Федеральное государственное бюджетное образовательное учреждение высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий

УТВЕРЖДАЮ
Начальник учебно-методического управления
Михайлова Анна Олеговна
Подписано цифровой подписью: Михайлова Анна Олеговна
«22» февраля 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность и защита информации

направление подготовки/специальность 09.03.03 Прикладная информатика

направленность (профиль)/специализация образовательной программы Прикладная информатика

Форма обучения очная

Санкт-Петербург, 2023

1. Цели и задачи освоения дисциплины (модуля)

Программа дисциплины направлена на формирование знаний, умений и навыков в области разработки новых и применения существующих современных методов обеспечения информационной безопасности и защиты информации при решении задач профессиональной деятельности. Современные методы защиты информации при реализации информационных технологий базируются на применении современных математических методов, алгоритмов и программ компьютерного анализа, а также при исследовании реальных процессов и явлений. Поэтому бакалавру важно уметь разрабатывать оригинальные алгоритмы и программные средства с использованием современных технологий. Планируемые результаты освоения дисциплины состоят в приобретении компетенций в области использования методов и средств системной инженерии для получения, передачи, хранения, переработки и представления информации. При этом предполагается, что технологии обеспечения информационной безопасности включает классические и неклассические методы, реализуемые на разных уровнях взаимодействия открытых систем.

Цель освоения дисциплины:

формирование знаний, умений и навыков разработки и использования в профессиональной деятельности методов и алгоритмов защиты информации при передаче, хранении, и разработке соответствующих программных средств.

Задачи освоения дисциплины:

– овладение методами теоретических и экспериментальных исследований в области информационной безопасности; получение знаний о современных информационно- коммуникационных технологиях, об инструментальных средах, о программно-технических платформах для решения профессиональных задач;

– обретение способности разрабатывать требования и проектировать программное обеспечение, реализующее методы защиты информации, умения обосновывать выбор современных информационно-коммуникационных технологий защиты информации, разрабатывать оригинальные программные средства для решения профессиональных задач;

– овладение методами практического применения методов и средств обеспечения информационной безопасности при проектировании информационных систем; приобретение навыков разработки оригинальных программных средств для решения профессиональных задач.

– понимать, разрабатывать и аргументировано применять методы обеспечения целостности, конфиденциальности и доступности данных в информационных системах.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов освоения ОПОП

ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.4 Осуществляет выбор программных средств	**знает** Необходимые требования к ПО и информационным технологиям для решения поставленных задач в вопросах информационной безопасности и защита информации **умеет** Применять использовать различное ПО по защита информации и информационной безопасности; Находить слабые места в защите web-ресурса **владеет навыками** Определять фальсификации данных и предотвращать получение незаконного доступа к web-ресурсу
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 Осуществляет выбор информационных ресурсов в соответствии с поставленной задачей с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**знает** основные термины и понятия информационно-коммуникационных технологий; основные требования информационной безопасности организации; инструменты создания систем защиты информации; виды угроз информационным системам и методы обеспечения информационной безопасности; современные подходы к построению систем защиты информации и критерии оценки защищенности информационной среды **умеет** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий осуществлять оценку защищенности и обеспечения информационной безопасности информационных среды; выявлять угрозы информационной безопасности и обосновывать организационно-технические мероприятия по защите информации в ИС **владеет навыками** навыками поиска, использования и анализа электронных информационных ресурсов на основе информационной и библиографической культуры; навыками работы со средствами защиты информации.

3. Указание места дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) включена в Блок «Дисциплины, модули» Б1.О.22 основной профессиональной образовательной программы 09.03.03 Прикладная информатика и относится к обязательной части учебного плана.

№ п/п	Предшествующие дисциплины	Код и наименование индикатора достижения компетенции
1	Практикум по программированию	ОПК-3.2, ОПК-7.1, ОПК-7.2

Практикум по программированию

знать:

- общие принципы построения вычислительных алгоритмов;

уметь:

- проводить разработку и анализ алгоритмов на основе современного математического аппарата;
- программировать алгоритм, используя средства языка высокого уровня;

владеть:

- методами практического использования современных компьютеров для обработки информации и основами численных методов решения инженерных задач.

№ п/п	Последующие дисциплины	Код и наименование индикатора достижения компетенции
1	Программирование для Интернет	ПК-1.2, ПК-1.4

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов	Из них часы на практическую подготовку	Семестр
			5
Контактная работа	48		48
Лекционные занятия (Лек)	16	0	16
Практические занятия (Пр)	32	0	32
Иная контактная работа, в том числе:	1,05		1,05
консультации по курсовой работе (проекту), контрольным работам (РГР)	0,4		0,4
контактная работа на аттестацию (сдача зачета, зачета с оценкой; защита курсовой работы (проекта); сдача контрольных работ (РГР))	0,4		0,4
контактная работа на аттестацию в сессию (консультация перед экзаменом и сдача	0,25		0,25
Часы на контроль	8,75		8,75
Самостоятельная работа (СР)	50,2		50,2
Общая трудоемкость дисциплины (модуля)			
часы:	108		108
зачетные единицы:	3		3

5. Содержание дисциплины (модуля), структурированное по разделам (темам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Тематический план дисциплины (модуля)

№	Разделы дисциплины	Семестр	Контактная работа (по учебным занятиям), час.						СР	Всего, час.	Код индикатора достижения компетенции
			лекции		ПЗ		ЛР				
			всего	из них на практическую подготовку	всего	из них на практическую подготовку	всего	из них на практическую подготовку			
1.	1 раздел. История информационной безопасности и защиты информации										
1.1.	История развития методов защиты информации. Обеспечение свойства информации: конфиденциальности, целостности, доступности. Криптографические методы защиты информации. Методы асимметричного и симметричного шифрования для обеспечения конфиденциальности информации. Методы обеспечения целостности информации на основе асимметричной криптографии. Биометрические методы защиты информации.	5	0,5		2				2	4,5	ОПК-2.4, ОПК-3.1
2.	2 раздел. Хэш-функции. Дайджесты сообщений										
2.1.	Математические односторонние функции и криптографические хэш-функции. История применения хэш-функций. Алгоритмы вычислениях хэш -функций. Критерии устойчивости хэш-функций. Устойчивость к коллизиям и к прообразам. Алгоритмы MessageDigest. Класс MessageDigest, поля и методы.	5	0,5		2				3,2	5,7	ОПК-2.4, ОПК-3.1
3.	3 раздел. MAC-коды, имитовставки сообщений										

