) невозможность несанкционированного изменения информации

***6. Установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем***

а) идентификация;

б) авторизация;

в) аутентификация;

г) контроль целостности

***7. Протокол Диффи-Хеллмана дает возможность***

а) безопасно обменяться общим секретом при условии аутентификации сторон;

б) безопасно обменяться общим секретом;

в) зашифровать сообщение;

г) подписать сообщение

***8. Аутентификация сторон в протоколе Диффи-Хеллмана необходима, потому что***

а) в противном случае атакующий может взломать дискретный логарифм;

б) в противном случае атакующий может перехватить передаваемые открытые ключи и заменить их своим открытым ключом;

в) в противном случае стороны не смогут вычислить общий секрет;

***9. Задачей дискретного логарифмирования является***

а) нахождение степени, в которую следует возвести простое число для получения заданного целого числа;

б) нахождение степени, в которую следует возвести целое число для получения заданного целого числа;

в) разложение числа на простые сомножители

***10. Электронная подпись – это***

а) имитовставка;

б) информация, необходимая для шифрования и расшифровки сообщений;

в) способ преобразования исходного секретного сообщения с целью его защиты;

г) присоединяемый к сообщению блок данных, полученный с использованием криптографического преобразования

***11. Функция, для которой легко найти прямое отображение и очень сложно найти обратное***

а) нелинейная;

б) односторонняя;

в) линейная;

г) многозначная

***12. Протокол Нидхема-Шредера применяется для***

а) шифрования;

б) аутентификации;

г) выработки электронной подписи

***13. Протокол Kerberos применяется для***

а) шифрования;

б) аутентификации;

г) выработки электронной подписи

Задания открытого типа

1. Описание распределенного алгоритма, в процессе выполнения которого два (или более) участников последовательно выполняют определенные действия и обмениваются сообщениями.

2. В зависимости от наличия третьей стороны, которой безразличен результат исполнения протокола и его участники, протоколы делят на (перечислить варианты).

3. Протоколы, в которых честность сторон гарантируется самими протоколами, называются ….

4. Назначение криптографических протоколов состоит в …. объема доверия, необходимого для взаимодействия участников.

5. Протокол является криптографическим, если он решает по крайней мере одну из трех задач криптографии (перечислить задачи).

6. Задача обращения функции $g^x$ в некоторой конечной мультипликативной группе G называется.

7. Криптографический протокол, используемый тогда, когда одному из абонентов следует назначить секретный случайный бит, который до определенного момента не должен быть известен другим абонентам.

8. Средство для обеспечения имитозащиты в протоколах аутентификации сообщений с доверяющими друг другу участниками – специальный набор символов, добавляемый к сообщению, предназначенный для обеспечения его целостности и аутентификации источника данных.

9. Каким условиям должны удовлетворять интерактивные системы доказательства?

10. Порядок использования ключей в асимметричных криптосистемах при шифровании и расшифровании данных. Шифрование на … ключе, расшифрование на … ключе.

11. Порядок использования ключей при создании и проверке электронной подписи (асимметричный вариант). Создание подписи на … ключе, проверка на … ключе.

12. Вид злоумышленных действий, при котором абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал.

Задания с развёрнутым ответом

***1. Дайте определение криптографического протокола. Распишите схему работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами.***

| Критерии оценивания | Шкала оценок |
|---|---|
| Обучающийся приводит полное и безошибочное определение криптографического протокола. Приводит корректное описание этапов работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами. | 3 балла |
| Обучающийся приводит полное и безошибочное определение криптографического протокола. Приводит описание основных этапов работы симметричного и асимметричного варианта протокола Нидхема-Шредера для аутентификации и обмена ключами. Описание может содержать незначительные неточности. | 2 балла |
| Обучающийся приводит корректное определение криптографического протокола. Приводит только один из вариантов (симметричный или асимметричный) протокола Нидхема-Шредера. Описание может содержать неточности. | 1 балл |
| Представлено неполное или некорректное определение криптографического протокола. Приведены неполные или некорректные описания вариантов протокола Нидхема-Шредера для аутентификации и обмена ключами. | 0 баллов |

***2. Распишите протокол Диффи-Хеллмана в классическом варианте и в варианте на эллиптических кривых.***

| Критерии оценивания | Шкала оценок |
|---|---|
| Обучающийся приводит корректные схемы распределения ключей Диффи-Хеллмана в классическом варианте и в варианте на эллиптических кривых, а также развернутое их описание. | 3 балла |
| Обучающийся приводит схемы распределения ключей Диффи-Хеллмана в классическом варианте и в варианте на эллиптических кривых и<br>краткое их описание. Описание может содержать незначительные неточности. | 2 балла |
| Приведены обе схемы распределения ключей Диффи-Хеллмана, но в них содержатся неточности. Приведена только одна из схем распределения ключей Диффи-Хеллмана (классический вариант либо вариант на эллиптических кривых). | 1 балл |
| Представлена одна их схем распределения ключей Диффи-Хеллмана (классический вариант либо вариант на эллиптических кривых). Схема содержит существенные ошибки. | 0 баллов |

