Приложение 4
к образовательной программе

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.03 Криптографические методы защиты информации
(индекс, наименование дисциплины, в соответствии с учебным планом)

38.04.05 Бизнес-информатика
(код,наименование направления подготовки)

«Аналитическое обеспечение информационной безопасности»
(наименование образовательной программы)

очная форма обучения
(форма обучения)

Год набора – 2026

Санкт-Петербург

Автор–составитель:
Доцент кафедры бизнес-информатики, к.т.н., доцент Зеленина Лариса Ивановна.

Заведующий кафедрой бизнес-информатики
Доктор военных наук, профессор Наумов Владимир Николаевич

РПД «Методы бизнес-аналитики» одобрена протоколом заседания кафедры бизнес-информатики № 6 от 26.03.2026 г.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

Дисциплина Б1.В.03 Криптографические методы защиты информации обеспечивает формирование у обучающихся следующих профессиональных компетенций*:

ОТФ/ТФ и реквизиты ПС *(при наличии)***	**Код компетенции ****	**Наименование компетенции ****	**Код индикатора достижения компетенций ****	**Наименование индикатора достижения компетенций ****	**Образовательный результат ****
С/02.7 Разработка систем защиты информации автоматизированных систем, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости / Разработка проектных решений по защите информации в автоматизированных системах 06.033 Специалист по защите информации в автоматизированных системах утв. приказом Министерства труда и социальной защиты Российской	ПКс-2	Способен обосновывать подходы и требования к системе обеспечения информационной безопасности, оценивать уровни безопасности компьютерных систем и сетей	ПКс-2.3	Оценивает уровни безопасности компьютерных систем и сетей	ПКс.2.3.-Зн.1 **Знать** Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
					ПКс.2.3-У-2 **Уметь** Применять нормативные документы по противодействию технической разведке

Федерации от 14.09.2022 № 525н					
0.6 МЕНЕДЖЕР ПО ИНФОРМАЦИОННЫМ ТЕХНОЛОГИЯМ 06.014 Управление сервисами ИТ организации B/06.014 Управление сервисами ИТ организации / Управление непрерывностью ИТ-сервисов	ПКс-4	Способен управлять информационными сервисами, ресурсами ИТ и ИТ-инновациями. Управлять ИАС в защищенном исполнении, обслуживать системы защиты	ПКс-4.2	Управляет ИАС в защищенном исполнении	ПКс-4.2. Зн.3 **Знать** Методы контроля непрерывности ИТ-сервисов
					ПКс-4.2. У.-.3 **Уметь** Формировать команду и организовывать персонал и стейкхолдеров для управления непрерывностью ИТ-сервисов

** Дисциплина может формировать компетенцию полностью или частично.*

***Должно соответствовать Приложению 1 к образовательной программе*

2. Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы/108 академических/81 астрономических часов.

Дисциплина реализуется частично с применением дистанционных образовательных технологий (далее – ДОТ).

Контактная работа обучающихся с преподавателем по видам учебных занятий: 20 ак. час на контактную работу с преподавателем, из них 8 ак.час на лекции, 12 ак.час на практические занятия и 79 ак.час на самостоятельную работу обучающихся.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.03 Криптографические методы защиты информации относится к части, формируемой участниками образовательных отношений, образовательной программы подготовки магистранта федерального государственного образовательного стандарта высшего образования и изучается на первом курсе.

Преподавание дисциплины Б1.В.03 Криптографические методы защиты

информации основано на знаниях, полученных при изучении дисциплин Б1.В.02 «Математические методы статистической обработки и анализа данных» и Б1.В.03 «Управление информационной безопасностью». В свою очередь она создаёт необходимые предпосылки для освоения программы дисциплины Б1.В.07 «Моделирование информационной безопасности. Управление рисками».

Знания, умения и навыки, полученные при изучении дисциплины, используются студентами при выполнении выпускных квалификационных работ (магистерских диссертаций).

Формой промежуточной аттестации в соответствии с учебным планом является зачет с оценкой.

3.Содержание и структура дисциплины

3.1. Структура дисциплины

Очная форма обучения

Формой промежуточной аттестации в соответствии с учебным планом является зачет с оценкой.

№ п/п	Наименование тем и (или) разделов		Объем дисциплины, ак.час												Форма текущего контроля успеваемости, промежуточной аттестации
		ВСЕГО	Контактная работа обучающихся с преподавателем по видам учебных занятий									Самостоятельная работа			
			Период теоретического обучения						Период промежуточной аттестации (сессия)						
			Занятия лекционного типа		Занятия семинарского типа		ИК	КСР	КЭ	Каттэк	Контроль	СРкр	СРэк	СР	
			Л	ВЛ	ЛР	ПЗ									
Тема 1	История криптографии. Классические шифры. Современные системы симметричной криптографии	41	4			4								33	ПЗ,Т
Тема 2	Асимметричная криптография	29	2			4								23	ПЗ,Т
Тема 3	Криптографические протоколы	29	2			4								23	ПЗ,Т
Промежуточная аттестация		9								9					Зачет с оценкой
Итого		108	8			12				9				79	

Используемые сокращения:

Л – лекции - занятия, предусматривающие преимущественную передачу учебной информации обучающимся педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях,).