3.1.	Недостатки хэширования. Коды аутентификации сообщений, усовершенствовавшие хэширование. Алгоритмы MAC: алгоритм генерации ключей, алгоритм подписи, алгоритм проверки. Отличие MAC от цифровых подписей. Класс MAC, Генерация ключей, выполнение и проверка MAC-кода.	5	1		1				4	6	ОПК-2.4, ОПК-3.1
4.	4 раздел. Цифровые подписи сообщений										
4.1.	Свойства цифровой подписи: целостность, авторство, неотказуемость сообщений. Симметричная и асимметричная схема цифровой подписи. Алгоритмы, применяемые для цифровых подписей: алгоритм DSA, алгоритм RSA и алгоритм SHA. Примеры генерации ключей. Классы генерации ключей ЦП, класс цифровой подписи, применение криптографическии стойкого генератора ПСП.	5	1		1				4	6	ОПК-2.4, ОПК-3.1
5.	5 раздел. Цифровые подписи объектов										
5.1.	Типы коллекций данных: массивы, списки, множества, таблицы, карты (отображения). Алгоритмы доступа к объектам коллекций: по индексу, по хэш-коду, по дереву. Объекты коллекций. Цифровые подписи объектов. Класс SignedObject, позволяющий создавать подписанные объекты, преобразованные в последовательную форму. Создание и проверка цифровых подписей объектов	5	1		2				4	7	ОПК-2.4, ОПК-3.1
6.	6 раздел. Шифрование с открытым ключом										

6.1.	Шифрование сообщений с открытым ключом по алгоритму RSA. Достоинства и недостатки асимметричного шифрования. Проблема низкой скорости алгоритма RSA Применение RSA для создания цифровых конвертов и для шифрования сеансовых ключей. Схе-ма шифрования сеансовых ключей с использованием методов класса Cipher. Создание потоков в программе Java для шифрования.	5	1		2				4	7	ОПК-2.4, ОПК-3.1
7.	7 раздел. Симметричное шифрование										
7.1.	Алгоритмы симметричного шифрования DES, 3DES, AES. Алгоритм Blowfish. Алгоритмы компании RSA Security. Режимы блочного шифрования: «электронная книга», «сцепление блоков шифротекста», «обратная связь по шифротексту» и «обратная связь по выходу».Применение вектора инициализации. Алгоритм дополнения блоков в блочном шифровании. Классы KeyGenerator, SecretKey, SecureRandom, Cipher.	5	1		2				2	5	ОПК-2.4, ОПК-3.1
8.	8 раздел. Кодирование Base-64										
8.1.	Кодирование Base-64. Кодирование ASCII, представление символов 7 битов, 33 управляющих символа, представление зашифрованных данных. Формат Base64 для преобразования последовательности байтов в формат по основанию 64.	5	1		2				2	5	ОПК-2.4, ОПК-3.1
9.	9 раздел. Согласование ключей										

9.1.	Протокол согласования ключей как инструмент Java Cryptography Architecture классом KeyAgreement. Установка одинакового криптографического ключ для нескольких сторон без передачи секретной информации между сторонами.	5	1		2				2	5	ОПК-2.4, ОПК-3.1
10.	10 раздел. Хранение ключей										
10.1.	Хранение ключей. Хранилище ключей (KeyStore). Документация JCA, раздел "KeyManagement". API для работы с хранилищем ключей.	5	1		2				2	5	ОПК-2.4, ОПК-3.1
11.	11 раздел. Сокеты для сетевых коммуникаций										
11.1.	Структура сокетов Windows и классы сокетов Java. Проблемы безопасности сетевых коммуникаций. Адреса и порты. Сканирование портов для поиска уязвимостей компьютера.	5	1		2				2	5	ОПК-2.4, ОПК-3.1
12.	12 раздел. Сокеты для передачи пакетов данных.										
12.1.	Классы дейтаграммных сокетов. Создание клиентов и серверов для передачи пакетов данных	5	1		2				2	5	ОПК-2.4, ОПК-3.1
13.	13 раздел. Сокеты для передачи потоков данных										
13.1.	Классы потоковых сокетов. Создание клиентов и серверов для передачи потоков данных. Многопоточные параллельные серверы.	5	1		2				2	5	ОПК-2.4, ОПК-3.1
14.	14 раздел. Безопасность передачи пакетов данных										
14.1.	Идентификация клиентов. Защита пакетов данных и использование методов асимметричного и симметричного шифрования.	5	1		2				2	5	ОПК-2.4, ОПК-3.1
15.	15 раздел. Безопасность передачи потоков данных										
15.1.	Безопасность передачи потоков данных	5	1		2				2	5	ОПК-2.4, ОПК-3.1

16.	16 раздел. Безопасные сокеты и SSL-протокол										
16.1.	Изучение стандартов, реализованных а SSL-протоколе. Создание SSL клиентов и серверов.	5	1		2				8	11	ОПК-2.4, ОПК-3.1
17.	17 раздел. Защита информации в базах данных										
17.1.	Шифрование и хэширование данных, контроль доступа, детальный аудит	5	1		2				3	6	ОПК-2.4, ОПК-3.1
18.	18 раздел. Иная контактная работа										
18.1.	Иная контактная работа	5								0,8	ОПК-2.4, ОПК-3.1
19.	19 раздел. Контроль										
19.1.	Зачет с оценкой	5								9	ОПК-2.4, ОПК-3.1

5.1. Лекции

№ разд	Наименование раздела и темы лекций	Наименование и краткое содержание лекций
1	История развития методов защиты информации. Обеспечение свойства информации: конфиденциальности, целостности, доступности. Криптографические методы защиты информации. Методы асимметричного и симметричного шифрования для обеспечения конфиденциальности информации. Методы обеспечения целостности информации на основе асимметричной криптографии. Биометрические методы защиты информации.	Обеспечение свойства информации: конфиденциальности, целостности, доступности. Криптографические методы защиты информации. Методы асимметричного и симметричного шифрования для обеспечения конфиденциальности информации. Методы обеспечения целостности информации на основе асимметричной криптографии. Биометрические методы защиты информации.
2	Математические односторонние функции и криптографические хэш-функции. История применения хэш-функций.	Математические односторонние функции и криптографические хэш-функции. История применения хэш-функций. Алгоритмы вычислениях хэш-функций. Критерии устойчивости хэш-функций. Устойчивость к коллизиям и к прообразам. Алгоритмы MessageDigest. Класс MessageDigest, поля и методы.

