МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____А.В. Замятин
«_02_» ___июля_____ 2021 г.

Фонд оценочных средств по дисциплине

Криптографические протоколы

Специальность
10.05.01 Компьютерная безопасность
код и наименование специальности

Анализ безопасности компьютерных систем
наименование специализации

Томск–2021

ФОС составил:
канд. техн. наук,
доцент кафедры компьютерной безопасности  В.Н. Тренькаев

Рецензент:
канд. техн. наук,
заведующий кафедрой компьютерной безопасности  С.А. Останин

Фонд оценочных средств одобрен на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор  С.П. Сущенко

Фонд оценочных средств (ФОС) является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	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	ОР-2.2.1 Уметь: формулировать предложения по применению программных средств, реализующих криптографические протоколы	Отлично сформированное умение формулировать предложения по применению программных средств, реализующих криптографические протоколы	Хорошее умение формулировать предложения по применению программных средств, реализующих криптографические протоколы	Удовлетворительное умение формулировать предложения по применению программных средств, реализующих криптографические протоколы .	Неудовлетворительное умение формулировать предложения по применению программных средств, реализующих криптографические протоколы

	отечественного производства, используемых для решения задач профессиональной деятельности.					
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	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.	ОР-10.1.1 Знать: типовые криптографические протоколы, используемые в компьютерных сетях	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.
ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.	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	ОР-13.1.1 Уметь: разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы	Отлично сформированное умение разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы	Хорошее умение разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы предложения по применению программных средств, реализующих	Удовлетворительное умение разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы .	Неудовлетворительное умение разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы

	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.			криптографические протоколы		
ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей	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	ОР-2.1.1 Знать: типовые атаки на криптографические протоколы	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

ПК-3 Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей	ИПК-3.2 Разработка проектов программных и аппаратных средств защиты информации в соответствии с техническим заданием	ОР-3.2.1 Знать: основные типы криптографических протоколов и принципы их построения с использованием шифрсистем	Высокий уровень знаний; способность самостоятельного анализа проблем предметной области.	В целом успешные, но содержащие отдельные пробелы знания.	Фрагментарные, неполные знания без грубых ошибок.	Не имеет четкого представления об изучаемом материале, допускает грубые ошибки.

2. Этапы формирования компетенций и виды оценочных средств

№	**Этапы формирования компетенций (разделы дисциплины)**	**Код и наименование результатов обучения**	**Вид оценочного средства** (тесты, задания, кейсы, вопросы и др.)
1.	Введение в криптографические протоколы	ОР-10.1.1, ОР-2.1.1 ОР-10.1.1 Знать: типовые криптографические протоколы, используемые в компьютерных сетях ОР-2.1.1 Знать: типовые атаки на криптографические протоколы	лабораторные работы, контрольные задания, опросы на занятиях
2	Протоколы аутентификации сообщений	ОР-3.2.1, ОР-2.1.1 ОР-3.2.1 Знать: основные типы криптографических протоколов и принципы их построения с использованием шифрсистем ОР-2.1.1 Знать: типовые атаки на криптографические протоколы	лабораторные работы, контрольные задания, опросы на занятиях
3.	Протоколы идентификации	ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1 ОР-3.2.1 Знать: основные типы криптографических протоколов и принципы их построения с использованием шифрсистем ОР-2.1.1 Знать: типовые атаки на криптографические протоколы ОР-2.2.1 Уметь: формулировать предложения по применению программных средств, реализующих криптографические протоколы ОР-13.1.1 Уметь: разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы	лабораторные работы, контрольные задания, опросы на занятиях
4.	Протоколы распределения ключей	ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1 ОР-3.2.1 Знать: основные типы криптографических протоколов и принципы их построения с использованием шифрсистем ОР-2.1.1 Знать: типовые атаки на криптографические протоколы ОР-2.2.1 Уметь: формулировать предложения по применению программных средств, реализующих криптографические протоколы ОР-13.1.1 Уметь: разрабатывать компоненты программных средств защиты информации, реализующих	лабораторные работы, контрольные задания, опросы на занятиях

		криптографические протоколы	
5.	Групповые криптографические протоколы	ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1 ОР-3.2.1 Знать: основные типы криптографических протоколов и принципы их построения с использованием шифрсистем ОР-2.1.1 Знать: типовые атаки на криптографические протоколы ОР-2.2.1 Уметь: формулировать предложения по применению программных средств, реализующих криптографические протоколы ОР-13.1.1 Уметь: разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы	лабораторные работы, контрольные задания, опросы на занятиях
6.	Прикладные криптографические протоколы	ОР-3.2.1, ОР-2.1.1, ОР-2.2.1, ОР-13.1.1 ОР-3.2.1 Знать: основные типы криптографических протоколов и принципы их построения с использованием шифрсистем ОР-2.1.1 Знать: типовые атаки на криптографические протоколы ОР-2.2.1 Уметь: формулировать предложения по применению программных средств, реализующих криптографические протоколы ОР-13.1.1 Уметь: разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы	лабораторные работы, контрольные задания, опросы на занятиях

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине.

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. В отчете по заданию требуется описать спецификацию реализованного протокола, важные детали и особенности реализации, формат сообщений протокола и пр. Лабораторная работа "сдается" преподавателю обоими исполнителями на базе подготовленного стенда и типовых сценариев работы, в которых демонстрируется штатный/нештатный режимы протокола.

Возможные варианты лабораторных заданий:

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

Типовые контрольные задания для текущего контроля:

1. Криптографический протокол.
2. Нарушитель. Противник.
3. Сервис безопасности.
4. Аутентификация сторон
5. Аутентификация источника данных
6. Отказ от авторства.
7. Приписывание авторства.
8. Атака на криптографический протокол.
9. Совершенная стойкость.
10. Строгое соблюдение типов.
11. Честность участников.
12. Аутентификация ключа.
13. Подтверждение правильности ключа.
14. Атака путем подмены участника
15. Атака повторением
16. Атака путем чередования сообщений
17. Атака отражением
18. Атака с параллельными сеансами
19. Атака «человек посередине»

20. Протокол аутентификации сообщений (ПАС)
21. Протокол идентификации (ПИ)
22. Протокол передачи ключей
23. Протокол открытого распределения ключей (ОРК)
24. Протокол предварительного распределения ключей (ПРК)
25. Стойкость к m-кратной компрометации ключей протокола ПРК.
26. Групповой протокол.
27. Протокол разделения секрета.
28. Цифровой сертификат.
29. Техника доказательства знаний
30. Полнота протокола доказательства знания
31. Корректность протокола доказательства знания
32. Нулевое разглашение протокола доказательства знания.
33. VPN - туннель
34. Туннельный режим (IPSec).
35. Транспортный режим (IPSec).
36. Свойство ключа: невозможность несанкционированного использования
37. Свойство ключа: конфиденциальность
38. Свойство ключа: аутентичность.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине.

Примерный перечень 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. 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.
11. 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 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.
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).
47. Жизненный цикл ключей (от регистрации пользователя до аннулирования ключа).

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Текущий контроль подразумевает выполнение лабораторных работ/контрольных заданий. 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/контрольных заданий, с оценкой за каждую не менее 80 баллов.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточный контроль знаний по дисциплине осуществляется в форме экзамена, который подразумевает подготовку студента и ответов в устной/письменной форме на несколько контрольных вопросов по всему курсу. Критерии выставления оценок:

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

Хорошо - студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Удовлетворительно - студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Неудовлетворительно - студент имеет существенные пробелы по отдельным теоретическим разделам специальной дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных занятиях.