ВЛ – видео лекции.

ЛР – лабораторные работы.

ПЗ – практические занятия (за исключением лабораторных работ).

ИК – индивидуальные консультации.

КСР – контроль самостоятельной работы

КЭ – консультации перед экзаменом

Каттэк – контактная работа на аттестацию в период экзаменационных сессий

Контроль - контактная работа на аттестацию в период экзаменационных сессий для заочной формы обучения

СРкр – самостоятельная работа на подготовку курсовой работы/ курсового проекта.

СРэк – самостоятельная работа на подготовку к экзамену.

СР – самостоятельная работа в семестре на подготовку к учебным занятиям.

Т – тестирование.

ПКЗ – практические контрольные задания.

ПИЗ – профессионально-исследовательские задания.

В процессе обучения применяются следующие интерактивные формы: лекция-диалог, работа в малых группах, спарринг-партнерство.

Темы 1-3 могут быть освоены с применением ЭО и ДОТ с контролем в системе электронного обучения Академии.

3.2. Содержание и структура дисциплины

Тема 1. История криптографии. Классические шифры. Современные системы симметричной криптографии

Основные понятия и задачи криптографии. Основные понятия и определения криптографии. Основные задачи криптографии. Криптографические протоколы.

Исторические шифры. Простые шифры перестановки. Шифры простой замены. Криптоанализ простых шифров. Пропорциональные шифры замены Шифры сложной (многоалфавитной) замены.

Свойства современных криптосистем. Классификация и виды шифров. Формальные модели шифров. Криптостойкость и имитостойкость шифра.

Блочные шифры. Структура блочных шифров. Американские стандарты блочного шифрования. Российские стандарты блочного шифрования ГОСТ 28147-89 и ГОСТ Р 34.12-2015. Основные методы анализа блочных криптосистем.

Потоковые шифры. Общие свойства потоковых шифров. Линейный рекуррентный регистр сдвига. Основные методы анализа поточных криптосистем. Потоковые шифры сетей GSM

Хэш- функции. Общие сведения о хэш-функциях. Бесключевые хэш-функции. Одноключевые хэш-функции. Код аутентификации HMAC.

Тема 2. Асимметричная криптография

Общие сведения об асимметрических криптосистемах.

Система распределения ключей Диффи-Хеллмана (DH).

Системы шифрования с открытым ключом. Криптографическая система RSA. Криптографическая система Эль-Гамаля

Электронная цифровая подпись. Общие сведения о цифровой подписи. ЭЦП на основе RSA. ЭЦП на основе схемы Эль-Гамаля. Атаки на схемы электронной цифровой подписи. Цифровые сертификаты.

Тема 3. Криптографические протоколы

Особенности и специальные виды криптографических протоколов.

Протоколы, связанные с ЭЦП. Разрешение споров по ЭЦП (протокол с судейством). Особые схемы электронной подписи

Протоколы аутентификации и распределения ключей. Распределение ключей с помощью симметричных криптосистем и арбитра. Обмен ключами с помощью асимметричных криптосистем. Взаимная аутентификация с помощью асимметричных криптосистем (протокол Нидхема-Шредера).

Специальные криптографические протоколы. Протоколы разделения секрета (распределения ответственности). Протокол доказательства с нулевым разглашением конфиденциальной информации. Электронные деньги (электронная наличность). Создание скрытого канала

4. Типы оценочных материалов, показатели и критерии оценивания

4.1. Оценочные материалы по дисциплине Б1.В.03 Криптографические методы защиты информации входят в состав оценочных материалов по образовательной программе. Совокупность оценочных материалов по всем дисциплинам образовательной программы составляет фонд оценочных средств (далее – ФОС). ФОС используется при проведении текущего контроля успеваемости и промежуточной аттестации обучающихся с

целью оценивания достижения обучающимися планируемых результатов обучения.

4.2. ФОС разработан как комплекс проверочных заданий различного типа и уровня сложности, включает критерии и шкалы оценивания, а также «ключи» правильных ответов. ФОС формируется как отдельный документ и хранится в электронном виде, доступ к ФОС предоставлен ограниченному кругу лиц.

4.3. Для самостоятельной работы обучающихся при подготовке к текущему контролю успеваемости и промежуточной аттестации в рабочих программах дисциплин размещены типовые проверочные задания, которые можно условно разделить на задания закрытого, комбинированного и открытого типов.

Задания закрытого типа — это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных.

