**Программа учебной дисциплины «Компьютерные сети и телекоммуникации»**

Утверждена

Академическим советом ООП

Протокол № от «\_\_»\_\_\_\_\_20\_\_ г.

|  |  |
| --- | --- |
| Автор | Пакулин Н.В, к.ф.-м.н., npak@ispras.ru |
| Число кредитов | 5 |
| Контактная работа (час.) | 64 |
| Самостоятельная работа (час.) | 126 |
| Курс | 1 |
| Формат изучения дисциплины | без использования онлайн курса. |

1. **ЦЕЛЬ, РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ПРЕРЕКВИЗИТЫ**

Целью освоения дисциплины является изучение основных средств обеспечения информационной безопасности в сетях открытых систем: криптографические примитивы, инфраструктура криптографии с открытым ключом, базовые сервисы безопасности (аутентификация, конфиденциальность и целостность), основные механизмы распределенных реестров.

Задачами данного курса являются:

• освоение студентами базовых понятий информационной безопасности в сетях открытых систем;

• формирование практических навыков использования средств выявления уязвимостей в сетях открытых систем.

В результате освоения дисциплины студент должен:

* 1. **Знать:**
* фундаментальные понятия современных сетей открытых систем;
* базовые криптографические примитивы;
* способы реализации базовых сервисов безопасности в телекоммуникационных сетях — аутентификации, целостности, конфиденциальности;
* базовые принципы протоколов обеспечения безопасности сетевого и транспортного уровня;
* методы оценки безопасности защищенных систем;
* базовые принципы построения распределенных реестров.
  1. **Уметь:**
* проектировать реализации сервисов безопасности;
* программировать сетевой обмен с использованием средств безопасности транспортного уровня TLS;
* создавать smart contracts для технологии Ethereum.
  1. **Иметь навыки (приобрести опыт):**
* освоения большого объема информации;
* самостоятельной работы с документацией по примитивам и сервисам безопасности;
* культурой разработки и реализации системного программного обеспечения современных компьютеров;
* разработки и отладки программ, использующих средства безопасности транспортного уровня.

Изучение данной дисциплины базируется на знаниях, полученных студентами при освоении учебных дисциплин:

• «Дискретная математика»,

• «Программирование»,

• «Основы криптографии»,

• «Архитектура сетей».

1. **СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

Тема 1. Введение. Понятие открытых систем. Многоуровневая модель стека протоколов. Стандартизация открытых систем.

Тема 2. Безопасность открытых систем. Основные понятия безопасности. Базовые серви-сы безопасности.

Тема 3. Базовые криптографические примитивы. Алгоритмы симметричного шифрования DES, ГОСТ, AES. Режимы шифрования. Хэш функции.

Тема 4. Алгоритмы асимметричного шифрования. Схемы RSA, Эль-Гамаля. Введение в криптографию на эллиптических кривых. Алгоритмы цифровой подписи DSA, ECDSA, ГОСТ. Инфраструктура PKI.

Тема 5. Аутентификация. Базовые криптографические средства. Пароли. Схема Challenge - Response. Многофакторная аутентификация. Аутентифицированный обмен Диффи-Хеллмана. Аутентификация в системе Kerberos. Схемы с нулевым разглашением.

Тема 6. Протоколы безопасности сетевого и транспортного уровня. Протокол IPsec. Про-токол TLS.

Тема 7. Критерии оценки защищенных систем. «Оранжевая книга». Общие критерии.

Тема 8. Введение в блокчейн. Блокчейн биткойна.

Тема 9. Блокчейн Ethereum. Смарт-контракты. Криптовалюты на базе Ethereum. Специ-фикация ERC20.

1. **ОЦЕНИВАНИЕ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Тип контроля | Форма контроля | 1 год | | |
|  |  | 1 модуль | 2 модуль |
| Текущий | Контрольная работа |  | \* |
| Итоговый | Экзамен (устный) |  | \* |

Критерии оценки знаний, навыков

В рамках курса слушателям предлагается выполнить 1 контрольную работу. За сдачу контрольной работы набираются баллы (максимум 10 баллов). Оценки за контрольную работу и экзамен выставляются по 10-ти балльной шкале.

Порядок формирования оценок по дисциплине

Оценка по курсу состоит из оценки за выполнение контрольной работы *ОКР* (10 баллов) и оценки за итоговый устный экзамен (10 баллов). В диплом выставляется результирующая оценка по учебной дисциплине, которая формируется по следующей формуле:

*Орезульт = 0,4*\**ОКР* + *0,6*\**Оэкз*

1. **ПРИМЕРЫ ОЦЕНОЧНЫХ СРЕДСТВ**

# Оценочные средства для текущего контроля студента

**Тема контрольной работы**

Необходимо разработать программу, которая диагностирует распространенные ошибки в настройке сертификатов для веб-сайтов.

