Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шутов Олег Леонтьевич
Должность: Ректор
Дата подписания: 16.11.2026 14:55:25
Уникальный программный ключ:
6892313c2153d214b87fca0fd68c13fa12d41989

Разработка программно-информационных систем
09.03.04 Программная инженерия
2023 год набора

Приложение В
к основной профессиональной образовательной программе
по направлению подготовки 09.03.04 Программная инженерия,
утвержденной приказом от 07.12.2022 г. № 1-О
(в редакции приказа от 02.11.2026 г. № 87-О)

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ
ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«КУБАНСКИЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»
(АНОО ВО «КИПО»)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.19 Криптография

Направление подготовки

09.03.04 Программная инженерия

Направленность (профиль)

Разработка программно-информационных систем

Уровень высшего образования
Бакалавриат

Квалификация

Бакалавр

Форма обучения
заочная

Год набора
2023

Рабочая программа дисциплины (модуля) Б1.В.19 «Криптография» предназначена для реализации основной профессиональной образовательной программы высшего образования.

Составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 09.03.04 Программная инженерия (Приказ Минобрнауки России от 19.09.2017 г. № 920 зарегистрирован в Минюсте России от 16.10.2017 г. № 48546).

СОДЕРЖАНИЕ

1 Цели и задачи изучения дисциплины(модуля)
1.1 Цель освоения дисциплины (модуля)
1.2 Задачи дисциплины (модуля)
1.3 Место дисциплины (модуля) в структуре образовательной программы
1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы
2. Структура и содержание дисциплины (модуля)
2.1 Распределение трудоёмкости дисциплины (модуля) по видам работ
2.2 Содержание дисциплины (модуля)
2.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
3. Образовательные технологии, применяемые при освоении дисциплины (модуля)
4. Фонды оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)
4.1. Структура оценочных средств для текущего контроля и промежуточной аттестации по дисциплине (модулю)
4.2. Типовые задания для текущего контроля и вопросы (теоретические и практические) для промежуточной аттестации по дисциплине (модулю)
5. Методические указания для обучающихся по освоению дисциплины (модуля)
6. Материально-техническое и учебно-методическое обеспечение по дисциплине (модулю)

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Целью изучения дисциплины Б1.В.19 «Криптография» является освоение студентами основных понятий в области алгоритмизации, свойства алгоритмов, методы анализа сложности алгоритмов и принципов современной криптографии и умение практического применения знаний для защиты информации. Научиться применять при решении задач типичные алгоритмы. Овладеть навыками формировать суждения о своей профессиональной деятельности.

1.2 Задачи дисциплины

дать представления о классических системах шифрование;
дать представление о современных симметричных блочных шифров и о методах их взлома;
дать представление о современных потоковых шифрах;
познакомить с современной ассиметричной криптографией.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.В.19 «Криптография» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» учебного плана.

В соответствии с рабочим учебным планом дисциплина изучается на 4 курсе по заочной форме обучения.

Вид промежуточной аттестации: экзамен.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенции	Код и наименование индикаторов достижения результатов обучения по дисциплине	Планируемые результаты обучения
ПК-7. Способен разрабатывать и анализировать алгоритмы защиты информации	ПК-7.1. Знает понимает математические основы криптографии ПК-7.2. Умеет проводить программную реализацию базовых криптографических примитивов ПК-7.3. Владеет навыками оценки криптографической стойкости алгоритмов, выявлять уязвимости и осуществлять базовый криптоанализ	**Знать:** основные понятия и определения криптографии; математический аппарат, необходимый для построения криптографических алгоритмов (делимость чисел, сравнения, теоремы Эйлера и Ферма, функция Эйлера); классификацию, принципы работы и области применения классических шифров (шифры перестановки, простой и сложной замены); архитектуру, режимы работы и область применения современных симметричных блочных и потоковых шифров; принципы построения асимметричных криптосистем (на примере RSA) и алгоритмов электронной цифровой подписи. **Уметь:** применять аппарат теории чисел для решения задач, связанных с генерацией ключей и шифрованием; выполнять ручное шифрование и дешифрование с использованием классических алгоритмов; выбирать режим шифрования блочного шифра

Код и наименование компетенции	Код и наименование индикаторов достижения результатов обучения по дисциплине	Планируемые результаты обучения
		в зависимости от решаемой прикладной задачи; программно реализовывать на языке высокого уровня базовые криптографические примитивы (шифры замены, перестановки, хеш-функции); использовать стандартные криптографические библиотеки для обеспечения конфиденциальности и целостности данных. **Владеть:** навыками криптоанализа (взлома) простейших классических шифров (частотный анализ, метод перебора); навыками оценки стойкости симметричных и асимметричных алгоритмов к основным видам атак; навыками использования криптографических средств для обеспечения безопасного хранения и передачи информации; навыками работы с нормативной и технической документацией в области криптографической защиты информации.