Задания комбинированного типа – это тестовые задания, в которых каждый вопрос сопровождается готовыми вариантами ответов, из которых необходимо выбрать один или несколько правильных и обосновать свой выбор.

Задания открытого типа — это задания, в которых на каждый вопрос должен быть предложен развернутый обоснованный ответ.

В зависимости от типа задания рекомендованы определенная последовательность выполнения и система оценивания выполнения заданий.

4.4. Типы заданий, сценарии выполнения, критерии оценивания

ТИП ЗАДАНИЯ	ИНСТРУКЦИЯ	СЦЕНАРИИ ВЫПОЛНЕНИЯ	КРИТЕРИИ ОЦЕНИВАНИЯ
Задание закрытого типа с выбором одного правильного ответа из нескольких вариантов предложенных	Прочитайте текст, выберите правильный ответ	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа (например, 3 или В).	Ответ считается верным, если правильно указана цифра или буква
Задание закрытого типа на установление соответствия	Прочитайте текст и установите соответствие	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов. 2. Внимательно прочитать оба списка: список 1 – вопросы, утверждения, факты, понятия и т.д.; список 2 – утверждения, свойства объектов и т.д. 3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов. 4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А1 или Б4).	Ответ считается верным, если правильно указаны цифры или буквы
Задание закрытого типа с выбором нескольких правильных ответов из нескольких вариантов	Прочитайте текст, выберите правильные ответы	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов. 2. Внимательно прочитать предложенные вариант-ты ответа. 3. Выбрать несколько правильных ответов. 4. Записать только номера (или буквы)	Ответ считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)

предложенных		выбранного варианта ответа (например, 1 4 или А Г).	
Задание закрытого типа на установление последовательности	Прочитайте текст и установите последовательность	1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов. 2. Внимательно прочитать предложенные варианты ответа. 3. Построить верную последовательность из предложенных элементов. 4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).	Ответ считается верным, если правильно указана вся последовательность цифр
Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора	Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа	1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов. 2. Внимательно прочитать предложенные варианты ответа. 3. Выбрать один верный ответ. 4. Записать только номер (или букву) выбранного варианта ответа. 5. Записать аргументы, обосновывающие выбор ответа (например, 4 текст обоснования).	Ответ считается верным, если правильно указана цифра или буква и приведены корректные аргументы, используемые при выборе ответа
Задание открытого типа с развернутым ответом	Прочитайте текст и запишите развернутый обоснованный ответ	1. Внимательно прочитать текст задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	Ответ считается верным: 1. Отсутствие фактических ошибок. 2. Раскрытие объема используемых понятий (полнота ответа). 3.Обоснованность ответа (наличие аргументов). 4. Логическая последовательность излагаемого материала.

4.5. Общая шкала оценивания результатов текущего контроля успеваемости и промежуточной аттестации обучающихся с применением БРС

Итоговая балльная оценка	Традиционная система	Бинарная система	ECTS	
			Для традиционной системы	Для бинарной системы
95-100	Отлично	Зачтено	A	P/ Passed
85-94			B	P/ Passed
75-84	Хорошо		C	P/ Passed
65-74			D	P/ Passed
55-64	Удовлетворительно		E	P/ Passed
0-54	Неудовлетворительно	Не зачтено	F	F/Failed

Соотношение баллов за текущий контроль успеваемости и промежуточную аттестацию, а также повторную промежуточную аттестацию:

Максимальная сумма баллов за текущий контроль успеваемости	Максимальная сумма баллов за промежуточную аттестацию	Максимальная итоговая балльная оценка	Максимальная сумма баллов за повторную промежуточную аттестацию
60 баллов	40 баллов	100 баллов	100 баллов

5. Формы аттестации, типовые оценочные материалы для текущего контроля успеваемости обучающихся, критерии и шкалы оценивания по контрольным точкам

5.1. В ходе реализации дисциплины используются следующие формы текущего контроля успеваемости обучающихся (в том числе, задания к контрольным точкам):

Т – тестирование, ПЗ – практические занятия.

Тема 1. История криптографии. Классические шифры. Современные системы симметричной криптографии

Тестовые задания:

1. Сформулировать основные понятия криптографии.
2. Определить основные задачи криптографии.
3. Что относится к криптографическим протоколам.
4. Что понимается под термином «исторические шифры»
5. Суть простых шифров перестановки.
6. Как работают шифры простой замены.
7. Как выполняется криптоанализ простых шифров.

Практическое задание

Задание 1.

Используя шифр перестановки «Поворотные решетки Кардано» создать свой трафарет

для поворотной решетки размером 6×6. Зашифровать текст с помощью созданного трафарета. Расшифровать криптограмму, полученную с помощью поворотной решетки, если известен использованный для шифрования трафарет.

Задание2.

