МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Институт компьютерных систем и информационных технологий
Кафедра компьютерных систем и сетей

УТВЕРЖДАЮ
Директор _____ Кочевский А. А.
(подпись)
«_10_» _____03_____ 20_25_ года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

«Защита информации»
09.03.01 Информатика и вычислительная техника
«Компьютерные системы и сети»

Разработчик:
ст.преп. _____ Зверева О.С.
(подпись)
ст.преп. _____ Зубков А.В.
(подпись)

ФОС рассмотрен и одобрен на заседании кафедры компьютерных систем и сетей

от «_10_» _____03_____ 20_25_ г., протокол № _8_

Заведующий кафедрой _____ Попов С. В.
(подпись)

Луганск 2025 г.

Комплект оценочных материалов по дисциплине
«Защита информации»

Задания закрытого типа

Задания закрытого типа на выбор правильного ответа

1. Выберите один правильный ответ

Какие основные угрозы могут быть связаны с технической защитой информации?

А) Вирусы и вредоносные программы

Б) Физическое повреждение оборудования

В) Несанкционированный доступ к данным

Г) Все перечисленное выше

Правильный ответ: Г

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

2. Выберите один правильный ответ

Что такое уровень целостности данных?

А) Способность данных быть доступными только для авторизованных пользователей

Б) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения

В) Способность данных быть достоверными и точными

Г) Способность данных быть сохраненными и доступными в случае сбоя системы

Правильный ответ: Б

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

3. Выберите один правильный ответ

Что такое антивирусное программное обеспечение?

А) Программное обеспечение для защиты систем от вирусов

Б) Программное обеспечение для шифрования данных

В) Программное обеспечение для контроля доступа

Г) Программное обеспечение для аутентификации пользователей

Правильный ответ: А

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

4. Выберите один правильный ответ

Кто является регулятором в области обеспечения технической защиты информации в Российской Федерации?

А) Федеральная служба по техническому и экспортному контролю

Б) Федеральная служба безопасности

В) Министерство обороны
Г) Министерство связи и массовых коммуникаций
Правильный ответ: Г
Компетенции (индикаторы): УК-1, УК-6

5. Выберите один правильный ответ
Какой из перечисленных методов является методом аутентификации?
А) Шифрование данных.
Б) Использование паролей.
В) Резервное копирование.
Г) Установка антивируса.
Правильный ответ: Б
Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

6. Выберите один правильный ответ
Что такое конфиденциальность информации?
А) Доступность данных для всех пользователей.
Б) Обеспечение целостности данных.
В) Возможность восстановления данных после сбоев.
Г) Защита данных от несанкционированного доступа.
Правильный ответ: Г
Компетенции (индикаторы): УК-1, УК-6, ОПК-1

7. Выберите один правильный ответ
Что такое фишинг?
А) Вид вредоносного программного обеспечения.
Б) Технология шифрования данных.
В) Метод социальной инженерии для получения конфиденциальных данных.
Г) Способ резервного копирования информации.
Правильный ответ: В
Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

8. Выберите один правильный ответ
Какой из перечисленных алгоритмов используется для шифрования данных?
А) MD5.
Б) AES.
В) SHA-256.
Г) CRC32.
Правильный ответ: Б
Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

Задания закрытого типа на установление соответствия

1. Сопоставьте названия программ и изображения.

Программа		Изображение	
1)	Antivir	А)	
2)	DrWeb	Б)	
3)	Nod 32	В)	
4)	Avast	Г)	

Правильный ответ:

1	2	3	4
Б	Г	А	В

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

2. Установите правильное соответствие. Каждому элементу левого столбца соответствует только один элемент правого столбца.

Термин		Определение
1) Троян	А)	компьютерный вирус, который для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой ОС
2) Файловый вирус	Б)	вредоносная программа, которая маскируется под легальное ПО
3) Макровирус	В)	компьютерный вирус, добавляющий свой код в макросы для создания документов, электронных таблиц и других файлов данных
4) Загрузочный вирус	Г)	вирус, который поражает загрузочный сектор жёсткого

диска или главную загрузочную запись жёсткого диска

Правильный ответ:

1	2	3	4
Б	А	В	Г

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

3. Установите правильное соответствие. Каждому элементу левого столбца соответствует только один элемент правого столбца.

