МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2026

Рабочая программа дисциплины (модуля) «Криптографические протоколы» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Етчо С.А.

Шумик Е.Г.

Утверждена на заседании кафедры информационной безопасности от 14.05.2026 , протокол № 8

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат	eg_1575874368
Номер транзакции	0000000000FB27B9
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Дисциплина "Криптографические протоколы" обеспечивает приобретение знаний иумений в соответствии с государственным образовательным стандартом, содействуетформированию мировоззрения и системного мышления.Целью преподавания дисциплины "Криптографические протоколы" являетсяформирование представления об использования криптографических протоколов длязащиты информации, о принципах применения совершенных информационныхтехнологий.

Задачи дисциплины:

дать основы знаний об основных криптографических протоколах;

познакомить с методикой выбора и оценки их качества.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-10 : Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1к : Понимает основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	РД1	Знание	типовые криптографические протоколы, используемые в компьютерных сетях
			РД2	Умение	разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Развитие патриотизма и гражданской ответственности	Гражданственность	Внимательность к деталям
Формирование духовно-нравственных ценностей		
Воспитание нравственности, милосердия и сострадания	Взаимопомощь и взаимоуважение	Внимательность к деталям

Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Служение Отечеству и ответственность за его судьбу	Дисциплинированность
Формирование коммуникативных навыков и культуры общения		
Развитие умения эффективно общаться и сотрудничать	Гражданственность	Доброжелательность и открытость

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Криптографические протоколы» относится к базовой части «Блока 1Дисциплины (модули)» учебного плана специальности 10.05.03 «Информационнаябезопасность автоматизированных систем».Входными требованиями, необходимыми для освоения дисциплины, являетсяналичие у обучающихся компетенций, сформированных при изучении дисциплин и/илипрохождении практик «Алгебра и геометрия», «Криптографические методы защиты информации», «Основы информационной безопасности». На данную дисциплинуопираются «Производственная практика по получению профессиональных умений и опыта профессиональной деятельности», «Угрозы информационной безопасности автоматизированных систем».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обуче-ния	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудо-емкость	Объем контактной работы (час)						СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная			Внеауди-торная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	8	4	70	36	18	0	1	15	74	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы		Кол-во часов, отведенное на	Форма

		Код результата обучения	Лек	Практ	Лаб	СРС	текущего контроля
1	Введение в криптографические протоколы	РД1, РД2	6	4	0	15	практическое задание
2	Протоколы аутентификации сообщений	РД1, РД2	6	2	0	15	практическое задание
3	Протоколы идентификации	РД1, РД2	6	2	0	15	практическое задание
4	Протоколы распределения ключей	РД1, РД2	6	4	0	15	практическое задание
5	Групповые криптографические протоколы.	РД1, РД2	6	2	0	15	практическое задание
6	Прикладные криптографические протоколы	РД1, РД2	6	4	0	15	практическое задание
Итого по таблице			**36**	**18**	**0**	**90**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Введение в криптографические протоколы.

Содержание темы: Основные понятия. Классификация криптографических протоколов. Атаки на криптографические протоколы. Свойства, характеризующие безопасность протоколов.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 2 Протоколы аутентификации сообщений.

Содержание темы: Схема имитозащиты. Оптимальные коды аутентификации. Атаки на протоколы аутентификации сообщений.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 3 Протоколы идентификации.

Содержание темы: Парольные схемы идентификации. Протоколы идентификации на основе техники “запрос-ответ”. Протоколы идентификации на основе техники доказательства знания. Протоколы с нулевым разглашением. Схема Лэмпорта (S/KEY) Протокол CHAP/MS-CHAP Атаки на протоколы идентификации.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 4 Протоколы распределения ключей.

Содержание темы: Протоколы передачи ключей Протоколы открытого распределения ключей Протоколы предварительного распределения ключей Протокол Диффи – Хеллмана. Протокола Oakley. Атаки на протоколы распределения ключей.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 5 Групповые криптографические протоколы.