Дешифровать криптограммы, полученные методами столбцовой и двойной перестановки.

Задание 3.

Зашифровать слово с помощью шифра Цезаря. Расшифровать криптограмму, полученную с помощью шифра Цезаря.

Задание 4.

Зашифровать слово с помощью шифра Виженера. Расшифровать криптограмму, полученную с помощью шифра Виженера.

Задание 5.

Дешифровать криптограмму, полученную шифром простой замены. Символы криптограммы закодированы двузначными числами. В тексте криптограммы сохранены пробелы и пунктуация. Символ пробела и знаки препинания в нормативный алфавит не входят.

Тема 2. Асимметричная криптография

Тестовые задания:

1. Что относится к асимметрическим криптосистемам.
2. В чем суть системы распределения ключей Диффи-Хеллмана.
3. В чем отличие систем шифрования с открытым ключом от систем шифрования с закрытым ключом.
4. В чем отличие криптографической системы RSA от криптографической системы Эль-Гамаля
5. Что представляет электронная цифровая подпись. Задачи, решаемые при ее использовании.
6. В чем отличие ЭЦП на основе RSA от ЭЦП на основе схемы Эль-Гамаля.
7. Кие атаки на схемы электронной цифровой подписи вам знакомы.
8. Что такое цифровые сертификаты.

Практическое задание

Задание 1.

Найти секретный ключ *K* учебного алгоритма с помощью с помощью обычной слайдовой атаки

Задание 2.

Выполнить «вручную» операцию *MixColumns* для заданного столбца байтов. Столбец байтов для преобразования приведен в таблице 1 (см ниже).

Задание 3.

Зашифровать с помощью алгоритма AES-128 заданный фрагмент на заданном ключе (см таблица 1).

Задание 4.

Дешифровать заданную криптограмму, полученную шифром AES-128 на ключе из задания ***3***, получить открытый текст сообщения. Криптограмма для расшифровывания приведена в таблице 1.

Таблица 1.

Столбец байтов	Блок текста: 38 AD C5 0F AC 3F C1 1B 4C 8E B2 80 57 90 23 2C Ключ: A4 83 01 77 CA 0F 68 EE AF 66 AB 45 A7 7B 89 08 Криптограмма: AB 0A 78 15 33 CC 17 49 18 74 F4 AA 2C 92 9F 07
AD	
41	
87	
AC	

Задание 5.

Зашифровать клавиатурный символ с помощью криптосистемы Блюма-Гольдвассер, сгенерировав 8-битовую псевдослучайную последовательность.

Из таблицы 2 выбрать значения параметров BBS-генератора p, q, случайное число s и подлежащий зашифрованию символ M (символ – русскоязычный).

Таблица 2

p	***q***	***s***	Открытый текст ***M***
883	367	65486	О

Задание 6.

Расшифровать криптограмму, полученную в криптосистеме Блюма-Гольдвассер. Известно, что использована эффективная реализация BBS-генератора с максимально допустимым числом младших битов.

Значения секретного ключа: чисел p и q, криптограмма C, состоящая из числа-подсказки x_6 и последовательности ASCII-кодов c_i символов зашифрованного текста представлены в таблице 3.

Таблица 3

p	***q***	Криптограмма ***C***	
		x_6	c_i
439	491	123530	130;222;119

Тема 3. Криптографические протоколы

Тестовые задания:

1. Каковы особенности криптографических протоколов.
2. Какие виды кпрптографических протоколов вам известны.
3. Охарактеризовать протоколы, связанные с ЭЦП.
4. Сравнить протоколы аутентификации и распределения ключей.
5. Как осуществляется распределение ключей с помощью симметричных криптосистем и арбитра.
6. В чем суть обмена ключами с помощью асимметричных криптосистем.
7. Каким образом осуществляется взаимная аутентификация с помощью асимметричных криптосистем.
8. Что относится к специальным криптографическим протоколам.
9. Протоколы распределения ответственности.
10. Протокол доказательства с нулевым разглашением конфиденциальной информации.
11. Что понимается под электронной наличностью.
12. каким образом осуществляется создание скрытого канала

Практическое задание

Задание 1.

Выполнить шифрование, проверку аутентичности и дешифрование по алгоритму RSA, зная только открытые ключи абонентов криптосистемы RSA.

По известным открытым ключам (N, e) абонентов криптосистемы RSA (табл. 4) и тому, что кодирование символов сообщения осуществляется с помощью таблицы 5 (буквы «е» и «ё» не различаются). Найти значение передаваемого между абонентами шифртекста Y.