Термин		Определение
1) Физическая защита	А)	метод защиты информации, основанный на преобразовании данных в код различного вида, чтобы информацию нельзя было прочитать, прослушать без расшифровки.
2) Криптографическая защита	Б)	это меры безопасности, применяемые для защиты вычислительных устройств, а также компьютерных сетей
3) Компьютерная защита	В)	это комплекс мер, направленных на защиту прав, свобод и законных интересов физических и юридических лиц в различных правовых ситуациях
4) Юридическая защита	Г)	комплекс мер и средств, направленных на обеспечение безопасности физического состояния объектов, лиц, защиты информации от несанкционированного доступа, вредоносных действий и других угроз

Правильный ответ:

1	2	3	4
Г	А	Б	В

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

4. Установите правильное соответствие. Каждому элементу левого столбца соответствует только один элемент правого столбца.

Термин		Определение
1) Конфиденциальность	А)	состояние, при котором информация либо остаётся неизменной, либо изменения

			осуществляются только теми, кто имеет на это право
2)	Защищенность	Б)	способность системы предоставлять данные и услуги в любое время, независимо от внешних факторов
3)	Целостность	В)	способность противостоять угрозам, защита физического и душевного здоровья
4)	Доступность	Г)	необходимость предотвращения разглашения, утечки какой-либо информации

Правильный ответ:

1	2	3	4
Г	В	А	Б

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

5 . Установите соответствие между типами угроз и их описаниями:

	Тип угроз		Описание
1)	Фишинг	А)	Вредоносное программное обеспечение, которое шифрует данные и требует выкуп.
2)	Вирус	Б)	Метод социальной инженерии для получения конфиденциальных данных.
3)	Ransomware	В)	Программа, способная к самокопированию и распространению по сети.
4)	Черви	Г)	Программа, которая внедряется в систему и нарушает её работу.

Правильный ответ:

1	2	3	4
Б	Г	А	В

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

6. Установите соответствие между методами защиты и их назначением:

	Метод защиты		Назначение
1)	Шифрование	А)	Обнаружение и удаление вредоносного программного обеспечения.
2)	Резервное копирование	Б)	Предотвращение утечки конфиденциальной информации.

3)	Антивирус	В)	Обеспечение доступности данных при сбоях.
4)	DLP-система	Г)	Защита данных от несанкционированного доступа.

Правильный ответ:

1	2	3	4
Г	В	А	Б

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

7. Установите соответствие между алгоритмами и их назначением:

Алгоритм		Назначение	
1)	AES	А)	Устаревший алгоритм хеширования.
2)	RSA	Б)	Асимметричное шифрование данных.
3)	SHA-256	В)	Симметричное шифрование данных.
4)	MD5	Г)	Хеширование данных для проверки целостности.

Правильный ответ:

1	2	3	4
В	Б	Г	А

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

8. Установите соответствие между компонентами информационной безопасности и их описаниями:

Компонент		Описание	
1)	Резервное копирование	А)	Процесс проверки и анализа системы на соответствие требованиям.
2)	Шифрование	Б)	Процесс распознавания пользователя или системы.
3)	Идентификация	В)	Преобразование данных для защиты от несанкционированного доступа.
4)	Аудит	Г)	Создание копий данных для восстановления в случае сбоев.

Правильный ответ:

1	2	3	4
Г	В	Б	А

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

Задания закрытого типа на установление правильной последовательности

1. Установите правильную последовательность этапов создания политики информационной безопасности::

А) Разработка правил и процедур

Б) Обучение сотрудников

В) Анализ рисков

Г) Внедрение и мониторинг

Правильный ответ: В, А, Б, Г

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

2. Установите правильную последовательность действий при реагировании на инцидент информационной безопасности:

А) Восстановление работоспособности

Б) Изоляция затронутых систем

В) Анализ и оценка угрозы.

