

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Вишневский Дмитрий Александрович
Должность: Ректор
Дата подписания: 20.10.2025 11:05:46
Уникальный программный ключ:
03474917c4d012283e5ad996a48a5e700f8da057

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и
автоматизации производственных процессов
Кафедра интеллектуальных систем и информационной безопасности



УТВЕРЖДАЮ
И.о. проректора
по учебной работе

Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические интерфейсы

(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем

(код, наименование специальности)

Безопасность открытых информационных систем

(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Криптографические интерфейсы» предоставить студентам теоретические знания и практические навыки по основам базовых знаний в области защиты информации, анализа стойкости алгоритмов шифрования.

Задачи изучения дисциплины. Приобретение студентами знаний, умений и практических навыков, необходимых для изучения основополагающих принципов разработки надежных протоколов защищенной передачи данных, помехоустойчивой передачи сообщений, теории информации, теории кодирования.

Дисциплина направлена на формирование общепрофессиональных (ОПК-14) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по направлениям подготовки 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности. Основывается на базе дисциплин: «Физика», «Математический анализ», «Основы теории электрических цепей», «Информатика», «Математические основы криптографии», «Криптографические методы защиты информации».

Является основой для изучения следующих дисциплин: «Технология построения защищенных распределенных приложений», «Программно-аппаратные средства обеспечения информационной безопасности», «Защита информации».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения общепрофессиональных задач деятельности, связанных с применением вычислительных систем в области информационной безопасности.

Курс является фундаментом для ориентации студентов в сфере разработки защищенных информационных систем.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единицы, 180 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия и самостоятельная работа студента (108 ак.ч.).

Дисциплина изучается на 4 курсе в 7 семестре. Форма промежуточной аттестации – дифференцированный зачет. По дисциплине предусмотрена курсовая работа.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Криптографические интерфейсы» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14	ОПК-14.1 Осуществляет разработку и внедрение автоматизированных систем с учетом требований по защите информации

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 5 зачётных единицы, 180 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к лабораторным занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к дифференцированному зачету.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		7
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	108	108
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	14	14
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	20	20
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	17	17
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	18	18
Работа в библиотеке	18	18
Подготовка к диф. зачету	12	12
Промежуточная аттестация – диф.зачет (ДЗ)	ДЗ	ДЗ
Общая трудоемкость дисциплины		
ак.ч.	180	180
з.е.	5	5

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 4 темы:

- тема 1 Использование Microsoft CryptoAPI и CNG. Структура и интерфейсы CNG;
- тема 2 Основы разработки криптопровайдеров;
- тема 3 Реализации криптографических алгоритмов в рамках криптопровайдера;
- тема 4 Знакомство с криптографическими библиотеками различных языков программирования.

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Использование Microsoft CryptoAPI и CNG. Структура и интерфейсы CNG	Криптографические интерфейсы. Назначение криптографических интерфейсов. Примеры криптографических АПИ. Структура CNG. Криптопровайдеры. Отличия от Crypto API. Гибридное шифрование.	8	-	-	CryptoAPI	6
2	Основы разработки криптопровайдеров	Использование CNG. Порядок получения хэш- суммы. Порядок выполнения симметричного шифрования. Порядок выполнения асимметричного шифрования. Порядок создания ЭЦП. Обмен ключами.	8	-	-	Симметричное и асимметричное шифрование данных средствами криптографического пакета OpenSSL Создание криптографических сообщений с использованием интерфейса Microsoft CryptoAPI и цифровых сертификатов x.509	4 4

Окончание таблицы 3

1	2	3	4	5	6	7	8	
3	Реализации криптографических алгоритмов в рамках криптопровайдера	Имитовставки. Способы генерации модификатора ключа. Протоколы обмена ключами. Примеры. Протокол Диффи-Хэлламана. Алгоритмы распределения ключей с использованием третьей доверенной стороны. Инфраструктура открытых ключей. Принципы работы. Преимущества и недостатки. Возможные уязвимости. Цепочки сертификатов. Структура сертификата X.509. Форматы хранения сертификатов.	10	-	-	Реализация защищенной передачи данных по протоколу TLS средствами криптографического пакета OpenSSL Практическое использование PGP и GPG для обеспечения конфиденциальности и целостности данных	4 6	∞
4	Знакомство с криптографическими библиотеками различных языков программирования	Объединение блочных шифров. Принцип работы. Преимущества и недостатки. Примеры схем. Цифровая подпись. Принцип работы. Подпись на основе алгоритма RSA. DSA.	10	-	-	Электронно-цифровая подпись Аутентификация сообщения	6 6	
Всего аудиторных часов		36		-		36		

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-14	Дифференцированный зачет	Комплект контролирующих материалов для экзамена

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

- рефераты (2 шт.) – всего 20 баллов;
- практические работы – всего 80 баллов.