Таблица 4. Справочник открытых ключей абонентов криптосистемы RSA

Абонент	Ключ (***N***, ***e***)	Абонент	Ключ (***N***, ***e***)	Абонент	Ключ (***N***, ***e***)
A	(5017, 251)	F	(8809, 307)	K	(4553, 241)
B	(8471, 125)	G	(6077, 619)	L	(6757, 233)
C	(4559, 311)	H	(5513, 607)	P	(8413, 507)
D	(3403, 211)	I	(7747, 353)	Q	(6313, 749)
E	(5177, 179)	J	(5561, 433)	R	(9301, 387)

Таблица 5. Таблица кодирования символов открытого текста

Символ	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
код	11	12	13	14	15	16	17	18	19	21	22	23	24	25	26	27
Символ	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
код	28	29	31	32	33	34	35	36	37	38	39	41	42	43	44	45

Задание 2.

Абоненты криптосистемы RSA обмениваются открытыми сообщениями с подтверждением авторства. Проверить аутентичность сообщения, если известны открытые

ключи (N, e) абонентов криптосистемы (табл. 4). Кодирование символов сообщения осуществляется с помощью таблицы 5 (буквы «е» и «ё» не различаются). Параметры передачи текста в системе RSA, передаваемый открытый текст и проверочный код приведены в таблице 6.

Таблица 6.

Передача текста	Подпись
R → A; акт	1019;8218

Задание 3.

При передаче между абонентами перехвачена криптограмма Y, полученная шифрованием по алгоритму RSA. Дешифровать Y, вычислив секретный ключ d. Известны открытые ключи абонентов (табл. 4). Кодирование символов сообщения осуществляется с помощью таблицы 5. Параметры шифра RSA и криптограмму $\boldsymbol{Y}$ указаны в табл. 7.

Таблица 7.

Абоненты	Криптограмма $\boldsymbol{Y}$
F → P	3872;5862

Задание 4.

Даны значения модуля шифрования N, открытого ключа e и шифртекста Y. Известно, что Y получен шифрованием на открытом ключе (N, e) по алгоритму RSA. Используя разложение модуля на простые числа методом Ферма, определить секретный ключ алгоритма RSA и дешифровать Y.

$N = 65815671868057$, $e = 7423489$, $Y = 64938654445479$.

5.2. Типовые оценочные материалы для текущего контроля успеваемости обучающихся (вне контрольных точек):

приведены в п.6.2.

5.3.Один или несколько тематических блоков дисциплины завершаются контрольной точкой (далее – КТ). Текущий контроль успеваемости по дисциплине предусматривает не менее 2 (двух) и не более 10 (десяти) КТ в течение периода освоения дисциплины.

Максимальное количество баллов за любой тип работ в рамках КТ составляет 100 (сто) баллов.

Распределение весовых коэффициентов по КТ в рамках текущего контроля успеваемости по дисциплине и формулы расчета:

Наименование контрольной точки	Максимальное количество баллов за работу в рамках	Коэффициент веса контрольной точки	Результат контрольной точки, участвующий в

	КТ, которое может набрать студент		формировании итоговой балльной оценки по дисциплине (отражается в журнале БРС в СДО)
КТ - 1	100	0,23	23
КТ - 2	100	0,23	23
КТ- 3	100	0,14	14
Итого:	х	0,6	60

Формула расчета результата контрольной точки:
Результат контрольной точки = Количество баллов за работу в рамках КТ х Коэффициент веса контрольной точки.

5.4. Формы текущего контроля успеваемости обучающихся в рамках КТ и типовые оценочные материалы:

КТ-1
Тема 1.
Тестирование.
Практическое занятие (ПЗ).

КТ-2
Тема 2.
Тестирование.
Практическое занятие (ПЗ).

КТ-3
Тема 3.
Тестирование.
Практическое занятие (ПЗ).

Для каждой формы текущего контроля успеваемости обучающихся в рамках КТ определены критерии оценивания результатов выполнения задания.

1. *Критерии оценивания тестирования:*

Критерии оценки	Диапазон баллов	Описание критерия
Количество правильных ответов	*0*	*Количество правильных ответов менее 55%*
	25	*Количество правильных ответов от 55% до 64%*
	50	*Количество правильных ответов от 65% до 74%*
	75	*Количество правильных ответов от 75% до 84%*
	100	*Количество правильных ответов от 85%*

		до 100%
Итого максимально:	100	

2. Критерии оценивания ПЗ:

Критерии оценки	Диапазон баллов	Описание критерия
Содержание и раскрытие выбранных понятий	*41-70*	*Детальное, последовательное описание всех понятий на примере выбранной системы*
	21-40	*Поверхностное описание без привязки к выбранной системе*
	0-20	*Понятия раскрыты минимально или не раскрыты вовсе*
Количество выполненных заданий	*30*	*Количество выполненных заданий от 85% до 100%*
	15	*Количество выполненных заданий от 55% до 84%*
	0	*Количество выполненных заданий менее 55%*
Итого максимально:	100	

5.5. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для решения задач открытого типа (ПЗ), тестовых заданий студенту разрешается использование калькулятора; программ для работы с электронными таблицами для обработки, анализа и визуализации данных. Для построения интеллект-карты и моделей в различных нотациях студенту можно использовать любой соответствующий онлайн-инструмент.