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 4 зачетные единицы (144 час.), их распределение по видам работ представлено в таблице

Виды работ		Всего часов		
		ОФО	ОЗФО	ЗФО
Контактная работа, в том числе:		**-**	**-**	**16**
Аудиторные занятия (всего):		**-**	**-**	**16**
занятия лекционного типа		-	-	8
практические занятия		-	-	8
Иная контактная работа:				
Контрольная работа		**-**	-	-
Курсовая работа		**-**	-	-
Самостоятельная работа, в том числе:		-	**-**	**119**
Самоподготовка по темам (разделам) дисциплины		-	-	100
Подготовка к текущему контролю		**-**	-	19
Контроль:		**-**	**-**	**9**
Промежуточная аттестация (экзамен)		-	-	9
Общая трудоемкость	**час.**	**-**	**-**	**144**
	в том числе контактная работа	**-**	**-**	**16**
	зач. ед	**-**	**-**	**4**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые на 4 курсе (заочная форма обучения)

№	Наименование темы/раздела	Количество часов				
		Всего	В том числе в виде практической подготовки	Аудиторная работа		Внеаудиторная работа (СР)
				Л	ПЗ	
1.	**Делимость.** 1.1 Простые и составные числа. НОД и НОК чисел. 1.2 Разложение числа на простые множители. 1.3 Сумма и произведение делителей числа.	13	-	1	-	12
2.	**Числовые сравнения.** 2.1 Полная и приведенная системы вычетов. 2.2 Кольцо вычетов по модулю n. 2.3 Функция Эйлера, свойство мультипликативности. Теорема Эйлера. 2.4 Теорема Ферма. 2.5 Диофантовы уравнения первой степени. 2.6 Китайская теорема об остатках.	17	-	1	1	15
3.	**Основные понятия и определения.** 3.1 Шифры перестановки: шифр перестановки «скитала», шифрующие таблицы, применение магических квадратов.	13	-	-	1	12
4.	**Шифры простой замены: полибианский квадрат, система шифрования Цезаря, аффинная система подстановок Цезаря, система Цезаря с ключевым словом.** 4.1 Шифрующие таблицы Трисемуса, биграммный шифр Плейфера, криптосистема Хилла, система омофонов.	16	-	1	1	14
5.	**Шифры сложной замены: шифр Гронсфельда, система шифрования Вижинера, шифр «двойной квадрат» Уитсона.** 5.1 Одноразовая система шифрования, шифрование методом Вернама, роторные машины.	14	-	1	1	12
6.	**Отечественный стандарт шифрования данных ГОСТ.** 6.1 Режим простой замены, режим гаммирования, режим гаммирования с обратной связью, режим выработки имитовставки.	16	-	1	1	14
7.	**Режимы шифрования.** 7.1 Принципы режима шифрования.	16	-	1	1	14
8.	**Другие блочные шифры**. 8.1 Методы блочных шифров.	14	-	1	1	12
9.	**Цифровая подпись.** 9.1 Характеристика цифровой подписи	16	-	1	1	14
	ИТОГО по разделам дисциплины	135	-	8	8	119
	Контрольная работа	-	-	-	-	-

	Курсовая работа	-	-	-	-	-
	Промежуточная аттестация (экзамен)	9	-	-	-	-
	Общая трудоемкость по дисциплине	144	-	8	8	119

Примечание: Л – лекции, ПЗ – практические занятия / семинары, СР – самостоятельная работа обучающегося

При изучении дисциплины могут применятся электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине)

Самостоятельная работа – это индивидуальная познавательная деятельность обучающегося как на аудиторных занятиях, так и во внеаудиторное время. Самостоятельная работа должна быть многогранной и иметь четко выраженную направленность на формирование конкретных компетенций.

Цель самостоятельной работы – овладение знаниями, профессиональными умениями и навыками, опытом исследовательской деятельности и обеспечение формирования профессиональных компетенций, воспитание потребности в самообразовании, ответственности и организованности, творческого подхода к решению проблем.