Оценка по дифференцированному зачету проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Дифференцированный зачет по дисциплине «Криптографические интерфейсы» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку в форме устного собеседования по приведенным ниже вопросам.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

1. Исторические и теоретические аспекты

1. Эволюция криптографических интерфейсов: от DES до постквантовых алгоритмов.
2. Принцип Керхгоффа и его значение для современных криптосистем.
3. Сравнение архитектуры CryptoAPI и CNG.
4. Криптография в открытом ключе: от Диффи-Хеллмана до криптографии на решетках.
5. История стандартов шифрования: от DES к AES.
6. Роль NIST в стандартизации криптографических алгоритмов.
7. Теоретические основы стойкости криптоалгоритмов.
8. Квантовые вычисления и их влияние на современную криптографию.
9. Криптографические протоколы в древности: от шифра Цезаря до Энигмы.
10. Развитие криптоанализа: от частотного анализа до атак по сторонним каналам.

2. Криптографические API и библиотеки

11. Microsoft CryptoAPI: возможности и ограничения.
12. CNG (Cryptography API: Next Generation) – современная замена CryptoAPI.
13. OpenSSL: структура, уязвимости и применение.
14. Libsodium: простота и безопасность в современных приложениях.
15. BouncyCastle: кроссплатформенная криптография для Java и C#.
16. Криптографические библиотеки Python: PyCryptodome, cryptography.
17. WebCrypto API: криптография в браузере.
18. Apple CryptoKit: безопасность в экосистеме iOS/macOS.
19. Google Tink: универсальная криптографическая библиотека.
20. Криптография в .NET: от System.Security.Cryptography до CNG.

3. Криптографические алгоритмы и их реализация

21. AES: стандарт симметричного шифрования и его оптимизации.
22. RSA: математические основы, реализация и уязвимости.
23. Эллиптические кривые в криптографии (ECDSA, ECDH).
24. Постквантовая криптография: алгоритмы NIST PQC.

25. Хеш-функции: SHA-2, SHA-3, BLAKE3.
26. Алгоритмы аутентификации: HMAC, Poly1305.
27. Режимы работы блочных шифров: CBC, GCM, OCB.
28. Генерация случайных чисел: /dev/random, CryptGenRandom, BCryptGenRandom.
29. Криптография на основе идентификаторов (IBE).
30. Алгоритмы ГОСТ: особенности и применение в России.
- 4. Безопасность и уязвимости**
31. Атаки по сторонним каналам: timing-атаки, power analysis.
32. Уязвимости в криптографических библиотеках (Heartbleed, ROCA).
33. Атаки на неправильную реализацию RSA (Bleichenbacher, Coppersmith).
34. Криптографические ошибки в TLS/SSL (POODLE, CRIME, FREAK).
35. Атаки на PKI: подделка сертификатов, компрометация CA.
36. Уязвимости в генераторах случайных чисел.
37. Атаки на криптографию IoT-устройств.
38. Криптоджекинг: использование чужих ресурсов для майнинга.
39. Анализ уязвимостей в блокчейн-криптографии.
40. Защита от reverse engineering в криптографических приложениях.
- 5. Криптография в современных технологиях**
41. Криптография в облачных сервисах (AWS KMS, Azure Key Vault).
42. Защита данных в контейнерах Docker и Kubernetes.
43. Криптография в мобильных приложениях (Android KeyStore, iOS Secure Enclave).
44. Криптографические методы защиты IoT-устройств.
45. Безопасность API банковских приложений.
46. Криптография в блокчейне: Bitcoin, Ethereum, Zcash.
47. Secure Multi-Party Computation (MPC) – распределенная криптография.
48. Криптография в играх: защита от читерства.
49. Zero-Knowledge Proofs (ZKP) – доказательства с нулевым разглашением.
50. Криптография в квантовых сетях.
- 6. Key Management и PKI**
51. Системы управления ключами (HSM, TPM, YubiKey).
52. Инфраструктура открытых ключей (PKI): принципы и уязвимости.
53. Сертификаты X.509: структура и применение.

