**Автономная некоммерческая организация высшего образования**
**«Информационно-технологический университет»**
**(АНО ВО ИТУ)**

| **ПРИНЯТО** | **УТВЕРЖДАЮ** |
|---|---|
| | Ректор АНО ВО ИТУ Б.С. Лиджиев |
| Решением Ученого Совета<br>АНО ВО ИТУ<br>Протокол № 01 | Сведения об электронной подписи<br>Подписано: Лиджиев Борис Саранович<br>Должность: ректор<br>Пользователь: blidzhiev |
| от « 17 » января 2025 г. | от « 17 » января 2025 г. |

**Фонд оценочных средств (материалов) (актуализированная версия)**
Текущего контроля и промежуточной аттестации
по дисциплине (модулю)

# Б1.В.ДЭ.02.02 СОВРЕМЕННАЯ КРИПТОГРАФИЯ И СТЕГАНОГРАФИЯ

**Для направления подготовки:**
09.03.01 Информатика и вычислительная техника
(уровень бакалавриата)

**Типы задач профессиональной деятельности**:
производственно-технологический

**Направленность (профиль):**
Информационные системы

**Форма обучения**:
очная, очно-заочная, заочная

**г. Элиста, 2025**

***Результаты обучения по дисциплине***

| Код и наименование компетенции | Индикаторы достижения компетенции | Результаты обучения |
|---|---|---|
| **УК-2**<br>Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | **УК-2.2.** Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения | **Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения<br>**Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений<br>**Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов |
| **ПК-2**<br>Способен разрабатывать компоненты программных комплексов и баз данных в соответствии с требованиями технического задания, используя современные инструментальные средства и технологии программирования, оформлять программную и пользовательскую документацию в соответствии с принятыми стандартами | **ПК-2.1.**<br>Выбирает современные инструментальные средства и технологии программирования для решения задач в профессиональной деятельности, оформляет программную и пользовательскую документацию в соответствии с принятыми стандартами | **Знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами данных<br>**Умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами<br>**Владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации |

***Показатели оценивания результатов обучения***

| Шкала оценивания | | | |
|---|---|---|---|
| Неудовлетворительно | Удовлетворительно | Хорошо | Отлично |
| **УК-2.2.** Выбирает оптимальный способ решения задач, учитывая действующие правовые | | | |

| | | | |
|---|---|---|---|
| нормы и имеющиеся условия, ресурсы и ограничения | | | |
| **Не знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Не умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Не владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов | **Поверхностно знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **В целом умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, но испытывает затруднения **В целом владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но испытывает сильные затруднения | **Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения, но допускает несущественные ошибки **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, но иногда допускает небольшие ошибки **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов, но иногда допускает ошибки | **Знает:** методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения **Умеет:** определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **Владеет:** способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов |
| **ПК-2.1.** Выбирает современные инструментальные средства и технологии программирования для решения задач в профессиональной деятельности, оформляет программную и пользовательскую документацию в соответствии с принятыми стандартами | | | |
| **Не знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами | **Поверхностно знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки | **Знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и | **Знает:** основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами |

| | | | |
|---|---|---|---|
| данных<br>**Не умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами<br>**Не владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации | программирования и работы с базами данных<br>**В целом умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами, но испытывает затруднения<br>**В целом владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации, но испытывает сильные затруднения | работы с базами данных, но допускает несущественные ошибки<br>**Умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами, но иногда допускает небольшие ошибки<br>**Владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации, но иногда допускает ошибки | данных<br>**Умеет:** кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами<br>**Владеет:** навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации |

**Оценочные средства (материалы)**

Назовите основные понятия:

| № | Определение | Ответ |
|---|---|---|
| 1. | Данные методы позволяют скрывать секретные сообщения путем их встраивания в послания так, чтобы невозможно было заподозрить существование встроенного тайного послания. | Стеганографические методы |
| 2. | Взаимно-однозначное математическое преобразование, зависящее от ключа (секретного параметра преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок зашифрованной информации, также представленной в цифровой кодировке. | Криптография |
| 3. | Процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц. | Шифрование |
| 4. | Процесс преобразования шифротекста в открытый текст. | Расшифрование |
| 5. | Криптосистема, в которой при шифровании и расшифровании используются одни и те же ключи. | Симметричная криптосистема |
| 6. | Данный вид криптосистем использует пару ключей, один из которых является открытым, а другой – закрытым, известным только его владельцу. | Асимметричная криптосистема |
| 7. | Наука о методах вскрытии шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся под шифрованным. | Криптоанализ |
| 8. | Попытка проведения криптоанализа шифра. | Криптоаналитическая атака |
| 9. | Успешная криптоаналитическая атака, в результате которой противнику становится известным содержание зашифрованного сообщения. | Взломом шифра |
| 10. | Способность шифра противостоять криптоаналитическим атакам. | Стойкость шифра |