	Алгоритмы вычислениях хэш-функций. Критерии устойчивости хэш-функций. Устойчивость к коллизиям и к прообразам. Алгоритмы MessageDigest. Класс MessageDigest, поля и методы.	
3	Недостатки хэширования. Коды аутентификации сообщений, усовершенствовавшие хэширование. Алгоритмы MAC: алгоритм генерации ключей, алгоритм подписи, алгоритм проверки. Отличие MAC от цифровых подписей. Класс MAC, Генерация ключей, выполнение и проверка MAC-кода.	Недостатки хэширования. Коды аутентификации сообщений, усовершенствовавшие хэширование. Алгоритмы MAC: алгоритм генерации ключей, алгоритм подписи, алгоритм проверки. Отличие MAC от цифровых подписей. Класс MAC, Генерация ключей, выполнение и проверка MAC-кода
4	Свойства цифровой подписи: целостность, авторство, неотказуемость сообщений. Симметричная и асимметричная схема цифровой подписи. Алгоритмы, применяемые для цифровых подписей: алгоритм DSA, алгоритм RSA и алгоритм SHA. Примеры генерации ключей. Классы генерации ключей ЦП, класс цифровой подписи, применение криптографическии стойкого генератора ПСП.	Свойства цифровой подписи: целостность, авторство, неотказуемость сообщений. Симметричная и асимметричная схема цифровой подписи. Алгоритмы, применяемые для цифровых подписей: алгоритм DSA, алгоритм RSA и алгоритм SHA. Примеры генерации ключей. Классы генерации ключей ЦП, класс цифровой подписи, применение криптографическии стойкого генератора ПСП.
5	Типы коллекций данных: массивы, списки, множества, таблицы, карты (отображения). Алгоритмы доступа к	Типы коллекций данных: массивы, списки, множества, таблицы, карты (отображения). Алгоритмы доступа к объектам коллекций: по индексу, по хэш-коду, по дереву. Объекты коллекций. Цифровые подписи объектов. Класс SignedObject, позволяющий создавать подписанные объекты, преобразованные в последовательную форму. Создание и проверка

	объектам коллекций: по индексу, по хэш- коду, по дереву. Объекты коллекций. Цифровые подписи объектов. Класс SignedObject, позволяющий создавать подписанные объекты, преобразованные в последовательную форму. Создание и проверка цифровых подписей объектов	цифровых подписей объектов.
6	Шифрование сообщений с открытым ключом по алгоритму RSA. Достоинства и недостатки асимметричного шифрования. Проблема низкой скорости алгоритма RSA Применение RSA для создания цифровых конвертов и для шифрования сеансовых ключей. Схема шифрования сеансовых ключей с использованием методов класса Cipher. Создание потоков в программе Java для шифрования.	Шифрование сообщений с открытым ключом по алгоритму RSA. Достоинства и недостатки асимметричного шифрования. Проблема низкой скорости алгоритма RSA Применение RSA для создания цифровых конвертов и для шифрования сеансовых ключей. Схема шифрования сеансовых ключей с использованием методов класса Cipher. Создание потоков в программе Java для шифрования.
7	Алгоритмы симметричного шифрования DES, 3DES, AES. Алгоритм Blowfish. Алгоритмы компании RSA Security. Режимы блочного шифрования: «электронная книга», «сцепление блоков шифротекста», «обратная связь по шифротексту» и «обратная связь по выходу».Применение вектора инициализации. Алгоритм дополнения	Алгоритмы симметричного шифрования DES, 3DES, AES. Алгоритм Blowfish. Алгоритмы компании RSA Security. Режимы блочного шифрования: «электронная книга», «сцепление блоков шифротекста», «обратная связь по шифротексту» и «обратная связь по выходу».Применение вектора инициализации. Алгоритм дополнения блоков в блочном шифровании. Классы KeyGenerator, SecretKey, SecureRandom, Cipher.

	блоков в блочном шифровании. Классы KeyGenerator, SecretKey, SecureRandom, Cipher.	
8	Кодирование Base-64. Кодирование ASCII, представление символов 7 битов, 33 управляющих символа, представление зашифрованных данных. Формат Base64 для преобразования последовательности байтов в формат по основанию 64.	Кодирование Base-64. Кодирование ASCII, представление символов 7 битов, 33 управляющих символа, представление зашифрованных данных. Формат Base64 для преобразования последовательности байтов в формат по основанию 64.
9	Протокол согласования ключей как инструмент Java Cryptography Architecture классом KeyAgreement. Установка одинакового криптографического ключ для нескольких сторон без передачи секретной информации между сторонами.	Протокол согласования ключей как инструмент Java Cryptography Architecture. Классом KeyAgreement. Установка одинакового криптографического ключ для нескольких сторон без передачи секретной информации между сторонами.
10	Хранение ключей. Хранилище ключей (KeyStore). Документация JCA, раздел "KeyManagement". API для работы с хранилищем ключей.	Хранение ключей. Протокол согласования ключей как инструмент Java Cryptography Architecture. Классом KeyAgreement. Установка одинакового криптографического ключ для нескольких сторон без передачи секретной информации между сторонами.
11	Структура сокетов Windows и классы сокетов Java. Проблемы безопасности сетевых коммуникаций. Адреса и порты. Сканирование портов для поиска уязвимостей компьютера.	Структура сокетов Windows и классы сокетов Java. Проблемы безопасности сетевых коммуникаций. Адреса и порты. Сканирование портов для поиска уязвимостей компьютера.
12	Классы дейтаграммных сокетов. Создание клиентов и серверов	Классы дейтаграммных сокетов. Создание клиентов и серверов для передачи пакетов данных.

	для передачи пакетов данных	
13	Классы потоковых сокетов. Создание клиентов и серверов для передачи потоков данных. Многопоточные параллельные серверы.	Классы потоковых сокетов. Создание клиентов и серверов для передачи потоков данных. Многопоточные параллельные серверы.
14	Идентификация клиентов. Защита пакетов данных и использование методов асимметричного и симметричного шифрования.	Идентификация клиентов. Защита пакетов данных и использование методов асимметричного и симметричного шифрования.
15	Безопасность передачи потоков данных	Безопасность передачи потоков данных. Обеспечение безопасности передачи потоков данных в проводных и в беспроводных сетях. Шифрование данных с использованием блочных и потоковых шифров.
16	Изучение стандартов, реализованных а SSL-протоколе. Создание SSL клиентов и серверов.	Безопасные SSL сокеты сервера Изучение стандартов, реализованных а SSL-протоколе. Создание SSL клиентов и серверов.
17	Шифрование и хэширование данных, контроль доступа, детальный аудит	Шифрование и хэширование данных, контроль доступа, детальный аудит. Защита баз данных, шифрование и хэширование, контроль доступа, детальный аудит.

5.2. Практические занятия

№ разд	Наименование раздела и темы практических занятий	Наименование и содержание практических занятий
1	История развития методов защиты информации. Обеспечение свойства информации: конфиденциальности, целостности, доступности. Криптографические методы защиты информации. Методы асимметричного и симметричного шифрования для обеспечения конфиденциальности информации. Методы обеспечения целостности	Написание, отладка и выполнение программы шифра Цезаря. Написание и выполнение программы.

	информации на основе асимметричной криптографии. Биометрические методы защиты информации.	
2	Математические односторонние функции и криптографические хэш-функции. История применения хэш-функций. Алгоритмы вычислениях хэш-функций. Критерии устойчивости хэш-функций. Устойчивость к коллизиям и к прообразам. Алгоритмы MessageDigest. Класс MessageDigest, поля и методы.	Написание, отладка и выполнение программы дайджестов. Написание и выполнение программы.
3	Недостатки хэширования. Коды аутентификации сообщений, усовершенствовавшие хэширование. Алгоритмы MAC: алгоритм генерации ключей, алгоритм подписи, алгоритм проверки. Отличие MAC от цифровых подписей. Класс MAC, Генерация ключей, выполнение и проверка MAC-кода.	Написание, отладка и выполнение программы MAC-кодов, имитовставок сообщений Написание и выполнение программы.
4	Свойства цифровой подписи: целостность, авторство, неотказуемость сообщений. Симметричная и асимметричная схема цифровой подписи. Алгоритмы, применяемые для цифровых подписей: алгоритм DSA, алгоритм RSA и алгоритм SHA.	Написание, отладка и выполнение программы цифровой подписи сообщений Написание и выполнение программы.