- 54. Механизмы отзыва сертификатов: CRL vs OCSP.
- 55. Self-Sovereign Identity (SSI) – децентрализованная идентификация.
- 56. Key Escrow – доверительное хранение ключей.
- 57. Распределенные ключи: Shamir's Secret Sharing.
- 58. Биометрическая криптография: безопасность и риски.
- 59. Криптография в системах электронного голосования.
- 60. Квантово-устойчивые ключевые системы.

7. Криптография и законодательство

- 61. Регулирование криптографии в России (ФЗ-152, ГОСТы).
- 62. Экспортный контроль криптографических технологий (Wassenaar Arrangement).
- 63. Криптография и GDPR: защита персональных данных.
- 64. PCI DSS: требования к криптографии платежных систем.
- 65. FIPS 140-3: сертификация криптографических модулей.
- 66. Криптография и право на приватность.
- 67. Юридические аспекты использования криптовалют.
- 68. Криптография в военной и государственной сферах.
- 69. Кибербезопасность и криптография в корпоративных стандартах.
- 70. Этика взлома: ответственное раскрытие уязвимостей.

8. Специальные темы

- 71. Стеганография: скрытие данных в цифровых медиа.
- 72. Криптография в кино: мифы и реальность.
- 73. Криптографические головоломки и CTF-задачи.
- 74. Криптография в космических технологиях.
- 75. Криптографические методы защиты от Deepfake.
- 76. Криптография и искусственный интеллект.
- 77. Криптография в медицинских системах.
- 78. Защита голосовых помощников (Siri, Alexa) с помощью криптографии.

- 79. Криптография в автомобильных системах (CAN-шина).
- 80. Будущее криптографии: прогнозы на 10 лет.

9. Практическая криптография

- 81. Разработка собственного шифра: плюсы и минусы.
- 82. Анализ производительности криптографических библиотек.
- 83. Реализация протокола Диффи-Хеллмана на Python.
- 84. Создание простого VPN с использованием OpenSSL.
- 85. Шифрование файлов с помощью GPG.
- 86. Анализ TLS-трафика в Wireshark.
- 87. Создание самоподписанного SSL-сертификата.

88. Визуализация работы AES с помощью Python.
89. Реализация электронной подписи на эллиптических кривых.
90. Криптографическая защита чат-бота.

10. Будущее криптографии

91. Постквантовая криптография: готовимся к угрозам.
92. Криптография в метавселенных.
93. Гомоморфное шифрование: вычисления на зашифрованных данных.
94. Криптография и интернет вещей (IoT).
95. Децентрализованные идентификаторы (DIDs).
96. Криптография в 6G-сетях.
97. Безопасность квантовой связи.
98. Криптография и биотехнологии.
99. Криптографические методы защиты от квантовых компьютеров.
100. Криптография как основа цифрового суверенитета.

Дополнительные темы рефератов

1. Применение привязки к биту и электронной жеребьевки для совместной выработки ключей.
2. Применение схем разделения секрета для безопасной отправки сообщений и депонирования ключей.
3. Идентификация и аутентификация в ОС Windows и Unix.
4. Разновидности цифровых подписей в электронном документообороте.
5. Схемы электронных денег WebMoney и payCash.
6. Схемы электронных денег eCash и PayCash.
7. Криптографические средства в электронном документообороте федеральных и местных органов управления в РФ.
8. Системы управления криптографическими ключами в федеральных и местных органах управления в РФ.
9. Обзор криптографических протоколов, использующих цифровую подпись.
10. Практика электронного голосования на примере ЕС.
11. Применение протокола «Покер по телефону» к раздаче электронных бланков.
12. Идентификация на основе биометрических данных.
13. Применение криптографических интерфейсов в области IoT.
14. Применение криптографических интерфейсов в электронном документообороте.
15. Применение криптографических интерфейсов в системах промышленной автоматизации.

16. Применение криптографических интерфейсов в современных автомобилях и автономных автомобилях.

17. Использование криптографических интерфейсов при заключении Smart контрактов.

18. Использование криптографических интерфейсов в робототехнике.

19. Применение криптографических интерфейсов в охранных системах.

20. Применение криптографических интерфейсов в системах аутентификации.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1 (Использование Microsoft CryptoAPI и CNG.)

Базовые тесты (выбор одного правильного ответа):

1. Что такое CNG?

a) Библиотека для работы с базами данных.

b) Криптографическая платформа следующего поколения от Microsoft.

c) Язык программирования для создания криптографических алгоритмов.

d) Протокол для обмена ключами.

Ответ: b) Криптографическая платформа следующего поколения от Microsoft.