Содержание темы: Схемы разделение секрета. Схемы цифровой подписи. Атаки на групповые криптографические протоколы.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

Тема 6 Прикладные криптографические протоколы.

Содержание темы: Семейство протоколов IPsec.. Протокол SSL/TLS. VPN-протоколы.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекция, практическое занятие.

Виды самостоятельной подготовки студентов по теме: подготовка к практическому занятию.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которуюони совершают без непосредственной помощи и указаний преподавателя, руководствуясьсформировавшимися ранее представлениями о порядке и правильности выполненияопераций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и вформировании умений и навыков по их использованию в новых условиях на новом учебномматериале. Самостоятельная работа призвана обеспечивать возможность осуществлениястудентами самостоятельной познавательной деятельности в обучении, и является видомучебного труда, способствующего формированию у студентов самостоятельности. Вданной учебной программе приведен перечень основных и дополнительных источников,которые предлагается изучить в процессе облучения по дисциплине. Кроме того, длярасширения и углубления знаний по данной дисциплине целесообразно использовать:научные публикации в тематических журналах; полнотекстовые базы данных библиотеки;имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажныхносителях. Успешное освоение дисциплины предполагает активную работу студентов навсех занятиях аудиторной формы: лекций и практических занятий, выполнениеаттестационный мероприятий, эффективную самостоятельную работу.

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560977 (дата обращения: 01.09.2025).

2. Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536453 (дата обращения: 19.05.2026).

3. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2025. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560804 (дата обращения: 01.09.2025).

7.2 Дополнительная литература

1. Кунин, Н. Т. Криптографические методы защиты информации : методические указания / Н. Т. Кунин, Ю. А. Паршенкова. — Москва : РТУ МИРЭА, 2023. — 32 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/368738 (дата обращения: 25.05.2026). — Режим доступа: для авториз. пользователей.

2. 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: 25.05.2026). — Режим доступа: для авториз. пользователей.

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "ЛАНЬ"
3. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
4. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
5. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры

Программное обеспечение:

- Microsoft Office Pro Plus 2019 MAK
- Microsoft Windows 10 Home SL

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2022

Форма обучения
очная

Владивосток 2026

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-10 : Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1к : Понимает основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-10 «Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-10.1к : понимает основные принципы построения средств криптографической и технической защиты информации для решения задач профессиональной деятельности	РД 1	Знание	типовые криптографические протоколы, используемые в компьютерных сетях	выполнение тестовых заданий
	РД 2	Умение	разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы	выполнение практических заданий

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения	Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
		Текущий контроль	Промежуточная аттестация
Очная форма обучения			

РД1	Знание : типовые криптографические протоколы, используемые в компьютерных сетях	1.1. Введение в криптографические протоколы	Тест	Экзамен в устной форме
		1.2. Протоколы аутентификации сообщений	Тест	Экзамен в устной форме
		1.3. Протоколы идентификации	Тест	Экзамен в устной форме
		1.4. Протоколы распределения ключей	Тест	Экзамен в устной форме
		1.5. Групповые криптографические протоколы.	Тест	Экзамен в устной форме
		1.6. Прикладные криптографические протоколы	Тест	Экзамен в устной форме
РД2	Умение : разрабатывать компоненты программных средств защиты информации, реализующих криптографические протоколы	1.1. Введение в криптографические протоколы	Практическая работа	Экзамен в устной форме
		1.2. Протоколы аутентификации сообщений	Практическая работа	Экзамен в устной форме
		1.3. Протоколы идентификации	Практическая работа	Экзамен в устной форме
		1.4. Протоколы распределения ключей	Практическая работа	Экзамен в устной форме
		1.5. Групповые криптографические протоколы.	Практическая работа	Экзамен в устной форме
		1.6. Прикладные криптографические протоколы	Практическая работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест	Практическое занятие	Экзамен	Итого
Лекционные занятия	20			20
Практическое занятие		60		60
Промежуточная аттестация			20	20
Итого	20	60	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.