Самостоятельная работа обучающихся направлена на углубленное изучение разделов и тем рабочей программы. Самостоятельная работа предполагает изучение литературных источников, выполнение контрольных заданий и работ, проведение исследований разного характера. Работа основывается на анализе литературных источников и других материалов, а также реальных фактов, личных наблюдений и т.д.

Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся:

- работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы;
- поиск (подбор) и обзор литературы, электронных источников информации по заданной проблеме курса, написание реферата (доклада, эссе), исследовательской работы по заданной проблеме;
- выполнение задания по пропущенной или плохо усвоенной теме;
- изучение материала, вынесенного на самостоятельную проработку (отдельные темы, параграфы);
- подготовка к практическим занятиям;
- подготовка к промежуточной аттестации.

№ п/п	Вид учебно-методического обеспечения
1.	Методические рекомендации по самостоятельной работе обучающихся.
2.	Методические рекомендации по изучению дисциплины.
3.	Вопросы для письменного/устного собеседования, реферат, сообщение, доклад, эссе, практико-ориентированные задания, мини-кейсы, задания в виде расчетных задач, ситуационные задачи.

Задания для самостоятельной работы обучающихся по дисциплине Б1.В.19 «Криптография» представлены в учебно-методическом отделе.

Контроль результатов самостоятельной работы обучающихся может осуществляться в пределах времени, отведенного на обязательные учебные занятия и

внеаудиторную самостоятельную работу обучающихся по дисциплине, может проходить в письменной, устной или смешанной форме.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) при изучении данной дисциплины предоставлена возможность выбора технологий обучения в зависимости от степени заболевания и осознания своей деятельности. При этом содержание программы дисциплины не изменяется, изменяются, как правило, форма обучения и образовательные технологии. Также обучающимся, имеющим инвалидность, и лицам с ограниченными возможностями здоровья созданы условия комфортного психологического климата в процессе обучения и возможности оказания помощи в установлении полноценных межличностных отношений с другими обучающимися.

3. Образовательные технологии, применяемые при освоении дисциплины (модуля)

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, практические занятия, проблемное обучение, модульная технология, подготовка письменных аналитических работ, самостоятельная работа обучающихся.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (проектных методик, мозгового штурма, разбора конкретных ситуаций, анализа педагогических задач, педагогического эксперимента, иных форм) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины Б1.В.19 «Криптография». Материалы для проведения текущего контроля успеваемости и промежуточной аттестации размещены в фонде оценочных средств по дисциплине Б1.В.19 «Криптография».

4.1. Структура оценочных средств для текущего контроля и промежуточной аттестации по дисциплине (модулю)

№ п/п	Код и наименование индикаторов достижения результатов обучения по дисциплине	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ПК-7.1. Знает понимает математические основы криптографии	**Знать:** основные понятия и определения криптографии; математический аппарат, необходимый для построения криптографических алгоритмов (делимость	Подготовка докладов/сообщений, вопросы для обсуждения по темам, задания открытого и закрытого типа	Вопросы на экзамене
2	ПК-7.2. Умеет проводить программную реализацию базовых		Подготовка докладов/сообщений, вопросы для обсуждения	Вопросы на экзамене

	криптографических примитивов	чисел, сравнения, теоремы Эйлера и Ферма, функция Эйлера); классификацию, принципы работы и области применения классических шифров (шифры перестановки, простой и сложной замены); архитектуру, режимы работы и область применения современных симметричных блочных и потоковых шифров; принципы построения асимметричных криптосистем (на примере RSA) и алгоритмов электронной цифровой подписи. **Уметь:** применять аппарат теории чисел для решения задач, связанных с генерацией ключей и шифрованием; выполнять ручное шифрование и дешифрование с использованием классических алгоритмов; выбирать режим шифрования блочного шифра в зависимости от решаемой прикладной задачи; программно реализовывать на языке высокого уровня базовые криптографические примитивы (шифры замены, перестановки, хеш-функции); использовать стандартные криптографические библиотеки для обеспечения конфиденциальности и целостности данных. Владеть: **навыками криптоанализа**	по темам, задания открытого и закрытого типа	
3	ПК-7.3. Владеет навыками оценки криптографической стойкости алгоритмов, выявлять уязвимости и осуществлять базовый криптоанализ		Подготовка докладов/сообщений, вопросы для обсуждения по темам, задания открытого и закрытого типа	Вопросы на экзамене

		(взлома) простейших классических шифров (частотный анализ, метод перебора); навыками оценки стойкости симметричных и асимметричных алгоритмов к основным видам атак; навыками использования криптографических средств для обеспечения безопасного хранения и передачи информации; навыками работы с нормативной и технической документацией в области криптографической защиты информации.		