	Примеры генерации ключей. Классы генерации ключей ЦП, класс цифровой подписи, применение криптографическии стойкого генератора ПСП.	
5	Типы коллекций данных: массивы, списки, множества, таблицы, карты (отображения). Алгоритмы доступа к объектам коллекций: по индексу, по хэш- коду, по дереву. Объекты коллекций. Цифровые подписи объектов. Класс SignedObject, позволяющий создавать подписанные объекты, преобразованные в последовательную форму. Создание и проверка цифровых подписей объектов	Написание, отладка и выполнение программы цифровой подписи объектов Написание и выполнение программы.
6	Шифрование сообщений с открытым ключом по алгоритму RSA. Достоинства и недостатки асимметричного шифрования. Проблема низкой скорости алгоритма RSA Применение RSA для создания цифровых конвертов и для шифрования сеансовых ключей. Схе -ма шифрования сеансовых ключей с использованием методов класса Cipher. Создание потоков в программе Java для шифрования.	Написание, отладка и выполнение программы шифрования сообщений с открытым ключом по алгоритму RSA Написание и выполнение программы.
7	Алгоритмы симметричного шифрования DES, 3DES, AES. Алгоритм Blowfish. Алгоритмы	Написание, отладка и выполнение программы симметричного шифрования DES, 3DES, AES. Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».

	компании RSA Security. Режимы блочного шифрования: «электронная книга», «сцепление блоков шифротекста», «обратная связь по шифротексту» и «обратная связь по выходу».Применение вектора инициализации. Алгоритм дополнения блоков в блочном шифровании. Классы KeyGenerator, SecretKey, SecureRandom, Cipher.	
8	Кодирование Base-64. Кодирование ASCII, представление символов 7 битов, 33 управляющих символа, представление зашифрованных данных. Формат Base64 для преобразования последовательности байтов в формат по основанию 64.	Написание, отладка и выполнение программы кодирования по основанию 64 Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».
9	Протокол согласования ключей как инструмент Java Cryptography Architecture классом KeyAgreement. Установка одинакового криптографического ключ для нескольких сторон без передачи секретной информации между сторонами.	Написание, отладка и выполнение программы согласования ключей Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».
10	Хранение ключей. Хранилище ключей (KeyStore). Документация JCA, раздел "KeyManagement". API для работы с хранилищем ключей.	Написание, отладка и выполнение программы согласования ключей Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».

11	Структура сокетов Windows и классы сокетов Java. Проблемы безопасности сетевых коммуникаций. Адреса и порты. Сканирование портов для поиска уязвимостей компьютера.	Написание, отладка и выполнение программы сетевого взаимодействия Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».
12	Классы дейтаграммных сокетов. Создание клиентов и серверов для передачи пакетов данных	Написание, отладка и выполнение программы дейтаграммных сокетов Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».
13	Классы потоковых сокетов. Создание клиентов и серверов для передачи потоков данных. Многопоточные параллельные серверы.	Написание, отладка и выполнение программы потоковых сокетов. Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».
14	Идентификация клиентов. Защита пакетов данных и использование методов асимметричного и симметричного шифрования.	Написание, отладка и выполнение программы идентификация клиентов. Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».
15	Безопасность передачи потоков данных	Написание, отладка и выполнение программы обеспечения безопасности потоков данных Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».
16	Изучение стандартов, реализованных а SSL-протоколе. Создание SSL клиентов и серверов.	Написание, отладка и выполнение программы SSL-сервера Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».
17	Шифрование и хэширование данных, контроль доступа, детальный аудит	Написание, отладка и выполнение программы соединения с базой данных. Студенты пишут, отлаживают и выполняют программы по теме занятия, указанной в разделе «Тема дисциплины».

5.3. Самостоятельная работа обучающихся

№ разд	Наименование раздела дисциплины и темы	Содержание самостоятельной работы
1	История развития методов защиты информации. Обеспечение свойства	Истоия развития методов защиты информации. Изучение лекционного материала. Изучение источников литературы, статей, интернет-ресурсов

	информации: конфиденциальности, целостности, доступности. Криптографические методы защиты информации. Методы асимметричного и симметричного шифрования для обеспечения конфиденциальности информации. Методы обеспечения целостности информации на основе асимметричной криптографии. Биометрические методы защиты информации.	
2	Математические односторонние функции и криптографические хэш-функции. История применения хэш-функций. Алгоритмы вычислениях хэш-функций. Критерии устойчивости хэш-функций. Устойчивость к коллизиям и к прообразам. Алгоритмы MessageDigest. Класс MessageDigest, поля и методы.	Математические односторонние функции и криптографические хэш-функции. Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
3	Недостатки хэширования. Коды аутентификации сообщений, усовершенствовавшие хэширование. Алгоритмы MAC: алгоритм генерации ключей, алгоритм подписи, алгоритм проверки. Отличие MAC от цифровых подписей. Класс MAC, Генерация ключей, выполнение и	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов

	проверка MAC-кода.	
4	Свойства цифровой подписи: целостность, авторство, неотказуемость сообщений. Симметричная и асимметричная схема цифровой подписи. Алгоритмы, применяемые для цифровых подписей: алгоритм DSA, алгоритм RSA и алгоритм SHA. Примеры генерации ключей. Классы генерации ключей ЦП, класс цифровой подписи, применение криптографически стойкого генератора ПСП.	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
5	Типы коллекций данных: массивы, списки, множества, таблицы, карты (отображения). Алгоритмы доступа к объектам коллекций: по индексу, по хэш- коду, по дереву. Объекты коллекций. Цифровые подписи объектов. Класс SignedObject, позволяющий создавать подписанные объекты, преобразованные в последовательную форму. Создание и проверка цифровых подписей объектов	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
6	Шифрование сообщений с открытым ключом по алгоритму RSA. Достоинства и недостатки асимметричного шифрования. Проблема низкой скорости алгоритма RSA Применение RSA для создания	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.

	цифровых конвертов и для шифрования сеансовых ключей. Схе -ма шифрования сеансовых ключей с использованием методов класса Cipher. Создание потоков в программе Java для шифрования.	
7	Алгоритмы симметричного шифрования DES, 3DES, AES. Алгоритм Blowfish. Алгоритмы компании RSA Security. Режимы блочного шифрования: «электронная книга», «сцепление блоков шифротекста», «обратная связь по шифротексту» и «обратная связь по выходу».Применение вектора инициализации. Алгоритм дополнения блоков в блочном шифровании. Классы KeyGenerator, SecretKey, SecureRandom, Cipher.	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
8	Кодирование Base-64. Кодирование ASCII, представление символов 7 битов, 33 управляющих символа, представление зашифрованных данных. Формат Base64 для преобразования последовательности байтов в формат по основанию 64.	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
9	Протокол согласования ключей как инструмент Java Cryptography Architecture классом KeyAgreement. Установка одинакового	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.