2. Какой из перечисленных интерфейсов НЕ является частью Microsoft CryptoAPI?

a) CryptAcquireContext.

b) CryptEncrypt.

c) CryptGenKey.

d) OpenSSL.

Ответ: d) OpenSSL.

3. Что такое криптопровайдер?

a) Программа для создания виртуальных машин.

b) Программный модуль, реализующий криптографические функции.

c) Устройство для хранения ключей.

d) Протокол для шифрования данных.

Ответ: b) Программный модуль, реализующий криптографические функции.

4. Какой из перечисленных алгоритмов поддерживается CNG?

a) AES.

b) SHA-1.

c) RSA.

d) Все перечисленные.

Ответ: d) Все перечисленные.

Тесты повышенного уровня (вставка пропущенного термина):

5. CNG поддерживает алгоритмы симметричного шифрования, такие как _____.

Ответ: AES.

6. Для работы с CNG необходимо использовать интерфейсы, такие как _____.

Ответ: BCrypt.

7. Гибридное шифрование сочетает в себе преимущества _____ и асимметричного шифрования.

Ответ: симметричного.

8. Криптопровайдеры в CNG делятся на два типа: _____ и сторонние.

Ответ: встроенные.

Тесты высокого уровня (формулы или определения):

9. Запишите формулу для шифрования в алгоритме RSA:

Ответ:

$$C = M^e \bmod n$$

Где:

C — шифротекст,

M — открытый текст,

e — открытый ключ,

n — модуль.

10. Дайте определение гибридного шифрования.

Ответ: Гибридное шифрование — это метод, при котором для шифрования данных используется симметричный алгоритм, а для передачи ключа — асимметричный.

Тема 2 (Основы разработки криптопровайдеров)

Базовые тесты (выбор одного правильного ответа):

1. Какой инструмент используется для разработки криптопровайдеров?

a) Visual Studio.

b) Microsoft Cryptographic Provider Development Kit.

c) OpenSSL.

d) PyCryptodome.

Ответ: b) Microsoft Cryptographic Provider Development Kit.

2. Какой интерфейс используется для хэширования в CNG?

a) BCryptHashData.

b) CryptEncrypt.

c) CryptGenKey.

d) OpenSSL.

Ответ: a) BCryptHashData.

3. Какой алгоритм используется для асимметричного шифрования в CNG?

a) AES.

b) RSA.

c) SHA-256.

d) DES.

Ответ: b) RSA.

4. Какой из перечисленных методов НЕ используется для создания ЭЦП?

a) RSA.

b) DSA.

c) AES.

d) ECDSA.

Ответ: c) AES.

Тесты повышенного уровня (вставка пропущенного термина):

5. Для создания хэш-суммы в CNG используется функция _____.

Ответ: BCryptHashData.

6. Алгоритм RSA использует ключи длиной _____ бит.

Ответ: 2048.

7. Для создания электронной цифровой подписи используется алгоритм _____.

Ответ: DSA.

8. Обмен ключами в CNG осуществляется с использованием протокола _____.

Ответ: Диффи-Хеллмана.

Тесты высокого уровня (формулы или определения):

9. Запишите формулу для вычисления хэш-суммы:

Ответ:

$H = \text{HashFunction}(M)$

Где:

H — хэш-сумма,

M — сообщение.

10. Дайте определение электронной цифровой подписи (ЭЦП).

Ответ: ЭЦП — это криптографический метод, позволяющий удостоверить подлинность и целостность электронного документа.

Тема 3 (Реализации криптографических алгоритмов в рамках криптопровайдера)

Базовые тесты (выбор одного правильного ответа):

1. Какой алгоритм используется для симметричного шифрования?

- a) RSA.
- b) AES.
- c) SHA-256.
- d) DSA.

Ответ: b) AES.

2. Какой протокол используется для обмена ключами?

- a) RSA.
- b) Диффи-Хеллман.
- c) AES.
- d) SHA-256.

Ответ: b) Диффи-Хеллман.

3. Какой формат используется для хранения сертификатов?

- a) X.509.
- b) JSON.
- c) XML.
- d) YAML.

Ответ: a) X.509.

4. Какой алгоритм используется для создания имитовставки?

- a) HMAC.
- b) RSA.
- c) AES.
- d) SHA-256.

Ответ: a) HMAC.

Тесты повышенного уровня (вставка пропущенного термина):

5. Протокол Диффи-Хеллмана используется для _____.

Ответ: обмена ключами.

6. Сертификаты X.509 содержат информацию о _____.