4.2. Типовые задания для текущего контроля и вопросы (теоретические и практические) для промежуточной аттестации по дисциплине (модулю)

Задания для текущего контроля и вопросы (теоретические и практические) для промежуточной аттестации, необходимые для оценки образовательных достижений обучающихся.

Текущий контроль успеваемости для обучающихся по заочной форме

Контрольная работа представляет собой систематическое, достаточно полное изложение авторского решения соответствующей проблемы и выполнение заданий в рамках дисциплины, которая является одним из видов текущего контроля успеваемости обучающихся заочной формы обучения.

Цели контрольной работы:

- проверка и оценка знаний обучающихся;
- закрепление практических навыков применения теоретических подходов и методов анализа на учебных примерах и задачах;
- получение информации об уровне самостоятельности и активности обучающегося, об эффективности форм и методов учебной работы.

Контрольные работы выполняются обучающимися в сроки, предусмотренные учебным планом и календарным учебным графиком.

Контрольная работа выполняется в рукописном или в печатном (компьютерном) варианте на листах формата А4 в 1 экземпляре с соблюдением установленного формата. Текст набирается шрифтом Times New Roman 12, через 1 интервал, абзацный отступ - 1,25 см, выравнивание по ширине страницы. Страница должна иметь следующие поля: левое - 25 мм, правое - 10 мм, верхнее и нижнее - 20 мм. Титульный лист содержит информацию об обучающемся выполнившем контрольную работу (ФИО обучающегося, направление подготовки, группа); наименование дисциплины; ФИО преподавателя, проверяющего работу.

Задания для контрольных работ разрабатываются преподавателем дисциплины по вариантам, которые содержат:

1) Задание в форме ответа на теоретический вопрос по теме (разделу) – объем не более 2-3 страниц;
2) Задания, составленные в форме тестов (2 задания открытого и закрытого типа, разработанные в фонде оценочных средств) или ответ на практическое задание (решить ситуацию, математическую задачу, расчетно-графическое задание и др.).

Готовая контрольная работа в электронном виде прикрепляется в электронную образовательную среду Moodle в профиль обучающегося выполнившего работу до начала сессии. Если работа в рукописном варианте, то она должна быть отсканирована и прикреплена.

Шкала и критерии оценивания контрольной работы

№ п/п	Критерии	Зачтено
Теоретический вопрос		
1	Глубина проработки материала	Основные теоретические положения по вопросу раскрыты. Имеются элементы обоснования выводов
2	Представление	Имеются элементы систематизации информации, факты применения профессиональной терминологии
3	Использование рекомендованной литературы	Основные источники рекомендованной литературы использованы
4	Грамотность изложения и качество оформления	Продемонстрирована культура речи. Соблюдены основные требования к оформлению
Выполнение тестовых заданий		

Если работа не отвечает названным критериям, выставляется оценка «не зачтено».

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен)

Теоретические вопросы к экзамену

1. Делимость целых чисел. Основные свойства делимости.
2. Простые и составные числа.
3. НОД и НОК чисел.
4. Числовые сравнения и их свойства.
5. Кольцо Z_n
6. Полна и приведенная система вычетов. Функция Эйлера.
7. Теорема Эйлера и Ферма.
8. Диофантовы уравнений первой степени и способы их решения.
9. Китайская терема об остатках.
10. Основные понятия криптографии.
11. Виды криптографических атак.
12. Шифры перестановки (определение, примеры).
13. Шифры простой замены (определение, примеры).
14. Шифры сложной замены (определение, примеры).
15. Симметричные системы шифрования.
16. Современные блочные шифры (общая схема и пример конкретного шифра с краткой характеристикой)
17. Режимы шифрование блочных шифров.
18. Современные потоковые шифры (общая схема и пример конкретного шифра с краткой характеристикой).