от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Примеры тестовых заданий

1 Протокол, обеспечивающий поддержку функций безопасности с применением

А) криптографических методов защиты информации, называется

Б) криптографический протокол

В) протокол передачи данных

Г) протокол обеспечения безопасности

2 Для обеспечения свойств защищаемой информации в протоколах применяются…

А) модели угроз

Б) политики безопасности

В) функции безопасности

3 Методами защиты криптографических протоколов от атак повтора являются

А) нумерация сообщений, метки времени, шифрование

Б) нумерация сообщений, метки времени, нонсы

В) нумерация сообщений, метки времени, нонсы, хэш-функции

4 Недостатком метода нумерации сообщений как метода защиты от атак повтора является…

А) непредсказуемость их значений

Б) цикличность их значений

В) непредсказуемость их значений

необходимость синхронизации времени всех пользователей в сети

5 Примитивный криптографический протокол предназначен для …

А) использования в виде базового компонента при построении прикладных

Б) криптографических протоколов

В) решения практических задач обеспечения функций безопасности с помощью криптографических систем

аутентификации и идентификации пользователей криптографической системы

6 Криптографический протокол, предназначенный для решения практических задач обеспечения функций безопасности с помощью криптографических систем, называется

А) примитивный

Б) распределенный

В) прикладной

7 Какой криптографический механизм используется для обеспечения целостности передаваемых сообщений

А) вычисление кода аутентификации сообщения от зашифрованных полей сообщения

Б) шифрование передаваемого сообщения на основе симметричной схемы шифрования

В) вычисление кода аутентификации сообщения от всех полей сообщения

8 Какой криптографический механизм используется для обеспечения свойства неотказуемости при передаче сообщений

А) шифрование симметричным алгоритмом

Б) электронная подпись

В) вычисление кода аутентификации сообщения

9 Если в процессе выполнения протокола нарушено хотя бы одно свойство безопасности, то …

А) протокол должен предусматривать возможность выбора участниками дальнейших действий

Б) протокол должен завершаться с ошибкой

В) протокол должен выполняться дальше

10 Если для обеспечения целостности сообщения применяется хэш-функция, то она должна вычисляться …

А) от всего сообщения

Б) только от полей сообщения, содержащих зашифрованную информацию

В) только от нонсов

11 Протоколы, которые позволяют выработать общий секретный ключ, не передавая его по каналу связи, называются

А) протоколы явного обмена ключами

Б) протоколы взаимного обмена ключами

В) протоколы неявного обмена ключами

12 Протоколы, в которых ключ в явном виде передается по каналу связи, называются

А) протоколы неявного обмена ключами

Б) протоколы слепой подписи

В) протоколы явного обмена ключами

13 Специфическим свойством протоколов электронных платежных систем является

А) целостность

Б) неотслеживаемость

В) конфиденциальность

14 Неотслеживаемость обеспечивается с помощью механизма…

А) кодов аутентификации сообщений

Б) слепой подписи

В) шифрования

15 Протоколы аутентификации участника информационного обмена предназначены …

А) для подтверждения источника информации в любой момент времени.

Б) для подтверждения участника протокола на время сеанса связи.

В) для подтверждения принимающего информация субъекта системы.

16 Цифровой документ, который связывает открытый ключ с его владельцем, называется

А) сертификат открытого ключа

Б) сертификат ключа формирования электронной подписи

В) сертификат безопасности

17 Для обеспечения конфиденциальности в протоколе ESP применяется

А) шифрование на основе асимметричных схем шифрования

Б) шифрование на основе симметричных схем шифрования

В) электронная подпись

18 В протоколах аутентификации без знания взаимных секретов…

А) проверяющий знает конфиденциальную информацию доказывающего.

Б) доказывающий убеждает проверяющего в подлинности заявленного им имени без

В) предъявления своих секретов.