Ответ: открытом ключе.

7. Имитовставка используется для обеспечения _____ данных.

Ответ: целостности.

8. Алгоритм HMAC использует _____ и хэш-функцию.

Ответ: ключ.

Тесты высокого уровня (формулы или определения):

9. Запишите формулу для протокола Диффи-Хеллмана:

Ответ:

$$K = g^{(ab)} \bmod p$$

Где:

К — общий секретный ключ,
 g — генератор,
 а и b — секретные ключи сторон,
 р — простое число.

10. Дайте определение инфраструктуры открытых ключей (PKI).

Ответ: PKI — это система, обеспечивающая создание, хранение, распределение и управление цифровыми сертификатами и ключами.

Тема 4 (Знакомство с криптографическими библиотеками различных языков программирования)

Базовые тесты (выбор одного правильного ответа):

1. Какая библиотека используется для криптографии в Python?

- a) PyCryptodome.
- b) OpenSSL.
- c) BouncyCastle.
- d) JCA.

Ответ: a) PyCryptodome.

2. Какой интерфейс используется для криптографии в Java?

- a) JCA/JCE.
- b) OpenSSL.
- c) CNG.
- d) CryptoAPI.

Ответ: a) JCA/JCE.

3. Какой алгоритм используется для цифровой подписи в C#?

- a) RSA.
- b) AES.
- c) SHA-256.
- d) DES.

Ответ: a) RSA.

4. Какой из перечисленных алгоритмов НЕ является блочным шифром?

- a) AES.
- b) DES.
- c) RSA.
- d) 3DES.

Ответ: c) RSA.

Тесты повышенного уровня (вставка пропущенного термина):

5. Для работы с криптографией в Java используется интерфейс _____.

Ответ: JCA/JCE.

6. Алгоритм RSA использует ключи длиной _____ бит.

Ответ: 2048.

7. Библиотека PyCryptodome поддерживает алгоритмы _____ шифрования.

Ответ: симметричного.

8. Цифровая подпись на основе RSA использует _____ ключ для подписи.

Ответ: закрытый.

Тесты высокого уровня (формулы или определения):

9. Запишите формулу для цифровой подписи на основе RSA:

Ответ:

$$S = M^d \bmod n$$

Где:

S — подпись,

M — сообщение,

d — закрытый ключ,

n — модуль.

10. Дайте определение блочного шифра.

Ответ: Блочный шифр — это алгоритм, который шифрует данные блоками фиксированной длины с использованием ключа.

6.5 Вопросы для подготовки к дифференцированному зачету

1. Понятие о криптографических протоколах. Основные виды протоколов.

Примитивные и прикладные протоколы.

2. Понятие о криптографических протоколах. Полнота и корректность.

3. Протоколы подбрасывания монеты. Применение протоколов подбрасывания монеты для выработки сеансовых ключей.

4. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью.

5. Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной секретностью.

6. Протоколы привязки к биту. Блоб.

7. Понятие о разделении секрета. Группа доступа, структура доступа. Требования к ним. Минимальная группа доступа.

8. Совершенная СРС (система разделения доступа), идеальная СРС.

9. Пороговые схемы разделения секрета. Схема Шамира, ее совершенность и идеальность.

10. Схема Блэкли. Вопрос о ее совершенности и идеальности.

11. СРС на основе Китайской теоремы об остатках. Вопрос о ее совершенности и идеальности.

12. СРС для произвольной структуры доступа. Вопрос о ее совершенности и идеальности.

13. Протоколы конфиденциальных вычислений.

14. Проверяемое разделение секрета.

15. Протоколы идентификации. Классификация. Требования.

16. Парольные схемы. Разновидности. Область применения.

17. Интерактивные системы доказательств. Полнота, корректность. Пример интерактивной системы доказательств для языка «Квадратичные невычеты».

18. Доказательства с нулевым разглашением. Статистическая неразличимость, вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов».

19. Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Их полнота и корректность.

20. Схема идентификации Шнорра. Схема Брикелла-МакКарли. Их полнота и корректность.

21. Схема идентификации Окамoto и теорема о ее условной стойкости.

22. Схема Гиллу-Кискатр. Ее полнота и корректность.

23. Слепая подпись.

24. Скрытый канал.

25. Протокол «Покер по телефону».

26. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Схема электронного кошелька с банкнотами одного достоинства.

27. Электронная монета. Электронные деньги. Требования к схемам электронных денег. Разного достоинства. Схема с копилкой.

28. Протоколы голосования.