Г) Обнаружение инцидента

Правильный ответ: Г, В, Б, А

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

3. Установите правильную последовательность этапов шифрования данных:

А) Применение шифрования к данным.

Б) Хранение и управление ключами

В) Генерация ключей.

Г) Выбор алгоритма шифрования

Правильный ответ: Г, В, А, Б

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

4. Установите правильную последовательность шагов для обеспечения резервного копирования данных:

А) Выбор метода резервного копирования

Б) Настройка расписания копирования

В) Проверка целостности резервных копий.

Г) Определение критически важных данных.

Правильный ответ: Г, А, Б, В

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

5. Установите правильную последовательность этапов аутентификации пользователя:

А) Проверка данных на сервере.

Б) Предоставление доступа к системе.

В) Ввод логина и пароля.

Г) Завершение сессии.

Правильный ответ: В, А, Б, Г

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

6. Установите правильную последовательность этапов обработки инцидента утечки данных:

А) Принятие мер по предотвращению повторных инцидентов.

Б) Обнаружение утечки.

В) Уведомление заинтересованных сторон.

Г) Анализ причин и масштаба утечки.

Правильный ответ: Б, Г, В, А

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

7. Установите правильную последовательность этапов внедрения DLP-системы:

А) Мониторинг и анализ работы системы.

Б) Обучение сотрудников.

В) Выбор и настройка DLP-системы

Г) Анализ бизнес-процессов и рисков

Правильный ответ: Г, В, Б, А

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

8. Установите правильную последовательность этапов защиты от вредоносного ПО:

А) Регулярное обновление антивирусных баз.

Б) Сканирование системы на наличие угроз.

В) Установка антивирусного программного обеспечения.

Г) Удаление или изоляция вредоносных программ.

Правильный ответ: В, А, Б, Г

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

Задания открытого типа

Задания открытого типа на дополнение

1. Напишите пропущенное слово (словосочетание).

Процесс представления информации в виде, удобном для ее хранения и передачи - это _____

Правильный ответ: кодирование.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

2. Как называется наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров (тайнописи).

Правильный ответ: криптография.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

3. Напишите пропущенное слово (словосочетание).

Знаковая система представления и передачи информации - это . _____.

Правильный ответ: язык.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

4. Полный набор символов, используемый для кодирования, называют:

Правильный ответ: алфавит.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

5. Напишите пропущенное слово (словосочетание).

Массированная отправка пакетов данных на узлы сети предприятия, с целью их перегрузки и выведения из строя это _____.

Правильный ответ: DOS атака.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

6. Напишите пропущенное слово (словосочетание).

Основные принципы информационной безопасности — это конфиденциальность, _____ и доступность.

Правильный ответ: целостность

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

7. Метод социальной инженерии, направленный на получение конфиденциальных данных, называется _____.

Правильный ответ: фишинг.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

8. Напишите пропущенное слово (словосочетание).

Алгоритм симметричного шифрования, используемый для защиты данных в современных системах, — это _____

Правильный ответ: AES.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

9. Напишите пропущенное слово (словосочетание).

Система, предназначенная для предотвращения утечек конфиденциальной информации, называется _____.

Правильный ответ: DLP.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

10. Напишите пропущенное слово (словосочетание).

Алгоритм хеширования, используемый для проверки целостности данных, — это _____.

Правильный ответ: SHA-256.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

Задания открытого типа с кратким свободным ответом

1. Дайте ответ на вопрос.

1. Какие основные принципы лежат в основе защиты информации?

Правильный ответ: Конфиденциальность, целостность, доступность

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

2. Дайте ответ на вопрос.

Какие методы используются для предотвращения несанкционированного доступа к данным?

Правильный ответ: Правовые, организационные, технические, аппаратные, программные.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

3. Дайте ответ на вопрос

Как называется мошенничество, целью которого является получение доступа к конфиденциальным данным пользователей?