	криптографического ключ для нескольких сторон без передачи секретной информации между сторонами.	
10	Хранение ключей. Хранилище ключей (KeyStore). Документация JCA, раздел "KeyManagement". API для работы с хранилищем ключей.	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
11	Структура сокетов Windows и классы сокетов Java. Проблемы безопасности сетевых коммуникаций. Адреса и порты. Сканирование портов для поиска уязвимостей компьютера.	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
12	Классы дейтаграммных сокетов. Создание клиентов и серверов для передачи пакетов данных	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
13	Классы потоковых сокетов. Создание клиентов и серверов для передачи потоков данных. Многопоточные параллельные серверы.	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
14	Идентификация клиентов. Защита пакетов данных и использование методов асимметричного и симметричного шифрования.	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
15	Безопасность передачи потоков данных	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.
16	Изучение стандартов, реализованных а SSL-протоколе. Создание SSL клиентов и серверов.	Подготовка доклада Изучение лекционного материала. Подготовка к лабораторной работе. Изучение источников литературы, статей, интернет-ресурсов.

17	Шифрование и хэширование данных, контроль доступа, детальный аудит	Работа с литературой Изучение лекционного материала. Подготовка к лабораторной работе. Студенты изучают источники литературы, статьи, интернет-ресурсы, составляют отчеты.

6. Методические материалы для самостоятельной работы обучающихся по дисциплине (модулю)

Программой дисциплины предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, и лабораторных занятий, предполагающих закрепление изученного материала и формирование у обучающихся необходимых знаний, умений и навыков. Кроме того, важнейшим этапом изучения дисциплины является самостоятельная работа обучающихся с использованием всех средств и возможностей современных образовательных технологий.

В объем самостоятельной работы по дисциплине включается следующее:

- изучение теоретических вопросов по всем темам дисциплины;
- подготовка к лабораторным занятиям;
- подготовка к текущему контролю успеваемости студентов;
- подготовка к зачету с оценкой.

Залогом успешного освоения дисциплины является обязательное посещение лекционных и лабораторных занятий, так как пропуск одного (тем более, нескольких) занятий может осложнить освоение разделов курса. На лабораторных занятиях материал, изложенный на лекциях, закрепляется при выполнении заданий.

Приступая к изучению дисциплины, обучающемуся необходимо в первую очередь ознакомиться с содержанием РПД, а также методическими указаниями по организации самостоятельной работы и подготовки к практическим занятиям.

При подготовке к лекционным занятиям студенту необходимо:

- ознакомиться с соответствующей темой занятия;
- осмыслить круг изучаемых вопросов и логику их рассмотрения;
- изучить рекомендуемую рабочей программой литературу по данной теме.

При подготовке к лабораторным занятиям и в рамках самостоятельной работы по изучению дисциплины обучающимся необходимо:

- повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники;
- выполнить лабораторные задания в рамках изучаемой темы;
- ответить на контрольные вопросы по теме, используя материалы ФОС, либо групповые индивидуальные задания, подготовленные преподавателем;
- подготовиться к проверочной работе, предусмотренной в контрольных точках;
- подготовиться к промежуточной аттестации.

Итогом изучения дисциплины является зачет с оценкой. Зачет проводится по расписанию. Форма проведения занятия может быть устная, письменная и в электронном виде. Студенты, не прошедшие аттестацию, должны ликвидировать задолженность в установленном порядке.

7. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

№ п/п	Контролируемые разделы дисциплины (модуля)	Код и наименование индикатора контролируемой компетенции	Вид оценочного средства
1	История развития методов защиты информации. Обеспечение свойства информации: конфиденциальности, целостности, доступности. Криптографические методы защиты информации. Методы асимметричного и симметричного шифрования для обеспечения конфиденциальности информации. Методы обеспечения целостности информации на основе	ОПК-2.4, ОПК-3.1	устный опрос, написание программ

	асимметричной криптографии. Биометрические методы защиты информации.		
2	Математические односторонние функции и криптографические хэш-функции. История применения хэш-функций. Алгоритмы вычислениях хэш-функций. Критерии устойчивости хэш-функций. Устойчивость к коллизиям и к прообразам. Алгоритмы MessageDigest. Класс MessageDigest, поля и методы.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
3	Недостатки хэширования. Коды аутентификации сообщений, усовершенствовавшие хэширование. Алгоритмы MAC: алгоритм генерации ключей, алгоритм подписи, алгоритм проверки. Отличие MAC от цифровых подписей. Класс MAC, Генерация ключей, выполнение и проверка MAC- кода.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
4	Свойства цифровой подписи: целостность, авторство, неотказуемость сообщений. Симметричная и асимметричная схема цифровой подписи. Алгоритмы, применяемые для цифровых подписей: алгоритм DSA, алгоритм RSA и алгоритм SHA. Примеры генерации ключей. Классы генерации ключей ЦП, класс цифровой подписи, применение криптографическии стойкого генератора ПСП.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
5	Типы коллекций данных: массивы, списки, множества, таблицы, карты (отображения). Алгоритмы доступа к объектам коллекций: по индексу, по хэш- коду, по дереву. Объекты коллекций. Цифровые подписи объектов. Класс SignedObject, позволяющий создавать подписанные объекты, преобразованные в последовательную форму. Создание и проверка цифровых подписей объектов	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
6	Шифрование сообщений с открытым ключом по алгоритму RSA. Достоинства и недостатки асимметричного шифрования. Проблема низкой скорости алгоритма RSA Применение RSA для создания цифровых конвертов и для шифрования сеансовых ключей. Схема шифрования сеансовых ключей с использованием методов класса Cipher. Создание потоков в программе Java для шифрования.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
7	Алгоритмы симметричного шифрования DES, 3DES, AES. Алгоритм Blowfish. Алгоритмы компании RSA Security. Режимы блочного шифрования:	ОПК-2.4, ОПК-3.1	устный опрос, написание программ