6. Формы промежуточной аттестации, критерии и шкала оценивания, типовые оценочные материалы по дисциплине

6.1. Промежуточная аттестация проводится в форме **зачета с оценкой.**

Экзамен поводится в устной форме. Обучающийся получает экзаменационный билет с вариантами 2-х заданий различного типа. На выполнение заданий дается 40 минут. По завершении подготовки необходимо представить ответы, подробно изложив ход выполнения задания, сделать выводы (при необходимости).

При реализации промежуточной аттестации в ЭО/ДОТ могут быть использованы следующие формы: устно в ДОТ - в форме обоснованных ответов на задания различного типа; письменно в СДО - в форме письменного решения заданий различного типа; тестирование в СДО.

6.2. Типовые оценочные материалы промежуточной аттестации.

Вопросы для подготовки к зачету с оценкой:

1. Основные понятия криптографии.
2. Основные задачи криптографии.

3. Криптографические протоколы.
4. Простые шифры перестановки и шифры простой замены
5. Криптоанализ простых шифров.
6. Шифры сложной (многоалфавитной) замены.
7. Свойства современных криптосистем.
8. Классификация и виды шифров.
9. Криптостойкость и имитостойкость шифра.
10. Структура блочных шифров.
11. Анализ российских и зарубежных стандартов блочного шифрования.
12. Основные методы анализа блочных криптосистем.
13. Свойства потоковых шифров.
14. Основные методы анализа поточных криптосистем.
15. Потоковые шифры сетей GSM
16. Общие сведения о хэш-функциях.
17. Бесключевые и одноключевые хэш-функции
18. Код аутентификации HMAC.
19. Асимметрические криптосистемы.
20. Система распределения ключей DH.
21. Системы шифрования с открытым ключом.
22. Криптографическая система RSA.
23. Криптографическая система Эль-Гамаля
24. Электронная цифровая подпись.
25. ЭЦП на основе RSA и схемы Эль-Гамаля.
26. Атаки на схемы электронной цифровой подписи.
27. Особенности и специальные виды криптографических протоколов.
28. Протоколы, связанные с ЭЦП.
29. Протоколы аутентификации и распределения ключей.
30. Протоколы разделения секрета (распределения ответственности).
31. Протокол доказательства с нулевым разглашением конфиденциальной информации.
32. Электронные деньги

Типовые проверочные задания для самоподготовки обучающегося к промежуточной аттестации:

<table>
<tr><th>ТИП ЗАДАНИЯ</th><th>СЦЕНАРИИ ВЫПОЛНЕНИЯ</th><th>ТИПОВЫЕ ЗАДАНИЯ</th></tr>
<tr><td>Задание комбинированного типа с выбором одного правильного ответа из нескольких вариантов предложенных</td><td>1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.
2. Внимательно прочитать предложенные варианты ответа.
3. Выбрать один верный ответ.
4. Записать только номер (или букву) выбранного варианта ответа (например, b).</td><td>На основе каких необратимых преобразований базируется алгоритм RSA?
1. Вычисление логарифма в конечном поле
2. Матричные преобразования
3. Разложение произведения больших простых чисел на сомножители
4. Вычисление корней алгебраических уравнений</td></tr>
<tr><td>Задание комбинированного типа на установление соответствия</td><td>1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидаются пары элементов.
2. Внимательно прочитать оба</td><td>Установить соответствие:
<table><tr><td>1.DES</td><td>А. Симметричный блочный алгоритм шифрования</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td>списка: список 1 – вопросы, утверждения, факты, понятия и т.д.;
список 2 – утверждения, свойства объектов и т.д.
3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.
4. Записать попарно буквы и цифры (в зависимости от задания) вариантов ответа (например, А или Б).</td><td><table><tr><td>2.AES</td><td>Б. Асимметричный алгоритм шифрования</td></tr><tr><td>3.RSA</td><td>В Симметричный алгоритм шифрования</td></tr></table></td></tr>
<tr><td>Задание комбинированного типа с выбором нескольких правильных ответов из нескольких вариантов предложенных</td><td>1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько правильных ответов из предложенных вариантов.
2. Внимательно прочитать предложенные варианты ответа.
3. Выбрать несколько правильных ответов.
4. Записать только номера (или буквы) выбранного варианта ответа (например, 1, 4 или a, d).</td><td>1.К алгоритмам с асимметричным шифрованием не относится …
1. ElGamal
2. .RC5
3 ECC
4.RSA
2. Для алгоритма Эль-Гамаля справедливы следующие утверждения
1. Получаемый шифротекст в два раза длиннее открытого текста
2. Открытый и закрытый ключ можно менять местами
3. В алгоритме Эль-Гамаля не используются простые числа
4.При равном значении ключа алгоритмы RSA и Эль-Гамаля имеют одинаковую криптостойкость</td></tr>
<tr><td>Задание комбинированного типа на установление последовательности</td><td>1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.
2. Внимательно прочитать предложенные варианты ответа.
3. Построить верную последовательность из предложенных элементов.
4. Записать буквы/цифры (в зависимости от задания) вариантов ответа в нужной последовательности (например, БВА или 135).</td><td>Установите порядок действий при использовании алгоритма ECDSA для создания подписи.
1 Выбирается случайный закрытый ключ
2 Вычисляется открытый ключ путем умножения базовой точки (G)
3 Подписывающая сторона выбирает случайное число k
4 Вычисляется значение s с использованием формулы s = k^(-1) * (hash(message) + d * x)) mod n</td></tr>
<tr><td>Задание комбинированного типа с выбором одного правильного ответа из предложенных и обоснованием выбора</td><td>1.Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.
2. Внимательно прочитать предложенные варианты ответа.
3. Выбрать один верный ответ.
4. Записать только номер (или букву) выбранного варианта ответа.
5. Записать аргументы, обосновывающие выбор ответа (например, текст обоснования).</td><td>Атака на подпись RSA по выбранному шифротексту базируется на следующем свойстве:
1. Свойстве мультипликативности при возведении в степень
2. Свойстве коммутативности при вычислении логарифма в конечном поле
3. Свойстве коммутативности при возведении в степень</td></tr>
<tr><td>Задание открытого</td><td>1. Внимательно прочитать текст</td><td>1.На основе каких необратимых преобразований</td></tr>
</table>