Г) проверяющий не знает конфиденциальную информацию доказывающего перед началом протокола и определяет ее в результате выполнения протокола.

19 Протокол IKE предназначен для…

А) аутентификации участников протокола и выработки общего секретного ключа

Б) передачи информации с обеспечением конфиденциальности

В) механизма реализации слепой электронной подписи

20 Протокол OCSP предназначен для…

А) взаимной аутентификации клиента и сервера перед установлением связи между ними

Б) передачи информации с обеспечением конфиденциальности

В) проверки статуса сертификата открытого ключа.__

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа.

Шкала оценки

Оценка	Баллы	Описание
5	5	Студент допустил не более 2х ошибок
4	4	Студент совершил от 3 до 6 ошибок в ответах на тест
3	2-3	Студент совершил от 7 до 10 ошибок в ответах на тест
2	0-1	Студент совершил 11 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

1. Введение в криптографические протоколы

Задача: Изучить основные понятия криптографических протоколов, реализовать простой протокол обмена сообщениями с симметричным шифрованием (например, используя AES) и проанализировать его безопасность.

2. Протоколы аутентификации сообщений

Задача: Реализовать и протестировать протокол аутентификации сообщений на основе HMAC (например, с использованием SHA-256), провести сравнение с простым цифровым подписыванием.

3. Протоколы идентификации

Задача: Разработать и реализовать протокол идентификации пользователя, например, используя схему протокола «Вызов-Ответ» (Challenge-Response) на основе хеширования пароля.

4. Протоколы распределения ключей

Задача: Смоделировать процесс распределения общего сеансового ключа с использованием протокола Диффи-Хеллмана, проанализировать устойчивость протокола к атакам "человек посередине".

5. Групповые криптографические протоколы

Задача: Исследовать и реализовать протокол группового обмена ключами, например, на основе расширения Диффи-Хеллмана для нескольких участников, проверить корректность и безопасность обмена.

6. Прикладные криптографические протоколы

Задача: Спроектировать и реализовать протокол защищенной электронной почты, включая шифрование, цифровую подпись и аутентификацию получателя, используя стандарты PGP или S/MIME.

Краткие методические указания

На выполнение одной практической работы отводится не менее одного двухчасового занятия. После выполнения каждой практической работы студент должен представить

отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/ или неверно применил методы необходимые его выполнения.

5.3 Вопросы к экзамену

1. Что такое криптографический протокол и какова его основная задача?
2. В чем разница между симметричным и асимметричным шифрованием?
3. Опишите процесс шифрования и дешифрования при использовании протокола обмена сообщениями на основе AES.
4. Что такое HMAC и как он используется для аутентификации сообщений?
5. Как работает протокол Challenge-Response для идентификации пользователя?
6. Какие основные этапы включает процесс распределения ключей в протоколе Диффи-Хеллмана?
7. Почему протокол Диффи-Хеллмана уязвим к атаке «человек посередине» и как можно защититься от такой атаки?
8. Объясните, что такое цифровая подпись и как она обеспечивает целостность и подлинность данных.
9. Какие требования предъявляются к генерации случайных чисел в криптографических протоколах?
10. В чем суть групповых криптографических протоколов и какие задачи они решают?
11. Опишите принцип работы протокола Burmester-Desmedt.
12. Что такое ключевой обмен в криптографии и почему он важен?
13. Какие основные угрозы безопасности существуют при реализации криптографических протоколов?
14. Как обеспечивается аутентификация отправителя и получателя в протоколах защищенной электронной почты?
15. Что такое PGP и какие основные функции он выполняет?
16. В чем заключается отличие между цифровой подписью и HMAC?
17. Какие типы атак могут быть направлены на протоколы идентификации?
18. Какова роль хеш-функций в криптографических протоколах?
19. Объясните, как протоколы распределения ключей обеспечивают секретность обмена данными.
20. Какие преимущества и недостатки имеет симметричное шифрование по сравнению с асимметричным в практических криптографических протоколах?

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.

4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.