Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Криптографические протоколы

по направлению подготовки / специальности

**10.05.01 Компьютерная безопасность**

Направленность (профиль) подготовки/ специализация:
**Анализ безопасности компьютерных систем**

Форма обучения
**Очная**

Квалификация
**Специалист по защите информации**

Год приема
**2025**

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

## 1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-10.1 Осуществляет анализ тенденций развития методов и средств криптографической защиты информации

ИОПК-10.2 Применяет средства криптографической защиты информации при решении задач профессиональной деятельности

ИОПК-13.1 Предпринимает необходимые действия по сбору и анализу исходных данных для проектирования компонент программных и программно-аппаратных средств защиты информации в компьютерных системах

ИОПК-13.2 Определяет параметры функционирования, архитектуру и интерфейсы компонент программных и программно-аппаратных средств защиты информации в компьютерных системах

ИОПК-13.3 Проводит анализ компонент программных и программно-аппаратных средств защиты информации в компьютерных системах с целью определения уровня обеспечиваемой ими защищенности и доверия

ИОПК-2.2 Определяет порядок настройки и эксплуатации программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности

ИОПК-2.3 Формулирует предложения по применению программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности

ИПК-2.1 Определяет угрозы безопасности и их возможные источники, каналы утечки информации

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации

ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации

ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием

## 2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– лабораторной работы.

Пример типового варианта задания для лабораторной работы:

- Требуется программно реализовать схему одноразовых паролей Лэмпорта (S/KEY). Описание криптографического протокола можно найти в слайдах лекций и rfc-документах: S/KEY (RFC 1760), https://datatracker.ietf.org/doc/html/rfc1760, A One-Time Password System (RFC 2289), https://datatracker.ietf.org/doc/html/rfc2289. При этом нужно найти партнера по заданию: один “пишет” клиента, другой - сервер, либо использовать технику парного программирования. При реализации возможны модификации и упрощения оригинала, которые не затрагивают базовые принципы работы протокола. В отчете по лабораторной работе требуется кратко описать спецификацию реализованного протокола, важные детали и особенности реализации, формат сообщений протокола, используемые классы и методы, а также структуры данных, приводятся выборочные примеры кода программы. Лабораторная работа "сдается" преподавателю обоими исполнителями на базе подготовленного стенда и типовых сценариев работы, в которых демонстрируется штатный/нештатный режимы работы протокола.

Возможные варианты лабораторных заданий
(ИОПК-10.1, ИОПК-10.2, ИОПК-13.1, ИОПК-13.2, ИОПК-13.3,
ИОПК-2.2, ИОПК-2.3, ИПК-2.1, ИПК-2.2, ИПК-2.3, ИПК-3.2):

1. Реализовать протокол MS-CHAP.
2. Реализовать протокол Диффи - Хеллмана.
3. Реализовать протокол Нидхема-Шредера.
4. Реализовать протокол Ву-Лама.
5. Реализовать протокол Фиата-Шамира.
6. Реализовать цифровую подпись со скрытым каналом.
7. Реализовать неоспоримую цифровую подпись.
8. Реализовать цифровую подпись с назначенным проверяющим.
9. Реализовать отметку о времени создания документа.
10. Реализовать протокол электронного голосования.
11. Реализовать безопасное совместное вычисление.
12. Реализовать вычисление с шифрованными данными.
13. Реализовать депонирование ключей.
14. Реализовать раскрытие секретов по принципу «все или ничего».
15. Реализовать протокол сертифицированной электронной почты.
16. Реализовать протокол электронного аукциона.

Выполнение лабораторной работы/контрольного задания оценивается в 100 баллов:

0-20 Студент не разбирается в задаче, не знает методов решения, не отвечает, либо отвечает, но с грубыми ошибками на вопросы преподавателя.

21-40 Студент слабо разбирается в задаче, плохо знает методы решения, не отвечает, либо отвечает, но с ошибками на вопросы преподавателя.

41-60 Студент в целом удовлетворительно разбирается в задаче, использует методы решения при подсказке преподавателя, отвечает на вопросы неуверенно, но с негрубыми ошибками. Представляет работу на защите удовлетворительно.

61-80 Студент в целом уверенно разбирается в задаче, знает и использует методы решения практически самостоятельно, отвечает на вопросы с замечаниями. Представляет работу на защите в целом хорошо, с замечаниями.

81-100 Студент отлично разбирается в задаче, знает и использует методы решения самостоятельно, отвечает на вопросы уверенно. Представляет работу на защите отлично, уверенно.

Допуском до экзамена является выполнение 80% лабораторных работ с оценкой за каждую не менее 50 баллов.