типа с развернутым ответом	задания и понять суть вопроса. 2.Продумать логику и полноту ответа. 3.Записать ответ, используя четкие компактные формулировки. 4.В случае расчетной задачи, записать решение и ответ	базируется алгоритм RSA. 2. По каким назначениям могут использоваться системы с открытым ключом (СОК)

6.3. Критерии и шкала оценивания на основе БРС.

Критерии и балльная шкала определяются преподавателем

КРИТЕРИИ ОЦЕНИВАНИЯ	РЕЗУЛЬТАТ В БАЛЛАХ
Дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок	40
Дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.	30-39
Дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.	20-29
Дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы	0-19

поверхностны. Решение практических заданий не выполнено, т.е. студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.	

6.4. Описание дополнительных материалов и оборудования, необходимых для выполнения проверочных заданий (*при необходимости*).

Для решения задач открытого типа (ПЗ), тестовых заданий студенту разрешается использование калькулятора; программ для работы с электронными таблицами для обработки, анализа и визуализации данных. Для построения интеллект-карты и моделей в различных нотациях студенту можно использовать любой соответствующий онлайн-инструмент.

7. Методические материалы по освоению дисциплины

Для изучения основных вопросов образовательной программы необходимо конспектировать материалы лекций, работать с рекомендованной преподавателем литературой, а также ресурсами информационно-телекоммуникационной сети «Интернет». Для приобретения навыков активного использования знаний полезно обсуждать плановые и возникающие вопросы, а также решаемые задачи на практических занятиях. Чтобы легче и прочнее усвоить материал следует постоянно использовать конкретные примеры, сравнения из уже полученных областей наук.

Для закрепления изученного материала даны вопросы по каждой теме дисциплины, на которые следует самостоятельно найти ответы.

Важной составной частью учебного процесса в вузе являются практические занятия. Практические занятия проводятся главным образом по дисциплинам, требующим закрепления навыков решения задач, и помогают студентам глубже усвоить учебный материал, приобрести умения применять принципы системного подхода к решению разнообразных задач, определять и оценивать ресурсы и существующие ограничения разного рода проектов.

При подготовке к практическим занятиям необходимо проанализировать конспект лекции, ознакомиться с рекомендованной литературой по соответствующей теме, осуществить подготовку по рекомендованным в рабочей программе вопросам для обсуждения темы, выполнить домашнее задание (при необходимости).

Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю (в том числе по электронной почте). Планируя консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам. Записи имеют первостепенное значение для самостоятельной работы студентов. Они помогают понять построение изучаемого материала,

выделить основные положения, проследить их логику. Кроме того, ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память. Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд методических материалов для быстрого повторения изученных вопросов, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе.

После изучения базовых тем курса проводится текущий контроль знаний студентов в виде опроса или письменного тестирования. Типовые тесты и задания по темам дисциплины приведены в специальном разделе данной рабочей программы.

Подготовка к текущему и промежуточному контролю предполагает изучение представленных вопросов к зачету, работу над тестами, представленными в данной рабочей программе, выполнение семестровой проектной работы по применению системного подхода и методов системного анализа к выбранной системе.