	«электронная книга», «сцепление блоков шифротекста», «обратная связь по шифротексту» и «обратная связь по выходу».Применение вектора инициализации. Алгоритм дополнения блоков в блочном шифровании. Классы KeyGenerator, SecretKey, SecureRandom, Cipher.		
8	Кодирование Base-64. Кодирование ASCII, представление символов 7 битов, 33 управляющих символа, представление зашифрованных данных. Формат Base64 для преобразования последовательности байтов в формат по основанию 64.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
9	Протокол согласования ключей как инструмент Java Cryptography Architecture классом KeyAgreement. Установка одинакового криптографического ключ для нескольких сторон без передачи секретной информации между сторонами.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
10	Хранение ключей. Хранилище ключей (KeyStore). Документация JCA, раздел "KeyManagement". API для работы с хранилищем ключей.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
11	Структура сокетов Windows и классы сокетов Java. Проблемы безопасности сетевых коммуникаций. Адреса и порты. Сканирование портов для поиска уязвимостей компьютера.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
12	Классы дейтаграммных сокетов. Создание клиентов и серверов для передачи пакетов данных	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
13	Классы потоковых сокетов. Создание клиентов и серверов для передачи потоков данных. Многопоточные параллельные серверы.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
14	Идентификация клиентов. Защита пакетов данных и использование методов асимметричного и симметричного шифрования.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
15	Безопасность передачи потоков данных	ОПК-2.4, ОПК-3.1	устный опрос, написание программ
16	Изучение стандартов, реализованных а SSL-протоколе. Создание SSL клиентов и серверов.	ОПК-2.4, ОПК-3.1	устный опрос, написание программ, доклад
17	Шифрование и хэширование данных, контроль доступа, детальный аудит	ОПК-2.4, ОПК-3.1	устный опрос
18	Иная контактная работа	ОПК-2.4, ОПК-3.1	
19	Зачет с оценкой	ОПК-2.4, ОПК-3.1	

7.2. Типовые контрольные задания или иные материалы текущего контроля успеваемости, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Тестовые задания

(для проверки освоения индикаторов достижения компетенций ОПК-2.4, ОПК-3.1)

Дайте определение и объясните важность таких свойств информации?

• Конфиденциальность
• Целостность
• Доступность

Какие свойства связаны с информационной безопасностью?

• Конфиденциальность
• Управляемость
• Наблюдаемость
• Доступность
• Целостность
• Недоступность

Фирма гарантирует защиту индивидуальных данных своих сотрудников. Какой тип конфиденциальности поддерживает фирма?

• Добровольную конфиденциальность - privacy
• Принудительную конфиденциальность - security
• Надежную конфиденциальность -reliability
• Законную конфиденциальность – legality

Фирма запрещает сотрудникам разглашать сущность работы. Какой тип конфиденциальности поддерживает фирма?

• Неподкупную конфиденциальность- incorrupt
• Законную конфиденциальность- legality
• Добровольную конфиденциальность - privacy
• Принудительную конфиденциальность - security

Данные были изменены во время хранения в базе данных. Какое свойство информации было нарушено?

• Конфиденциальность
• Достоверность
• Наблюдаемость
• Доступность
• Целостность
• Надежность

Сервер базы данных перегружен и не может обсуживать клиентов. Какое свойство информации нарушено?

• Конфиденциальность
• Достоверность
• Наблюдаемость
• Доступность
• Целостность
• Надежность

Алгоритм симметричного шифрования использует?

• Один и тот же ключ для шифрования и дешифрования
• Ключ для шифрования и симметричный ключ для дешифрования
• Два разных ключа для шифрования и дешифрования

С какой целью используется вектор инициализации?

• Вектор инициализации позволяет генерировать одинаковые ключи для симметричного шифрования
• Вектор инициализации позволяет одновременно сменить ключ шифрования
• Вектор инициализации является вторым ключом шифрования
• Вектор инициализации изменяет шифруемый текст во избежание повтора символа

Какой из алгоритмов обеспечивает более высокий уровень защиты информации?

• DES3 -Triple DES
• AES- Advanced Encryption Standard
• DES- Data Encryption Standard

Какими методами обеспечивают свойства информации?

• Конфиденциальность

• Целостность

• Доступность

Какие исторические шифры Вы знаете?

• Шифр Цезаря.

• Шифры перестановки.

• Шифры подстановки.

Какой из методов шифрования не приводит к распростарнению ошибок между блоками?

• CBC -сцепление блоков шифротекста

• ECB-электронная книга

• CFB-обратная связь по шифротексту

• OFB-обратная связь по выводу

Удовлетворяет ли контрольная сумма требования к криптографической хеш-функции?

• Да. Но требуется добавить криптографическую соль

• Нет. Функция контрольной суммы вычисляется слишком долго

• Да Функция контрольной суммы удовлетворяет всем требованиям хеш-функции.

• Нет. Функция контрольной суммы- не стойкий прообраз. Можно найти несколько сообщений, контрольная сумма которых советует данной.

Какими свойствами обладает хеш-функция?

• Назначение, свойства, алгоритмы дайджеста.

• Чем отличаются дайджест и MAC-код

• Последовательность действий при вычислении дайджеста

• Последовательность действий при вычислении MAC-кода

• Цифровая подпись

• Назначение цифровых подписей

• Последовательность действий при получении цифровой подписи

• Алгоритмы цифровой подписи

Какое утверждение верно?

• Для предотвращения коллизий хеш-функция должна быть как минимум в два раза больше, чем требуется для сопротивления прообразу

• Для сопоставления прообразу хеш-функция должна быть как минимум в два раза больше, чем требуется для предотвращения коллизий.

• Для предотвращения коллизий хеш-функция должна быть вычислен путем деления полиромов.

• Для предотвращения коллизий хеш-функция должна быть вычислена путем деления по модулю.

Какие свойства алгоритмов хешированя имеют важное значение?

• Разрядность хеш-функции

• Вычислительная сложность алгоритма

• Секретность алгоритма вычисления хеш-функции

• Обратимость алгоритма вычисления хеш-функции

Когда применяется хеш-функция?

• При создании шифров с открытым ключом.

• При создании симметричных шифров с секретным ключом

• При построении уникальных идентификаторов для данных

• При вычислении контрольных сумм данных(сигнала) для последующего обнаружения в них ошибок

• При сохранении паролей в системах защиты в виде хеш-кода.

7.3. Система оценивания результатов обучения по дисциплине (модулю) при проведении текущего контроля успеваемости

Оценка «отлично» (зачтено)	знания: - систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; - точное использование научной терминологии, систематически грамотное и логически правильное изложение ответа на вопросы; - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин навыки: - высокий уровень сформированности заявленных в рабочей программе компетенций; - владеет навыками самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; - применяет теоретические знания для выбора методики выполнения заданий; - грамотно обосновывает ход решения задач; - безупречно владеет инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; - творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активно участвует в групповых обсуждениях, высокий уровень культуры исполнения заданий
Оценка «хорошо» (зачтено)	знания: - достаточно полные и систематизированные знания по дисциплине; - усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в основных теориях, концепциях и направлениях дисциплины и давать им критическую оценку; - использует научную терминологию, лингвистически и логически правильно излагает ответы на вопросы, умеет делать обоснованные выводы; - владеет инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач навыки: - самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; - средний уровень сформированности заявленных в рабочей программе компетенций; - без затруднений выбирает стандартную методику выполнения заданий; - обосновывает ход решения задач без затруднений