Требования к программе.

1. Программа принимает на вход имя сайта и устанавливает соединение по протоколу TLS на порт 443 (HTTPS).
2. Программа должна идентифицировать следующие проблемы с сайтом:
   * Истекший срок действия сертификата. Необходимо вывести на экран допустимый срок действие сертификата.
   * Сертификат ещё не начал действовать. Необходимо вывести на экран допустимый срок действие сертификата.
   * Несоответствие имени сайта и имени сертификата. Необходимо вывести на экран доменные имена, которые допускает сертификат.
   * Недоверенный корневой сертификат. Необходимо вывести информацию о корневом сертификате.
   * Самоподписной сертификат сайта. Необходимо обосновать, что сертификат самоподписной.
   * Использование слабых алгоритмов хеширования: MD5, SHA1. Необходимо вывести на экран алгоритм, который используется в сертификате.

Программа может быть разработана на любом языке программирования.

Не допускается использование сторонних утилит, таких как команда openssl. Допускается использовать специализированные криптографические библиотеки.

Оценочные средства для промежуточной аттестации

**Вопросы для экзамена**

**Базовые понятия информационно безопасности**

1. Открытые системы. Причины возникновения. Архитектуры стеков протоколов OSI и TCP/IP. Стандартизация сетевых технологий. Задачи стандартизации.
2. Представление о безопасности сетей. Безопасность и открытые системы. Основные понятия безопасности: угрозы, атаки, уязвимости, меры безопасности, риск. Цели безопасности. Ответственность. Политика безопасности.
3. Основные сервисы безопасности. Аутентификация, конфиденциальность, целостность. Основные задачи сервисов, взаимосвязи между сервисами. Аналоги из неэлектронной сферы.
4. Оценка доверенных систем: «Оранжевая книга». Цели и задачи. Понятие об уровнях защищенности.
5. Оценка доверенных систем: Общие критерии. Цели и задачи. Понятие профиля. Понятие уровня доверия оценке.

**Криптографические средства обеспечения защиты**

1. Симметричные криптосистемы, режимы. Основные блочные шифры: DES, AES, ГОСТ. Сеть Фейстеля.
2. Криптосистемы с открытым ключом. RSA. Схема Эль-Гамаля.
3. Сертификаты. Цепочки доверия. Инфраструктура PKI.
4. Хэш-функции. Обеспечение аутентичности сообщения. Цифровая подпись. DSA и ГОСТ.
5. Основы криптографии на эллиптических кривых. Алгоритмы ECDSA и ГОСТ.
6. Аутентификация. Цели и задачи, общие концепции. Использование паролей. Уязвимости парольной схемы и меры противодействия.
7. Аутентификация. Цели и задачи, общие концепции. Применение криптосистем с открытым ключом. Обмены X.509. Общие уязвимости аутентификационных протоколов. Аутентифицированный обмен Диффи-Хеллмана.
8. Безопасность на сетевом уровне. Протокол IPsec. Протокол TLS/SSL.

**Блокчейн**

1. Блокчейн Bitcoin. Транзакции, истребование средств (redeem), вход и выход транзакций, скрипты. Майнинг, сложность, вознаграждение за майнинг. Атаки на блокчейн, повторное использование.
2. Блокчейн Ethereum. Транзакции, состояние, обновление состояния. Майнинг, proof of work, proof of stake, газ, комиссия за майнинг.
3. Смарт-контракты Ethereum. Структура контракта, storage переменные, методы, события. Вызов методов, изменение состояния при майнинге. Стандарт ERC20.
4. **РЕСУРСЫ**
   1. **Основная литература**
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 806 с.
6. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.
7. Мао B. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.
8. Бехроуз А. Фороузан. Криптография и безопасность сетей. Бином. Лаборатория знаний, 2010 г. 784 с.
   1. **Дополнительная литература**
9. Описание протоколов SSL/TLS. Информационный документ. ООО КриптоПро.  
   <https://www.cryptopro.ru/sites/default/files/docs/TLS_description.pdf>
10. IETF RFC 4031. Security Architecture for the Internet Protocol. IETF, 2005 г. 101 с.
11. IETF RFC 5246. The Transport Layer Security (TLS) Protocol Version 1.2. IETF, 2008. 104 c.
12. G. Wood. Ethereum: a Secure Decentralised Generalised Transaction Ledger. EIP-150 rev. 32
13. Andreas M. Antonopoulos. Mastering Bitcoin: Programming the Open Blockchain 2nd Edition. O’Reily, 2016. 408 c.