Работа в малых группах – это одна из самых популярных форм проведения занятий, так как она дает всем обучающимся (в том числе и стеснительным) возможность участвовать в работе, практиковать навыки сотрудничества, межличностного общения (в частности, умение активно слушать, вырабатывать общее мнение, разрешать возникающие разногласия). Цель данной формы проведения занятий: продемонстрировать сходство или различия определенных явлений, выработать стратегию или разработать план, выяснить отношение различных групп участников к одному и тому же вопросу. В ходе этой работы дополнительно решаются следующие задача: развитие навыков общения и взаимодействия в группе, формирование ценностно-ориентационного единства группы, поощрение к гибкой смене социальных ролей в зависимости от ситуации.

Группа студентов делится на несколько малых групп. Количество групп определяется числом творческих заданий, которые будут обсуждаться в процессе занятия. Малые группы формируются либо по желанию студентов, либо по родственной тематике для обсуждения. Каждая малая группа обсуждает творческое задание в течение отведенного времени. Основной этап – проведение обсуждения творческого задания. Заслушиваются суждения, предлагаемые каждой малой группой по творческому заданию. Преподаватель дает оценочное суждение и работе малых групп, по решению творческих заданий, и эффективности предложенных путей решения.

В качестве самостоятельной работы студентами выполняется семестровая работа по применению системного подхода и методов системного анализа к выбранной системе по всем темам. Рекомендуется выбрать организационно-техническую систему. Перед выполнением задания по теме 1 выбранную систему необходимо согласовать с преподавателем. При выполнении заданий по темам могут использоваться представленные студентом материалы по предыдущим темам. Выполненная семестровая работа представляется студентом на открытой защите на промежуточной аттестации.

8. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет

8.1. Основная литература

1. Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2020. - 216 с. http://znanium.com/bookread.php?book=432654 Электронный ресурс
2. Баранова Е. К. Информационная безопасность и защита информации: Учебное пособие/ Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2021. - 322 с. - (Высшее образование) ISBN 978-5-369-01450-9 - Режим доступа http://znanium.com/bookread2.php?book=495249
3. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2021 - 120 с. http://znanium.com/bookread.php?book=476047 Электронный ресурс
4. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2022. - 392 с.: http://znanium.com/bookread.php?book=474838 Электронный ресурс

8.2. Дополнительная литература

1. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. - Режим доступа: http://znanium.com/bookread2.php?book=405313
2. Девянин П.Н., Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - 2-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203289.html
3. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. - 118 с. - Режим доступа: http://znanium.com/bookread2.php?book=507334
4. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63099.html
5. Молдовян Н. А. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб.: БХВ-Петербург, 2010. - 293 с. - (Учебное пособие) http://znanium.com/bookread.php?book=351283 Электронный ресурс
6. Партыка Т. Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. http://znanium.com/bookrea,d.php?book=420047 Электронный ресурс
7. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 67 с. — 2227- 8397. — Режим доступа: http://www.iprbookshop.ru/61738.html

8.3. Нормативные правовые документы и иная правовая информация

Не используются

8.4 Интернет-ресурсы

Обучающимся обеспечен доступ к материалам курса в СДО Академии http://lms.ranepa.ru, а так же через сайт научной библиотеки к следующим подписным электронным ресурсам:

Русскоязычные ресурсы

- Электронные учебники электронно-библиотечной системы (ЭБС) *«Айбукс»*
- Электронные учебники электронно-библиотечной системы (ЭБС) *«Юрайт»*
- Электронные учебники электронно-библиотечной системы (ЭБС) *«Лань»*
    - Электронные учебники электронно-библиотечной системы (ЭБС) «*ZNANIUM.COM*»
    - Электронные учебники электронно-библиотечной системы (ЭБС) «BOOK.RU»
- Электронные учебники электронно-библиотечной системы (ЭБС) *«IPRSMART»*

9. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

№ п/п	Наименование
1.	Специализированные залы для проведения лекций, оснащенные персональным компьютером/ноутбуком и мультимедийным проектором
2.	Аудитории и компьютерные классы, оборудованные посадочными местами и персональными компьютерами с выходом в Интернет для проведения практических занятий
3.	Пакет MS Office 2017, Ramus Educational, StarUML, SilaUnion, Archi.
4.	«МТС Линк» — российская платформа для онлайн-коммуникаций и совместной работы команд ; «Яндекс Телемост» — сервис для видеоконференций от Яндекса; Я-мессенджер
5.	Технические средства обучения: персональные компьютеры; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV; программы для работы с электронными таблицами для обработки, анализа и визуализации данных; соответствующие онлайн-инструменты для построения интеллект-карты и моделей в различных нотациях
6.	Научная библиотека (в т.ч. электронные информационные ресурсы научной библиотеки)
7.	СДО Академии https://lms.ranepa.ru/