19. Ассиметричные системы шифрования (основные принципы).
20. Комбинированным метод шифрования.
21. Алгоритм RSA.
22. Хеш-функции (определение, примеры).
23. Цифровая подпись (определение, примеры).
24. Криптографические протоколы (определение, примеры)

Практические задания к экзамену

1. В 100-значном числе 12345678901234 ... 7890, вычеркнули все цифры, стоящие на нечетных местах; в полученном 50-значном числе вновь вычеркнули все цифры, стоящие на нечетных местах, и т. д. Вычеркивание продолжалось до тех пор, пока было что вычеркивать. Какая цифра была вычеркнута последней?

2. Как-то раз Таня ехала в поезде. Чтобы не скучать, она стала зашифровывать названия разных городов, заменяя буквы их порядковыми номерами в алфавите. Когда Таня зашифровала пункты прибытия и отправления поезда, то с удивлением обнаружила, что они записываются с помощью всего лишь двух цифр: 21221 - 211221. Откуда и куда шел поезд?

3. Русский алфавит.

Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Дана криптограмма

ФН * Ы = ФАФ

\+ * -

ЕЕ + Е = НЗ

= = =

ИША + МП = ИМН

Восстановите цифровые значения букв, при которых справедливы все указанные равенства, если разным буквам соответствуют различные цифры. Расставьте буквы в порядке возрастания их цифровых значений и получите искомый текст.

4. Какое наименьшее число соединений требуется для организации проводной сети связи из 10 узлов, чтобы при выходе из строя любых двух узлов связи сохранялась возможность передачи информации между любыми двумя оставшимися (хотя бы по цепочке через другие узлы)?

5. Комбинация (x, y, z) трех натуральных чисел, лежащих в диапазоне от 10 до 20 включительно, является отпирающей для кодового замка, если выполнено соотношение F(x, y, z) = 99. Найдите все отпирающие комбинации для замка с F(x,y,z) = 3x2 - y2 - 7z.

6. Ключом шифра, называемого "поворотная" решетка, является трафарет, изготовленный из квадратного листа клетчатой бумаги размера n * n. Некоторые из клеток вырезаются. Одна из сторон трафарета помечена. При наложении этого трафарета на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы полностью покрывают всю площадь квадрата, причем каждая клетка оказывается под вырезом ровно один раз. Буквы сообщения, имеющего длину n2, последовательно вписываются в вырезы трафарета, сначала наложенного на чистый лист бумаги помеченной стороной вверх. После заполнения всех вырезов трафарета буквами сообщения трафарет располагается в следующем положении и т.д. После снятия трафарета на листе оказывается зашифрованное сообщение. Найдите число различных ключей для произвольного четного числа n.

7. Дана последовательность чисел C1, C2, C3, ..., Cn, ..., где Cn есть последняя цифра числа n^n, т.е. $Cn = n^n \bmod 10$. Докажите, что эта последовательность периодическая и ее наименьший период равен 20.

8. Исходное сообщение, состоящее из русских букв и знака пробела (_) между словами, преобразуется в цифровое сообщение заменой каждого ее символа парой цифр согласно следующей таблице:

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	
01	02	03	04	05	06	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Для зашифрования полученного цифрового сообщения используется отрезок последовательности из предыдущей задачи, начинающийся с некоторого Ck. При зашифровании каждая цифра сообщения складывается с соответствующей цифрой отрезка и заменяется последней цифрой полученной суммы. Восстановите сообщение

233986721645816067061731558 8

9. Сколько существует упорядоченных пар натуральных чисел a и b, для которых известны их наибольший общий делитель d = 6 и наименьшее общее кратное m = 6930. Сформулируйте ответ в общем случае, используя канонические разложения d и m на простые множители.

10. Пришло зашифрованное сообщение Ф М Е Ж Т И В Ф Ю Найдите исходное сообщение, если известно, что шифропреобразование заключалось в следующем. Пусть x1, x2 - корни трехчлена $x2 + 3x + 1$. К порядковому номеру каждой буквы в стандартном русском алфавите (33 буквы) прибавлялось значение многочлена $f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$, вычисленное либо при x = x1 либо при x = x2 (в неизвестном нам порядке), а затем полученное число заменялось соответствующей ему буквой.

11. Одна фирма предложила устройство для автоматической проверки пароля. Паролем может быть любой непустой упорядоченный набор букв в алфавите {a, b, c}. Будем обозначать такие наборы большими латинскими буквами. Устройство перерабатывает введенный в него набор P в набор Q = F(P). Отображение F держится в секрете, однако про него известно, что оно определено не для каждого набора букв и обладает следующими свойствами. для любого набора букв P

1) F(aP) = P;

2) F (bP) = F (P)a F(P);

3) набор F(cP) получается из набора F(P) переписыванием его букв в обратном порядке.