29. Протоколы установления подлинности.

30. Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами.

31. Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана.

32. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра.

33. Схемы Wide-Mouth Frog, Yahalom. Их анализ.

34. Протокол Нидхема-Шредера. Его анализ.

35. Протокол Отвея-Рииса. Его анализ.

36. Бесключевой протокол Шамира и атака «Человек посередине».

37. Протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке.

38. Протокол Нидхема-Шредера на основе шифра с открытым ключом.

39. Широковещательное распределение ключей.

40. Протокол Kerberos.

41. Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей. Многоуровневая система удостоверяющих центров

6.6 Тематика и содержание курсового проекта

Темы, связанные с аппаратными модулями безопасности (HSM):

1. Разработка системы защиты TLS-сертификатов с использованием HSM.
2. Интеграция HSM в банковскую систему для защиты операций с платёжными картами.
3. Реализация шифрования базы данных с использованием HSM и стандарта Transparent Data Encryption (TDE).
4. Создание REST API для работы с ключами в облачном HSM (например, AWS CloudHSM).
5. Автоматизация процесса ротации ключей в корпоративной инфраструктуре на базе HSM.
6. Реализация процедуры цифровой подписи файлов с использованием API PKCS #11.
7. Разработка скрипта для мониторинга и управления состоянием HSM.
8. Исследование архитектуры и применения HSM в инфраструктуре PKI.
1. Пример: внедрение HSM для защиты сертификатов TLS в корпоративной сети.
9. Сравнительный анализ производительности облачных HSM (AWS CloudHSM, Google KMS, Azure Key Vault).
10. Разработка и тестирование API-интеграции с HSM с использованием PKCS #11.

Темы, связанные с модулями доверенной платформы (TPM):

1. Создание системы аутентификации устройств в локальной сети на основе TPM.
2. Реализация доверенной загрузки для Linux с использованием TPM и модулей PCR.
3. Разработка приложения для удаленной аттестации устройства с помощью TPM API.

4. Шифрование данных на основе TPM в рамках IoT-платформы.
5. Интеграция TPM с популярными шифрующими системами, такими как BitLocker или LUKS.
6. Реализация схемы защищённого хранения паролей с использованием TPM.
7. Создание доверенной среды для виртуальной машины с поддержкой TPM.
8. Создание доверенной платформы на базе TPM и реализация сценария доверенной загрузки.
9. Практическое применение TPM для шифрования данных в системе BitLocker и его интеграция в Linux (LUKS).
10. Разработка прототипа удаленной аттестации с использованием TPM.

Темы по смарт-картам и токенам:

1. Разработка системы защищенной аутентификации пользователей с помощью смарт-карт.
2. Интеграция токенов для электронной подписи в онлайн-сервис (например, система подачи заявлений).
3. Создание интерфейса для работы с смарт-картами в среде Windows/Linux.
4. Исследование и реализация протоколов передачи данных между смарт-картой и терминалом.
5. Разработка системы входа в корпоративную сеть с использованием USB-токенов.
6. Применение смарт-карт для защиты доступа к VPN.
7. Автоматизация проверки статуса смарт-карты в процессе работы системы аутентификации.
8. Разработка системы аутентификации на основе смарт-карт с поддержкой стандарта ГОСТ.
9. Исследование безопасности криптографических токенов на примере USB-устройств.
10. Разработка программного обеспечения для работы с смарт-картами через PC/SC-интерфейс.

Темы по интеграции криптографических интерфейсов:

1. Проектирование системы взаимодействия HSM и TPM для хранения мастер-ключа и подписания данных.
2. Создание IoT-устройства с защищённой коммуникацией через TPM.

3. Разработка прототипа гибридной системы безопасности, использующей HSM для корпоративных ключей и TPM для локальных устройств.
4. Интеграция аппаратного модуля безопасности в блокчейн-сеть для защиты приватных ключей.
5. Построение защищённого облачного хранилища с использованием HSM и смарт-карт для управления ключами.
6. Моделирование системы шифрования корпоративной почты на основе HSM.
7. Интеграция TPM в систему управления контейнерами Docker/Kubernetes для обеспечения доверенной загрузки.
8. Моделирование работы интерфейса PKCS #11 для управления ключами и криптографическими операциями.
9. Разработка библиотек для работы с криптографическими интерфейсами в Python.
10. Интеграция криптографического интерфейса OpenSSL с аппаратными HSM.
11. Проектирование системы взаимодействия HSM и TPM для защиты ключей и аутентификации.
12. Создание облачной инфраструктуры безопасности с использованием HSM и смарт-карт.
13. Разработка прототипа IoT-устройства с поддержкой TPM для защищённого обмена данными.