**3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания**

Экзамен в девятом семестре проводится в устной/письменной форме с использованием перечня контрольных вопросов по курсу. Схема вопросов экзамена должна соответствовать компетентностной структуре дисциплины. При оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций. Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Примерный перечень контрольных вопросов к экзамену:

1. Действия противника при атаке на криптографические протоколы.
2. Свойства, характеризующих безопасность криптографических протоколов.
3. Общие предположения криптоанализа протоколов.
4. Классификация криптографических протоколов.
5. Протоколы аутентификации сообщений (ПАС), когда стороны доверяют друг другу.
6. ПАС, когда стороны не доверяют друг другу.
7. Атаки на ПАС и защита от них.
8. Виды протоколов идентификации на основе паролей
9. Схема Лэмпорта (протокол S/KEY).
10. Протокол CHAP/MS-CHAP
11. Протоколы идентификации (ПИ) на основе техники “запрос-ответ” с использованием симметричного шифрования
12. ПИ на основе техники “запрос-ответ” с использованием асимметричного шифрования
13. ПИ на основе техники “запрос-ответ” с использованием цифровой подписи
14. Протокол идентификации ISO и атака на него.
15. Протокол идентификации Нидхема-Шредера (NSPK) и атака на него.
16. Протокол идентификации Фиата-Шамира (свойства).
17. Протокол идентификации GQ (свойства).
18. Протокол идентификации Шнора (свойства).
19. Доказательство с нулевым разглашением гамильтонова цикла в графе.
20. Протокол привязки к биту (общая схема). Свойства связывания и сокрытия.
21. Протокол передачи ключей на основе техники “запрос-ответ”
22. “Бесключевой” протокол А.Шамира и атака на него.
23. Протокол широкоротой лягушки и атака на него
24. Протокол Нидхема-Шредера (NS) и атака на него
25. Протокол Kerberos.
26. Протокол передачи ключей Нидхема-Шредера (NSPK).
27. Протокол Oakley
28. Протокол Ву-Лама и атака на него.
29. Протоколы передачи ключей с использованием ЦП.
30. Протокол EKE (Encrypted Key Exchange) и атака на него.
31. Инфраструктура сертификатов открытых ключей.

32. Протокол DH (Диффи-Хеллмана) и атака “человек посередине”.
33. Протокол STS (station-to-station) и атака на него
34. Протокол MTI (Мацумото-Такашима-Имаи) и атака на него
35. Формальная схема $S(n)$ ПРК для сети с $n$ абонентами.
36. Неравенство Блома.
37. Схема Блома.
38. KDP($n$,$q$) - схема.
39. Пороговая схема А.Шамира.
40. Протокол DH с тремя участниками.
41. Протоколы AH и ESP. Туннельный и транспортный режимы IPSec.
42. Понятие защищенной ассоциации (SA). Организация работы IPsec.
43. Протокол SKEME.
44. Протокол ISAKMP (особенности, назначение, принципы работы).
45. Протокол IKE (особенности, назначение, принципы работы).
46. Протокол SSL/TLS (фаза рукопожатия - аутентификация и распределение ключа).

Критерии оценивания промежуточной аттестации:

Отлично - студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении *всех* лабораторных работ.

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал требуемые умения и навыки при выполнении *большинства* лабораторных работ.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, а также показал требуемые умения и навыки при выполнении *части* лабораторных работ.

Неудовлетворительно - студент имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины и не показал требуемые умения и навыки при выполнении части лабораторных работ.

## 4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Примерный перечень контрольных вопросов для проверки остаточных знаний (при оценивании необходимо продемонстрировать достижение **всех** запланированных индикаторов достижения компетенций):

1. Действия противника при атаке на криптографические протоколы.
2. Свойства, характеризующих безопасность криптографических протоколов.
3. Общие предположения криптоанализа протоколов.
4. Классификация криптографических протоколов.
5. Протоколы аутентификации сообщений (ПАС).
6. Атаки на ПАС и защита от них.
7. Виды протоколов идентификации на основе паролей
8. Схема Лэмпорта (протокол S/KEY).
9. Протокол CHAP/MS-CHAP.
10. Протоколы идентификации на основе техники “запрос-ответ”.
11. Протокол идентификации ISO.
12. Протокол идентификации Нидхема-Шредера.
13. Протокол идентификации Фиата-Шамира.
14. Протокол идентификации GQ.
15. Протокол идентификации Шнора.

16. Доказательство с нулевым разглашением гамильтонова цикла в графе.
17. Протокол передачи ключей на основе техники “запрос-ответ”
18. “Бесключевой” протокол А.Шамира.
19. Протокол передачи ключей широкоротой лягушки.
20. Протокол передачи ключей Нидхема-Шредера.
21. Протокол передачи ключей Kerberos.
22. Протокол передачи ключей Oakley
23. Протокол передачи ключей Ву-Лама.
24. Протоколы передачи ключей с использованием ЦП.
25. Протокол EKE (Encrypted Key Exchange).
26. Инфраструктура сертификатов открытых ключей.
27. Протокол DH (Диффи-Хеллмана).
28. Протокол STS (station-to-station).
29. Протокол MTI (Мацумото-Такашима-Имаи).
30. Схема Блома.
31. KDP($n$,$q$) - схема.
32. Пороговая схема А.Шамира.
33. Протокол DH с тремя участниками.
34. Протоколы AH и ESP. Туннельный и транспортный режимы IPSec.
35. Понятие защищенной ассоциации (SA). Организация работы IPsec.
36. Протокол SKEME.
37. Протокол ISAKMP (особенности, назначение, принципы работы).
38. Протокол IKE (особенности, назначение, принципы работы).
39. Протокол SSL/TLS (фаза рукопожатия).

**Информация о разработчиках**

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности НИ ТГУ.