Устройство признает предъявленный пароль верным, если F(P) =P. Например, трехбуквенный набор bab является верным паролем, так как F(bab) = F(ab) a F(ab) = bab. Подберите верный пароль, состоящий более чем из трех букв.

12. При установке кодового замка каждой из 26 латинских букв, расположенных на его клавиатуре, сопоставляется произвольное натуральное число, известное лишь обладателю замка. Разным буквам сопоставляются не обязательно разные числа. После набора произвольной комбинации попарно различных букв происходит суммирование числовых значений, соответствующих набранным буквам. Замок открывается, если сумма делится на 26. Докажите, что для любых числовых значений букв существует комбинация, открывающая замок.

13. Рассмотрим преобразование цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена $F(x) = b(x^3 + 7x^2 + 3x + a)$ на число 10, где a, b фиксированные натуральные числа. Выясните, при каких значениях a, b указанное преобразование может быть шифрпреобразованием (то есть допускает однозначное расшифрование).

14. Сообщение, записанное в алфавите АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ зашифровывается при помощи последовательности букв этого же алфавита. Длина последовательности равна длине сообщения. Шифрование каждой буквы исходного сообщения состоит в сложении ее порядкового номера в алфавите с порядковым номером соответствующей буквы шифрующей последовательности и замене такой суммы на букву алфавита, порядковый номер которой имеет тот же остаток от деления на 30, что и эта сумма. Восстановите два исходных сообщения, каждое из которых содержит слово КОРАБЛИ, если результат их зашифрования при ПОМОЩИ ОДНОЙ и той же шифрующей последовательности известен: ЮПТЦАРГШАЛЖЖЕВЦЩЫРВУУ и ЮПЯТБНЩМСДТЛЖГПСГХСЦЦ

15. В компьютерной сети используются пароли, состоящие из цифр. Чтобы избежать хищения паролей, их хранят на диске в зашифрованном виде. При необходимости использования происходит однозначное расшифрование соответствующего пароля. Зашифрование пароля происходит посимвольно одним и тем же преобразованием. Первая цифра остается без изменения, а результат зашифрования каждой следующей цифры зависит только от нее и от предыдущей цифры. Известен список зашифрованных паролей: 4249188780319,4245133784397, 5393511, 428540012393, 4262271910365, 4252370031465,4245133784735 и два пароля 4208212275831, 4242592823026, имеющиеся в зашифрованном виде в этом списке. Можно ли определить какие-либо другие пароли? Если да, то восстановите их.

16. Для передачи сообщений по телеграфу каждая буква русского алфавита (Е и Ё отождествлены) представляется в виде пятизначной комбинации из нулей и единиц, соответствующих двоичной записи номера данной буквы в алфавите (нумерация букв начинается с нуля). Например, буква А представляется в виде 00000, буква Б - 00001, буква Ч - 10111, буква Я - 11111. Передача пятизначной комбинации производится по кабелю, содержащему пять проводов. Каждый двоичный разряд передается по отдельному проводу. При приеме сообщения перепутали провода, поэтому вместо переданного слова получен набор букв ЭАВЬЩО. Найдите переданное слово. «ПАРОЛЬ»

17. При шифровании открытый текст разбивается на блоки одинаковой длины и в каждом блоке осуществляется перестановка букв по одной и той же схеме. Восстановите исходное сообщение по криптограмме.

ПЬОКМ РХТЮЕ ШИРОО МОПЙО ККНЩИ ТОИРП ФАРГА
(45213) (45213) ….
КОМПЬЮТЕР ХОРОШИЙ ПОМОЩНИК КРИПТОГРАФА

18. Коммерсант для передачи цифровой информации с целью контроля передачи разбивает строчку передаваемых цифр на пятерки и после каждых двух пятерок приписывает две последние цифры от суммы чисел, изображенных этими пятерками. Затем процесс шифрования осуществляется путем прибавления к шифруемым цифрам членов арифметической прогрессии с последующей заменой сумм цифр остатками от деления на 10. Прочитайте зашифрованное сообщение:

4 2 3 4 6 1 4 0 5 3 1 3.