Темы по безопасности криптографических интерфейсов:

1. Разработка механизма защиты от атак на цепочку поставок для HSM.
2. Практическое исследование атаки на смарт-карту и разработка методов её предотвращения.
3. Реализация системы контроля доступа к криптографическим токенам с использованием биометрии.
4. Создание системы реагирования на инциденты безопасности, связанные с утечкой ключей из HSM.
5. Анализ рисков и разработка защитного слоя для облачного HSM.
6. Исследование методов защиты от атак на TPM с использованием аппаратных и программных средств.
7. Разработка системы обнаружения вредоносных изменений в PCR регистрах TPM.
8. Исследование атак на криптографические интерфейсы HSM и разработка защитных мер.

9. Анализ уязвимостей и реализация средств защиты для системы на основе TPM.

10. Исследование цепочек поставок и анализ рисков безопасности при использовании HSM.

Темы для прикладной разработки:

1. Создание библиотеки на Python для работы с PKCS #11.
2. Разработка инструмента для анализа производительности криптографических операций в HSM.
3. Реализация мобильного приложения для работы со смарт-картами через NFC.
4. Создание оболочки для управления TPM в ОС Linux.
5. Разработка GUI-интерфейса для администрирования HSM в корпоративной сети.
6. Автоматизация процесса развертывания инфраструктуры безопасности с HSM и TPM.
7. Реализация метода безопасной передачи данных через незащищенные каналы с использованием смарт-карт.

Простые темы для начинающих:

1. Генерация и управление ключами RSA на HSM.
2. Практическая работа с TPM для создания и хранения ключей.
3. Подключение смарт-карты к системе и выполнение базовых операций (чтение/запись).
4. Программная эмуляция HSM для тестирования приложений.
5. Реализация простого механизма аутентификации на основе USB-токена.

Инновационные разработки

1. Разработка интерфейса для квантово-устойчивых криптографических систем с использованием HSM.
2. Применение аппаратных интерфейсов в блокчейне: защита приватных ключей и транзакций.
3. Создание кастомного токена для защищённой работы в корпоративной сети.

Теоретические исследования

1. Исследование стандартов и API криптографических интерфейсов (PKCS #11, TSS, PC/SC).
2. Анализ стандартов безопасности (FIPS 140-3, TCG) для криптографических модулей.
3. Роль аппаратных криптографических модулей в обеспечении соответствия требованиям GDPR и PCI DSS.

Типовые задания для курсовых работ:

1. Моделирование атаки "Человек посередине" (Man-in-the-middle).
2. Реализация протокола "Держась за руки" (Interlock protocol).
3. Обмен ключами с использованием цифровых подписей.
4. Реализация протокола Yahalom.
5. Реализация схемы разделения секрета Блэкли 3,m.
6. Честное подбрасывание монеты на основе цифровых подписей.
7. Реализация центра выдачи сертификатов.
8. Разработка Интернет-мессенджера с шифрованием.
9. Разработка криптовалюты
10. Разработка криптокошелька цифровой валюты.
11. Разработка приложения шифрованной папки на жестком диске.
12. Разработка приложения для интернет голосования.
13. Разработка приложения для формирования и проверки цифровой подписи с использованием КристоПро CSP 5.0.
14. Разработка приложения платежной системы для оплаты с использованием банковских CryptoAPI.

ВНИМАНИЕ

Крайним разделом в курсовой работе должен быть раздел «Порядок сертификации средства криптографической защиты информации» (СКЗИ). Оказывать услуги по настройке и обслуживанию СКЗИ или, например, разработке систем, защищенных с помощью этих средств, можно только с лицензией ФСБ России (Центр по лицензированию, сертификации и защите государственной тайны ФСБ России) (<http://clsz.fsb.ru/>). Процесс ее получения регулирует Постановление Правительства РФ от 16.04.2012 № 313. В нем же перечислены работы, которые можно проводить на основании специального разрешения, то есть лицензии и получения сертификата соответствия.

В случае, если сертификация не требуется, данный раздел должен все равно присутствовать с обоснованием, почему он не требуется.