***3. Опишите схему централизованного управления распределением открытых ключей.***

| Критерии оценивания | Шкала оценок |
|---|---|
| Обучающийся приводит развернутое и безошибочное описание схемы централизованного управления распределением открытых ключей. | 3 балла |
| Обучающийся приводит развернутое описание схемы централизованного управления распределением открытых ключей, которое может содержать незначительные неточности. | 2 балла |
| Обучающийся приводит недостаточно развернутое описание схемы централизованного управления распределением открытых ключей. Описание может содержать отдельные неточности. | 1 балл |
| Представлено неполное или некорректное описание схемы централизованного управления распределением открытых ключей. Присутствуют грубые ошибки или неточности. | 0 баллов |

***4. Опишите компоненты и схему работы протокола аутентификации Kerberos. Сформулируйте основные преимущества данного протокола.***

| Критерии оценивания | Шкала оценок |
|---|---|
| Обучающийся приводит развернутое и безошибочное описание схемы работы протокола аутентификации Kerberos. Корректно формулирует его преимущества. | 3 балла |
| Обучающийся приводит достаточно развернутое описание схемы работы протокола аутентификации Kerberos. Корректно формулирует его преимущества. Описание может содержать незначительные неточности. | 2 балла |
| Обучающийся приводит краткое, содержащее незначительные неточности, описание схемы работы протокола аутентификации Kerberos. Преимущества протокола не приводятся. | 1 балл |
| Представлено неполное или некорректное описание схемы работы протокола аутентификации Kerberos. Преимущества протокола сформулированы некорректно или не приводятся. | 0 баллов |

## 20.2 Промежуточная аттестация

Промежуточная аттестация может включать в себя проверку теоретических вопросов, а также, при необходимости (в случае невыполнения в течение семестра), проверку выполнения установленного перечня лабораторных заданий, позволяющих оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

Для оценки теоретических знаний используется перечень контрольно-измерительных материалов. Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает два задания - вопросов для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции. При оценивании используется количественная шкала. Критерии оценивания приведены в таблице, приведенной ниже.

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;
2. умение проводить обоснование и представление основных теоретических и практических результатов;
3. умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторных заданий;

4. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;
5. владение навыками программирования в рамках выполняемых лабораторных заданий.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

**Критерии оценивания компетенций и шкала оценок на экзамене**

| Критерии оценивания компетенций | Уровень сформированности компетенций | Шкала оценок |
|---|---|---|
| Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем. | Повышенный уровень | Отлично |
| Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем. | Базовый уровень | Хорошо |
| Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.<br>Успешно выполнены лабораторные работы в соответствии с установленным перечнем. | Пороговый уровень | Удовлетворительно |
| Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем. | – | Неудовлетворительно |

**Примерный перечень вопросов к экзамену**

| № | Содержание |
|---|---|
| 1 | Понятие криптографического протокола. Требования к криптографическим протоколам |
| 2 | Классификация криптографических протоколов |
| 3 | Атаки на криптографические протоколы |
| 4 | Жизненный цикл криптографических ключей |
| 5 | Протокол передачи сообщений с обеспечением свойства конфиденциальности |
| 6 | Протокол передачи сообщений с обеспечением свойства целостности |
| 7 | Протокол передачи сообщений с обеспечением свойства неотказуемости |
| 8 | Протоколы аутентификации на основе паролей |
| 9 | Протоколы аутентификации с использованием систем ассиметричного шифрования |
| 10 | Протокол Нидхема-Шредера (варианты) |
| 11 | Протокол Фиата-Шамира |
| 12 | Пртокол Шнора |
| 13 | Протоколы доказательства с нулевым разглашением |
| 14 | Протоколы привязки к биту |
| 15 | Протокол ключевого обмена Диффи-Хеллмана |
| 16 | Протокол ключевого обмена Диффи-Хеллмана на эллиптических кривых |
| 17 | Атаки на протоколы распределения ключей |
| 18 | Протоколы цифровой подписи |
| 19 | Протокол Kerberos |
| 20 | Инфраструктура открытых ключей |
| 21 | Семейство протоколов IPsec |
| 22 | Протоколы SSL/TLS |

**Пример контрольно-измерительного материала**

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2024

Направление подготовки / специальность 10.05.01 Компьютерная безопасность

Дисциплина Б1.О.46 Криптографические протоколы

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

**Контрольно-измерительный материал № 1**

1. Криптографические протоколы. Определение, требования, классы
2. Протокол Диффи-Хеллмана для конференц-связи

Преподаватель_____ М.А. Дрюченко