19. Буквы русского алфавита занумерованы в соответствии с таблицей: Для зашифровки сообщения, состоящего из n букв, выбирается ключ К - некоторая последовательность из n букв приведенного выше алфавита. Шифрование каждой буквы сообщения состоит в сложении ее номера в таблице с номером соответствующей буквы ключевой последовательности и замене полученной суммы на букву алфавита, номер которой имеет тот же остаток от деления на 30, что и эта сумма. Прочтите шифрованное сообщение: РБЬНПТСИТСРРЕЗОХ, если известно, что шифрующая последовательность не содержала никаких букв, кроме А, Б и В.

20. Тридцати двум буквам русского алфавита А, Б, В, ..Э, Ю, Я приписаны соответственно числа 1, 2, 3, ..30, 31, 0 (буквы Е и Ё отождествляются). Выбрано некоторое нечетное число k (секретный ключ). Шифрование текста осуществляется побуквенно следующим образом:

1) число a, соответствующее данной букве, умножается на k,

2) вычисляется остаток r от деления a*k на 32

3) выписывается буква, соответствующая числу r.

Расшифруйте криптограммы:

1. ЕЦВ РФЗФЧНЙОЯ ЗМСФЦМ АМХХЛЭ

2. ЦОДШФДЮ ПКЫМЙМЯ

3. ЁРЪЫШРЫЪЩДБ ПЪДЛЪКООВЪДАКЩВБ

21. Рассмотрим модель шифра для цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена

$f(x) = b(x3 + 7x7 + 3x + a)$ на число 10, где a, b — фиксированные натуральные числа. Выяснить, при каких значениях a и b возможно однозначное расшифрование.

А-00000 З-01000 Р-10000 Ш-11000
Б-00001 И-01001 С-10001 Щ-11001
В-00010 К-01010 Т-10010 Ъ-11010
Г-00011 Л-01011 У-10011 Ы-11011
Д-00100 М-01100 Ф-10100 Ь-11100
Е-00101 Н-01101 Х-10101 Э-11101
Ё-00110 О-01110 Ц-10110 Ю-11110
Ж-00111 П-01111 Ч-10111 Я-11111

Критерии оценивания промежуточной аттестации: экзамен

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает обучающийся, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает обучающийся, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает обучающийся, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические

	навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает обучающийся, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых институтом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Результат обучения считается сформированным, если теоретическое содержание курса освоено полностью; при устных собеседованиях обучающийся исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными

требованиями, обучающийся способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий.

Результат обучения считается несформированным, если обучающийся при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям.

Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Методические указания для обучающихся по освоению дисциплины на занятиях практического типа

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта

между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

6. Материально-техническое и учебно-методическое обеспечение по дисциплине (модулю)

Основная литература:

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2026. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583783

2. Сдвижков, О. А. Основы математической логики и криптографии. Практикум в Excel. : учебное пособие / О. А. Сдвижков. — Москва : КноРус, 2024. — 356 с. — ISBN 978-5-406-12297-6. — URL: https://book.ru/book/950673 (дата обращения: 10.07.2026). — Текст : электронный.

Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС) и базы данных

Доступ к ЭБС предоставляется из любой точки, в которой имеется доступ к сети «Интернет», как на территории Института, так и вне ее (удаленный доступ).

1. Образовательная платформа «ЮРАЙТ» - URL: https://urait.ru/
2. Электронно-библиотечная система «BOOK.ru» - URL: https://www.book.ru
3. Научная электронная библиотека eLIBRARY.RU - URL: https://elibrary.ru (крупнейшая российская база научных публикаций, доступ к рефератам и полным текстам статей).
4. КиберЛенинка - URL: https://cyberleninka.ru (научная электронная библиотека открытого доступа).

Информационные справочные системы

1. Справочная правовая система «Консультант Плюс» - доступ по локальной сети с компьютеров библиотеки и компьютерных классов (актуальная база законодательства РФ, в т.ч. в сфере образования и социальной защиты).
2. Справочная правовая система «Гарант» - доступ по локальной сети с компьютеров библиотеки и компьютерных классов (актуальная база законодательства РФ, включая сферы образования и социальной защиты).

Профессиональные сообщества и IT-порталы

1. Habr - URL: https://habr.com/ (крупнейшее русскоязычное сообщество IT-специалистов, статьи, новости, обсуждения).
2. Stack Overflow - URL: https://stackoverflow.com/ (международный ресурс для программистов, вопросы и ответы).
3. GitHub - URL: https://github.com/ (платформа для хостинга кода, совместной разработки и открытых проектов).
4. CodeProject - URL: https://www.codeproject.com/ (статьи, примеры кода, обсуждения для разработчиков).
5. Microsoft Learn - URL: https://learn.microsoft.com/ (бесплатные учебные материалы и документация по продуктам Microsoft, .NET, Azure и др.).