Вопросы открытого типа:

| № | Вопрос | Ответ |
|---|---|---|
| 1. | Как называется совокупность методов и средств, которые используются для формирования скрытого канала передачи информации? | Стеганографическая система |
| 2. | Как называется любая открытая информация, предназначенная для сокрытия тайных сообщений? | Контейнер |
| 3. | Что представляет собой конфиденциальная информация любого типа (например, текст, изображение, аудиоданные), подлежащая скрытию? | Сообщение |
| 4. | Как называется техника сокрытия или скрытой передачи информации внутри других незаметных цифровых объектов, таких как изображения, звуковые файлы, видео или текстовые документы? | Метод компьютерной стеганографии |
| 5. | Как называется наука о методах вскрытии шифров, которая отвечает на вопрос о том, как прочесть открытый текст, скрывающийся под шифрованным? | Криптоанализ |
| 6. | Что представляет собой процесс применения криптографических методов и алгоритмов для обеспечения конфиденциальности, целостности и аутентификации данных и коммуникаций, использующий различные математические и алгоритмические техники для шифрования информации таким образом, чтобы только авторизованные пользователи могли получить доступ к расшифрованной информации? | Криптографическая защита |
| 7. | При использовании какого способа символы открытого текста переставляются в соответствии с задаваемым ключом шифрования правилом? | Шифрование способом перестановки |
| 8. | Как называется разновидность шифрования с применением многоалфавитной подстановки, при котором каждый следующий байт открытого текста складывается с предыдущим байтом, а нулевой байт открытого текста — с последним байтом? | Побайтное шифрование |
| 9. | При каком виде шифрования шифротекст получается путем наложения на открытый текст гаммы шифра с помощью какой-либо обратимой операции? | Шифрование способом гаммирования |
| 10. | Что представляет собой относительно небольшой по объему блок данных, передаваемый (хранящийся) вместе (реже — отдельно) с подписываемым с ее помощью документом? | Электронная цифровая подпись |

Тестовые задания:

| | |
|---|---|
| 1 | Электронные и электронно-механические устройства, включаемые в состав технических средств компьютерной системы и выполняющие некоторые функции обеспечения информационной безопасности, называются:<br>a) аппаратными средствами защиты информации;<br>b) антивирусной программой;<br>**c) криптографической системой защиты информации;**<br>d) электронным сторожем. |
| 2 | Криптосистема, в которой при шифровании и расшифровании используются разные ключи, называется<br>a) двухфазной системой;<br>b) ключевой системой;<br>c) симметричной криптосистемой;<br>**d) асимметричной криптосистемой.** |
| 3 | Процесс преобразования шифротекста в открытый текст, называется:<br>a) шифрованием;<br>b) открытием кода;<br>**c) расшифрованием;**<br>d) преобразованием кода. |
| 4 | Криптосистема, в которой при шифровании и расшифровании используются одни и те же ключи, называется:<br>**a) симметричной криптосистемой;**<br>b) продольной криптосистемой;<br>c) простой ключевой системой;<br>d) однородной кодовой системой. |
| 5 | Процесс преобразования открытого текста в шифротекст или криптограмму с целью сделать его содержание непонятным для посторонних лиц: |

| | |
|---|---|
| | a) криптографированием;<br>b) дешифрованием;<br>c) **шифрованием;**<br>d) ниделированием. |
| 6 | Однозначное распознавание уникального имени субъекта компьютерной системы, называется:<br>a) рекриацией;<br>**b) идентификацией;**<br>c) паспортеризацей. |
| 7 | Порция секретной информации (секретный ключ), необходимая для встраивания и извлечения сообщения из контейнера.<br><br>**Стеганографический ключ** |
| 8 | Канал передачи заполненных стегоконтейнеров. Стеганографический канал образует скрытый канал передачи сообщений, когда неочевиден сам факт передачи секретной информации.<br>**Стеганографический канал** |
| 9 | Атрибут электронного документа, который позволяет установить авторство и неизменность после подписания, называется:<br>a) *астрибутивом;*<br>**b)** ***электронной подписью;***<br>c) *провайзером.* |
| 10 | Действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости, называется:<br>a) спинанием;<br>b) инкременцией системы;<br>**c) атакой на компьютерную систему.** |