Информация к размышлению: Выписка из перечня средств защиты информации, сертифицированных ФСБ России и <http://www.fsb.ru/fsb/regions.htm>.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Владимиров, С. М. Криптографические методы защиты информации. Учебное пособие. [Электронный ресурс], 2021. – 433 с., ил. – Режим доступа: <https://github.com/vlsergey/infosec/releases/tag/v2021.11.06>. (Дата обращения 26.08.2024).
2. Бутакова, Н.Г. Криптографические методы и средства защиты информации: учеб. пособие / Н.Г.Бутакова, Н.В.Федоров. – СПб.: ИЦ «Интермедия», 2019. – 384 с. – Режим доступа: <https://obuchalka.org/20190604109900/kriptograficheskie-metodi-i-sredstva-zaschiti-informacii-uchebnoe-posobie-butakova-n-g-fedorov-n-v-2019.html>. (Дата обращения 26.08.2024).
3. Запечников, С.В. Криптографические методы защиты информации: учебник для вузов / С.В. Запечников, О.В. Казарин, А.А. Тарасов. – Москва: Издательство Юрайт, 2022. – 309 с. - Режим доступа: https://vk.com/wall-206723877_9876. (Дата обращения 26.08.2024).
4. Гладких, Анатолий Афанасьевич Основы современных криптографических систем и перспективы их развития : учебное пособие / А. А. Гладких, В. Е. Дементьев, Н. Ю. Чилихин. – Ульяновск : УлГТУ, 2020. – 214 с. - Режим доступа: <https://lib.ulstu.ru/venec/disk/2021/74.pdf>. (Дата обращения 26.08.2024).

Дополнительная литература

1. Хорев, П. Б. Использование криптографических интерфейсов : учебное пособие по курсам "Защита информации " и "Методы и средства защиты компьютерной информации" для студентов, обучающихся по специальностям "Прикладная математика" и "Информационные системы и технологии" / П. Б. Хорев ; под ред. М. М. Марана ; М-во образования и науки Российской Федерации, Федеральное агентство по образованию, Московский энергетический ин-т (Технический университет) (МЭИ). — Москва : Издательский дом МЭИ, 2007. — 112 с.: ил. - Режим доступа: <https://opac.nsuem.ru/mm/2012/000170431.pdf>. (Дата обращения: 26.08.2024).
2. Ильин, М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учеб. для студ. учреждений сред. проф. образования / М.Е.Ильин, Т.И.Калинкина, В.Н.Пржегорлинский. — М. : Издательский центр «Академия», 2019. — с. - Режим доступа: https://dblib.rsreu.ru/data/publications/6360_text.pdf. (Дата обращения 26.08.2024).

3. Щербаков Л.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов М.: ИТД Русская Редакция, 2003. — 416 с.: ил. — Режим доступа: <https://h.twirpx.one/file/5462/>. (Дата обращения 26.08.2024).

Учебно-методические материалы и пособия

1. Закутний А.С. Криптографические интерфейсы: лабораторный практикум [Электронный ресурс] – URL: <https://3kl.dontu.ru/course/>. Режим доступа: для авториз. пользователей. — Текст: электронный. (Дата обращения 26.08.2023).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education. — Текст : электронный.
2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: <http://ntb.bstu.ru/jirbis2/>. — Текст : электронный.
3. Консультант студента : электронно-библиотечная система.— Москва. — URL: <http://www.studentlibrary.ru/cgi-bin/mb4x>. — Текст : электронный.
4. Университетская библиотека онлайн: электронно-библиотечная система. – URL: http://biblioclub.ru/index.php?page=main_ub_red. – Текст : электронный.
5. IPR BOOKS : электронно-библиотечная система.—Красногорск. — URL: <http://www.iprbookshop.ru/>. —Текст : электронный.
6. Сайт кафедры ИСИБ <http://scs.dstu.education>.

Материально-техническое обеспечение представлено в таблице 6.

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: Аудитории для проведения лекций: <i>Мультимедийная аудитория. (60 посадочных мест),</i> оборудованная специализированной (учебной) мебелью (парта трехместная – 18 шт., парта двухместная – 6 шт, стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. <i>Компьютерные классы (22 посадочных места),</i> оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:	ауд. <u>207</u> корп. <u>4</u> ауд. <u>217</u> корп. <u>3</u> ауд. <u>211</u> корп. <u>4</u>

Лист согласования РПД

Разработал:

ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)


(подпись)

А.С. Закутный
(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Протокол № 1 заседания кафедрыот 27.08.2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)


(подпись)

В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03
Информационная безопасность
автоматизированных систем


(подпись)

Е.Е. Бизянов
(Ф.И.О.)

Начальник учебно-методического центра


(подпись)

О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	