6. MDN Web Docs - URL: https://developer.mozilla.org/ (ресурс для **веб-разработчиков с документацией по HTML, CSS, JavaScript и API).**

Научные базы данных зарубежных издательств (открытый доступ)

7. IEEE Xplore - URL: https://ieeexplore.ieee.org/ (доступ к книгам, статьям и материалам конференций по компьютерным наукам, электротехнике и информационным технологиям).

8. ACM Digital Library - URL: https://dl.acm.org/ (библиотека статей и материалов конференций Ассоциации вычислительной техники).

9. SpringerLink - URL: https://link.springer.com/ (книги и журналы издательства Springer, включая серии по информатике).

10. Wiley Online Library - URL: https://onlinelibrary.wiley.com/ (коллекция журналов и книг по направлению «Computer Science & Information Technology»).

Образовательные платформы и онлайн-курсы

11. Национальная платформа «Открытое образование» - URL: https://openedu.ru/ (курсы ведущих российских вузов).

12. Stepik - URL: https://stepik.org/ (российская образовательная платформа с курсами по программированию и информатике).

13. Intuit - URL: https://intuit.ru/ (национальный открытый университет, курсы по информационным технологиям).

Официальные органы государственной власти и управления

1. Министерство науки и высшего образования Российской Федерации - URL: https://www.minobrnauki.gov.ru/.

2. Министерство просвещения Российской Федерации - URL: https://edu.gov.ru/.

3. Министерство труда и социальной защиты Российской Федерации - URL: https://mintrud.gov.ru/.

4. Федеральная служба по надзору в сфере образования и науки (Рособрнадзор) - URL: http://obrnadzor.gov.ru/.

5. Государственная система правовой информации «Законодательство России» - URL: http://pravo.gov.ru/.

Образовательные и справочные порталы

Федеральный портал «Российское образование» - URL: http://www.edu.ru/.

Российское общество «Знание» - URL: https://znanierussia.ru/.

Справочно-информационный портал «Грамота.ру» - URL: http://gramota.ru/ (русский язык и культура речи).

Образовательный портал «Учеба» - URL: http://www.ucheba.com/.

Словари и энциклопедии на Академике - URL: https://dic.academic.ru/.

Проект Государственного института русского языка им. А.С. Пушкина «Образование на русском» - URL: https://pushkininstitute.ru/.

Комплект лицензионного и свободно распространяемого программного обеспечения:

1. LibreOffice - офисный пакет
2. PDFedit – программа для работы с pdf
3. Yandex Browser – браузер
4. Менеджер архивов
5. Libre Base – программа для работы с БД
6. Inkscape – ПО для компьютерной графики
7. DIA – ПО для блока схем и диаграмм
8. 1С: Предприятие – Учебная версия
9. GiMP - Программа обработки изображений

Перечень материально-технического обеспечения включает:

учебные аудитории для проведения занятий лекционного типа, занятий практического (семинарского) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы оснащенные компьютерной техникой с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду Института.

Наименование помещения. Перечень основного оборудования	Адрес
Учебная аудитория № 217 Учебная аудитория для проведения занятий лекционного и практического типа, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля, промежуточной и итоговой аттестации). Оборудование: рабочее место преподавателя (1); рабочие места обучающихся (36); ноутбук с лицензионным ПО (LibreOffice) и возможностью выхода в интернет (1); мультимедийное оборудование (1); доска учебная (1); книжный шкаф (1); сплит-система(1); учебно-наглядные пособия; доступ в электронную информационно-образовательную среду Института.	350002, Краснодарский край, г. Краснодар, Центральный внутригородской округ, ул. им. Леваневского, д. 187/1
Аудитория № 218 Помещение для самостоятельной работы обучающихся Оборудование: рабочие места обучающихся (17); персональный компьютер с лицензионным ПО и возможностью выхода в Интернет (17); книжный шкаф (1); сплит-система (1); учебно-наглядные пособия; доступ в электронную информационно-образовательную среду Института.	350002, Краснодарский край, г. Краснодар, Центральный внутригородской округ, ул. им. Леваневского, д. 187/1