Ключ к тестовым заданиям

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| c | d | c | a | c |
| **6** | **7** | **8** | **9** | **10** |
| b | Стеганографический ключ | Стеганографический канал | b | c |

**Критерии оценки при проведении промежуточной аттестации**

Оценивание знаний обучающихся осуществляется по 4-балльной шкале при проведении экзаменов и зачетов с оценкой (оценки «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно») или 2-балльной шкале при проведении зачета («зачтено», «не зачтено»).

При прохождении обучающимися промежуточной аттестации оцениваются:

1. Полнота, четкость и структурированность ответов на вопросы, аргументированность выводов.
2. Качество выполнения практических заданий (при их наличии): умение перевести теоретические знания в практическую плоскость; использование правильных форматов и методологий при выполнении задания; соответствие результатов задания поставленным требованиям.
3. Комплексность ответа: насколько полно и всесторонне обучающийся раскрыл тему вопроса и обратился ко всем ее аспектам.

**Критерии оценивания**

| **4-балльная шкала и 2-балльная шкалы** | **Критерии** |
|---|---|
| «Отлично» или «зачтено» | 1. Полные и качественные ответы на вопросы, охватывающие все необходимые аспекты темы. Обучающийся обосновывает свои выводы с использованием соответствующих фактов, данных или источников, демонстрируя глубокую аргументацию.<br>2. Обучающийся успешно переносит свои теоретические знания в практическую реализацию. Выполненные задания соответствуют высокому уровню качества, включая использование правильных форматов, методологий и инструментов.<br>3. Обучающийся анализирует и оценивает различные аспекты темы, демонстрируя способность к критическому мышлению и самостоятельному исследованию. |
| «Хорошо» или «зачтено» | 1. Обучающийся предоставляет достаточно полные ответы на вопросы с учетом основных аспектов темы. Ответы обучающегося имеют ясную структуру и последовательность, делая их понятными и логически связанными.<br>2. Обучающийся способен применить теоретические знания в практических заданиях. Выполнение задания в целом соответствует требованиям, хотя могут быть некоторые недочеты или неточные выводы по полученным результатам.<br>3. Обучающийся представляет хорошее понимание темы вопроса, охватывая основные аспекты и направления ее изучения. Ответы обучающегося содержат достаточно информации, но могут быть некоторые пропуски или недостаточно глубокие суждения. |
| «Удовлетворительно» или «зачтено» | 1. Ответы на вопросы неполные, не охватывают всех аспектов темы и не всегда структурированы или логически связаны. Обучающийся предоставляет верные выводы, но они недостаточно аргументированы или основаны на поверхностном понимании предмета вопроса.<br>2. Обучающийся способен перенести теоретические знания в практические задания, но недостаточно уверен в верности примененных методов и точности в их выполнении. Выполненное задание может содержать некоторые ошибки, недочеты или расхождения.<br>3. Обучающийся охватывает большинство основных аспектов темы вопроса, но демонстрирует неполное или поверхностное их понимание, дает недостаточно развернутые объяснения. |
| «Неудовлетворительно» или «не зачтено» | 1. Обучающийся отвечает на вопросы неполно, не раскрывая основных аспектов темы. Ответы обучающегося не структурированы, не связаны с заданным вопросом, отсутствует их логическая обоснованность. Выводы, предоставляемые обучающимся, представляют собой простые утверждения без анализа или четкой аргументации.<br>2. Обучающийся не умеет переносить теоретические знания в |

| | |
|---|---|
| | практический контекст и не способен применять их для выполнения задания. Выполненное задание содержит много ошибок, а его результаты не соответствуют поставленным требованиям и (или) неправильно интерпретируются.<br>3. Обучающийся ограничивается поверхностным рассмотрением темы и не показывает понимания ее существенных аспектов. Ответ обучающегося частичный или незавершенный, не включает анализ рассматриваемого вопроса, пропущены важные детали или связи. |