Оценка «удовлетворительно» (зачтено)	знания: - достаточный минимальный объем знаний по дисциплине; - усвоение основной литературы, рекомендованной рабочей программой; - использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок умения: - умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; - владеет инструментарием учебной дисциплины, умение его использовать в решении типовых задач; - умеет под руководством преподавателя решать стандартные задачи навыки: - работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; - достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций; - испытывает затруднения при обосновании алгоритма выполнения заданий
Оценка «неудовлетворительно» (не зачтено)	знания: - фрагментарные знания по дисциплине; - отказ от ответа (выполнения письменной работы); - знание отдельных источников, рекомендованных рабочей программой по дисциплине; умения: - не умеет использовать научную терминологию; - наличие грубых ошибок навыки: - низкий уровень культуры исполнения заданий; - низкий уровень сформированности заявленных в рабочей программе компетенций; - отсутствие навыков самостоятельной работы; - не может обосновать алгоритм выполнения заданий

7.4. Теоретические вопросы и практические задания для проведения промежуточной аттестации обучающихся, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

7.4.1. Теоретические вопросы для проведения промежуточной аттестации обучающихся

1. Свойства информации. Исторические шифры перестановки и подстановки.
2. Дайджесты: алгоритмы и применение.
3. MAC-код: алгоритмы и применение.
4. Цифровые подписи: алгоритмы и применение. Ключи для цифровых подписей.
5. Симметричное шифрование. Типы шифров. Генерация ключей.
6. Особенности ASCII-кодов. Кодирование Base-64. Особенности ASCII-кодов.
7. Шифрование на базе пароля. Назначение.
8. Передача данных в UDP-пакетах между клиентом и сервером.
9. Сканирование портов.
10. Передача данных в TCP-сегментах между клиентом и сервером.
11. Защищенные сокеты.
12. Обработка исключений и информация об ошибках.
13. Потоки ввода-вывода. Низкоуровневые потоки.
14. Потоки ввода-вывода. Высокоуровневые потоки.
15. Классы коллекций на java.
16. Модификаторы private & friendly & protected & public
17. Сдвиговые операции в java.

7.4.2. Практические задания для проведения промежуточной аттестации обучающихся

Задание 1. Написать программу по реализации шифра Цезаря на Java

Цель: Написать программу на Java, которая шифрует и расшифровывает текст с использованием метода шифра Цезаря.

Входные данные:

Пользовательский текст

Значение сдвига для процесса шифрования/дешифрования

Входные данные:

Зашифрованный/расшифрованный текст

Требования:

Программа должна предложить пользователю ввести текст, который он хочет зашифровать или расшифровать.

Программа должна позволять пользователю вводить значение сдвига для процесса шифрования/дешифрования.

В программе должны быть опции для шифрования и дешифрования

Программа должна отображать зашифрованный/расшифрованный текст

Пример:

Введите текст: Hello World

Введите значение сдвига: 3

Шифровать или расшифровывать? (Ш/Р): Ш

Зашифрованный текст: Khoor Zruog

Введите текст: Khoor Zruog

Введите значение сдвига: 3

Шифровать или расшифровывать? (Ш/Р): Р

Расшифрованный текст: Hello World

Задание 2. Задача: Написать программу по созданию дайджеста сообщений Java

Цель: реализовать программу на Java, которая создает дайджест сообщения из входного текста, используя выбранный алгоритм хеширования.

Входные данные:

Пользовательский текст

Выходные данные:

Дайджест сообщения входного текста в шестнадцатеричном формате

Требования:

Программа должна предложить пользователю ввести текст, для которого он хочет создать дайджест сообщения.

Программа должна позволять пользователю выбирать желаемый алгоритм дайджеста сообщения из списка доступных алгоритмов.

Программа должна отображать дайджест сообщения входного текста в шестнадцатеричном формате.

Задание 3. Написать программу вычисления MAC-кода (message authentication code) на Java:

Задача: Программа расчета MAC-кода на Java

Цель: реализовать программу на Java, которая вычисляет MAC (код аутентификации сообщения) для заданного сообщения, используя указанную хеш-функцию.

Входные данные:

Пользовательское сообщение

Желаемая хэш-функция (например, SHA-256, MD5 и т. д.)

Выходные данные:

MAC-код для данного сообщения

Требования:

Программа должна предложить пользователю ввести сообщение, для которого он хочет рассчитать MAC-код.

Программа должна позволять пользователю выбирать нужную хеш-функцию из списка часто

Программа должна отобразить рассчитанный MAC-код

Пример:

Введите сообщение: This is a test message.

Доступные хэш-функции:

1. SHA-256
2. MD5

Выберите хэш-функцию (1 или 2): 1

Расчетный MAC-код: fc75f0bbd34dc05a7f6f47cb6a7a638cc8e7d1118c9a6f9b1d08ddb7d6b9980a

Задание 4. Написать программу программу вычисления цифровой подписи на Java

Задача: Программа расчета цифровой подписи на Java

Цель: Написать программу на Java, которая вычисляет цифровую подпись для заданного сообщения, используя заданный алгоритм шифрования.

Входные данные:

Пользовательское сообщение

Желаемый алгоритм шифрования (например, RSA, DSA и т. д.)

Закрытый ключ для подписи

Выходные данные:

Цифровая подпись для данного сообщения

Требования:

Программа должна предложить пользователю ввести сообщение, для которого он хочет рассчитать цифровую подпись.

Программа должна позволять пользователю выбирать желаемый алгоритм шифрования из списка часто используемых алгоритмов (например, RSA, DSA и т. д.).

Программа должна использовать Java Cryptography API (например, java.security.Signature) для выполнения вычисления подписи.

Программа должна отображать рассчитанную цифровую подпись

Пример:

Введите сообщение: This is a test message.

Доступные алгоритмы шифрования:

1. RSA
2. DSA

Выберите алгоритм шифрования (1 or 2): 1

Введите private key: 1234567890abcdef

Цифровая подпись: efcdab90987654321

Задание 5.Написать Программа шифрования с открытым ключом на Java

Задача: Программа шифрования с открытым ключом

Цель: реализовать программу на Java, которая использует открытый ключ для шифрования сообщения и другую программу, использующую закрытый ключ для расшифровки зашифрованного сообщения.

Входные данные:

Пользовательское сообщение

Открытый ключ для шифрования

Закрытый ключ для расшифровки

Выходные данные:

Зашифрованное сообщение

Расшифрованное сообщение

Требования:

Программа должна предложить пользователю ввести сообщение, которое он хочет зашифровать.

Программа должна использовать Java Cryptography API (например, java.security.Cipher) для выполнения шифрования с открытым ключом.

Зашифрованное сообщение должно быть сохранено в файл

Введите сообщение: This is a test message.

Введите public key: abcdef1234567890

Зашифрованное сообщение: qwerty0987654321

Расшифрованное сообщение: This is a test message.
Задание 6. Программа симметричного шифрования
Задание 7. Программа Base-64 кодирования
Задание 8. Программа хранения ключей
Задание 9. Программа шифрования на базе пароля
Задание 10. Программа клиентского сокета
Задание 11. Программа серверного сокета
Задание 12. Программа безопасного клиентского сокета
Задание 13. Программа безопасного клиентского сокета
Задание 14. Программа, выполняющая SSL протокол

7.4.3. Примерные темы курсовой работы (проекта) (при наличии)

Курсовые работы (проекты) учебным планом не предусмотрены

7.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта профессиональной деятельности, характеризующие этапы формирования компетенций

Процедура проведения промежуточной аттестации и текущего контроля успеваемости регламентируется локальным нормативным актом, определяющим порядок организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся.

Процедура оценивания формирования компетенций при проведении текущего контроля приведена в п. 7.2.

Типовые контрольные задания или иные материалы текущего контроля приведены в п. 7.3.

Промежуточная аттестация по дисциплине проводится в форме зачета с оценкой.

Зачет проводится в форме собеседования.

7.6. Критерии оценивания сформированности компетенций при проведении промежуточной аттестации

	Уровень освоения и оценка			
	Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»
	«не зачтено»	«зачтено»		
Критерии оценивания	Уровень освоения компетенции «недостаточный». Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы	Уровень освоения компетенции «пороговый». Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	Уровень освоения компетенции «продвинутый». Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Уровень освоения компетенции «высокий». Компетенции сформированы. Знания аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка

знания	Обучающийся демонстрирует: -существенные пробелы в знаниях учебного материала; -допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий билета.	Обучающийся демонстрирует: -знания теоретического материала; -неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; -неуверенные и неточные ответы на дополнительные вопросы.	Обучающийся демонстрирует: -знание и понимание основных вопросов контролируемого объема программного материала; - знания теоретического материала -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; -правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы.	Обучающийся демонстрирует: -глубокие, всесторонние и аргументированные знания программного материала; -полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий, в рамках обсуждаемых заданий; -способность устанавливать и объяснять связь практики и теории, -логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора.
умения	При выполнении практического задания билета обучающийся продемонстрировал недостаточный уровень умений. Практические задания не выполнены Обучающийся не отвечает на вопросы билета при дополнительных наводящих вопросах преподавателя.	Обучающийся выполнил практическое задание билета с существенными неточностями. Допускаются ошибки в содержании ответа и решении практических заданий. При ответах на дополнительные вопросы было допущено много неточностей.	Обучающийся выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Предложенные практические задания решены с небольшими неточностями. Ответил на большинство дополнительных вопросов.	Обучающийся правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Решает предложенные практические задания без ошибок Ответил на все дополнительные вопросы.

владение навыками	Не может выбрать методику выполнения заданий. Допускает грубые ошибки при выполнении заданий, нарушающие логику решения задач. Делает некорректные выводы. Не может обосновать алгоритм выполнения заданий.	Испытывает затруднения по выбору методики выполнения заданий. Допускает ошибки при выполнении заданий, нарушения логики решения задач. Испытывает затруднения с формулированием корректных выводов. Испытывает затруднения при обосновании алгоритма выполнения заданий.	Без затруднений выбирает стандартную методику выполнения заданий. Допускает ошибки при выполнении заданий, не нарушающие логику решения задач Делает корректные выводы по результатам решения задачи. Обосновывает ход решения задач без затруднений.	Применяет теоретические знания для выбора методики выполнения заданий. Не допускает ошибок при выполнении заданий. Самостоятельно анализирует результаты выполнения заданий. Грамотно обосновывает ход решения задач.

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной, и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, владение навыками).

Оценка «отлично»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0.

Оценка «хорошо»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4.

Оценка «удовлетворительно»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 2,5 до 3,4.

Оценка «неудовлетворительно»/«не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

8. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля)

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Количество экземпляров/электронный адрес ЭБС
	Основная литература	
1	Вязовик Н. А., Программирование на Java, Москва: Интернет- Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/73710.html
2	Никифоров С. Н., Защита информации. Защищенные сети, СПб., 2017	ЭБС
3	Никифоров С. Н., Защита информации, СПб., 2015	ЭБС
	Дополнительная литература	
1	Монажв В. В., Язык программирования Java и среда NetBeans, Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	http://www.iprbookshop.ru/73739.html

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
Классы безопасности Java	http://spec-zone.ru/RU/Java/Docs/7/technotes/guides/security/overview/jsoverview.html

8.3. Перечень современных профессиональных баз данных и информационных справочных систем

Наименование	Электронный адрес ресурса
Электронно-библиотечная система издательства "ЮРАЙТ"	https://www.biblio-online.ru/
Электронно-библиотечная система издательства "IPRbooks"	http://www.iprbookshop.ru/
Электронно-библиотечная система издательства "Лань"	https://e.lanbook.com/
Единый электронный ресурс учебно-методической литературы СПбГАСУ	www.spbgasu.ru
Научная электронная библиотека eLIBRARY.RU	Научная электронная библиотека eLIBRARY.RU
Система дистанционного обучения СПбГАСУ Moodle	https://moodle.spbgasu.ru/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения

Наименование	Способ распространения (лицензионное или свободно распространяемое)
Microsoft Windows 10 Pro	Договор № Д32009689201 от 18.12.2020г Программные продукты Майкрософт, договор № Д32009689201 от 18.12.2020 с АО "СофтЛайн Трейд": Windows 10, Project Professional 2016, Visio Professional 2016, Office 2016.
Microsoft Office 2016	Договор № Д32009689201 от 18.12.2020г Программные продукты Майкрософт, договор № Д32009689201 от 18.12.2020 с АО "СофтЛайн Трейд": Windows 10, Project Professional 2016, Visio Professional 2016, Office 2016.
Microsoft Visual Studio 2017	Договор № Д32009689201 от 18.12.2020г Программные продукты Майкрософт, договор № Д32009689201 от 18.12.2020 с АО "СофтЛайн Трейд": Windows 10, Project Professional 2016, Visio Professional 2016, Office 2016.

8.5. Материально-техническое обеспечение дисциплины

Сведения об оснащенности учебных аудиторий и помещений для самостоятельной работы

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащенность оборудованием и техническими средствами обучения

47. Учебные аудитории для проведения лекционных занятий	Учебная аудитория для проведения занятий лекционного типа, комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудио-система), доска маркерная белая эмалевая, экран, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.
47. Компьютерный класс	Рабочие места с ПК (стол компьютерный, системный блок, монитор, клавиатура, мышь), стол рабочий, подключение к компьютерной сети СПбГАСУ, выход в Internet.
47. Помещения для самостоятельной работы	Помещение для самостоятельной работы (читальный зал библиотеки, ауд. 217): ПК-23 шт., в т.ч. 1 шт.- ПК для лиц с ОВЗ (системный блок, монитор, клавиатура, мышь) с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СПбГАСУ. ПО Microsoft Windows 10, Microsoft Office 2016
47. Учебные аудитории для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная аудитория для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудио-система), доска маркерная белая эмалевая, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.

Для инвалидов и лиц с ОВЗ обеспечиваются специальные условия для получения образования в соответствии с требованиями нормативно-правовых документов.