Правильный ответ: Фишинг/ Метод социальной инженерии/ Кибермошенничество

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

4. Дайте ответ на вопрос

Какие меры помогают защитить данные от фишинговых атак?

Правильный ответ: обучение сотрудников/ использование антифишинговых фильтров/ проверка подлинности сайтов/ использование фильтров

Компетенции (индикаторы): УК-1, УК-6, ПК-5

5. Дайте ответ на вопрос

Какие технологии используются для шифрования данных?

Правильный ответ: AES/RSA/DES/методы кодирования/ алгоритмы криптографии.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

6. Дайте ответ на вопрос

Атака, направленная на перегрузку системы или сети с целью нарушения её работы, называется _____.

Правильный ответ: DDoS/ Distributed Denial of Service/кибератака /Ботнет-атака.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

7. Дайте ответ на вопрос.

1. Назовите основные методы аутентификации пользователя?

Правильный ответ: Пароли, биометрические данные, одноразовые коды

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

8. Дайте ответ на вопрос.

Перечислите типы вредоносного программного обеспечения?

Правильный ответ: Вирусы, черви, трояны.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

9. Дайте ответ на вопрос

Перечислите технологии, используемые для защиты сетей?

Правильный ответ: VPN, антивирус, брандмауэр, Sandbox, Управление доступом

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

10. Дайте ответ на вопрос

Назовите три метода резервного копирования данных.

Правильный ответ: Полное, инкрементное, дифференциальное копирование.

Компетенции (индикаторы): УК-1, УК-6, ОПК-1

Задания открытого типа с развернутым ответом

1. Зашифровать текст, используя алгоритм на основе задачи об укладке ранца:

Привести расширенное решение.

Время выполнения – 60 мин.

Ожидаемый результат:

Содержательная постановка задачи.

Дано множество предметов различного веса.

Полный вес равен 270, а последовательность весов предметов равна {2, 3, 6, 13, 27, 52, 105, 210}. Самый большой вес – 210. Он меньше 270, поэтому предмет весом 210 кладут в ранец. Вычитают 210 из 270 и получают 60. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в ранец не кладут. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в ранец. Аналогично проходят процедуру укладки в ранец предметы весом 6 и 2. В результате полный вес уменьшится до 0. Если бы этот ранец был бы использован для дешифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101_2.

Пример дешифрования на основе задачи об укладке ранца

Шифрограмма (нераспределенный вес ранца, S)	Закрытый ключ (вес предмета, M_i)	Открытый текст (бинарный множитель, b_i)
270	210	1

60	105	0
60	52	1
8	27	0
8	13	0
8	6	1
2	3	0
2	2	1

Открытый ключ представляет собой не сверхвозрастающую (нормальную) последовательность. Он формируется на основе закрытого ключа и, как принято считать, не позволяет легко решить задачу об укладке ранца. Для его получения все значения закрытого ключа умножаются на число m по модулю n. Значение модуля n должно быть больше суммы всех чисел последовательности (например, n = 420 [2+3+6+13+27+52+105+210 = 418]). Множитель m должен быть взаимно простым числом с модулем n (например, m = 31). Результат построения нормальной последовательности (открытого ключа) представлен в следующей таблице.

Пример получения открытого ключа

Закрытый ключ, d_i	2	3	6	13	27	52	105	210
Открытый ключ, $e_i = (d_i*m) \bmod n = (d_i*31) \bmod 420$	62	93	186	403	417	352	315	210

Для зашифрования открытый текст сначала преобразуется в бинарный вид и разбивается на блоки, по размерам равные числу элементов последовательности (ключа). Затем, считая, что единица указывает на присутствие элемента последовательности в ранце, а ноль – на его отсутствие, вычисляются полные веса ранцев – по одному ранцу для каждого блока открытого текста.

В качестве примера возьмем открытый текст «АБРАМОВ», символы которого представим в бинарном виде в соответствии с кодировкой Windows 1251. Результат зашифрования с помощью открытого ключа e = {62, 93, 186, 403, 417, 352, 315, 210} представлен в следующей таблице.

Пример зашифрования

Открытый текст		Сумма весов	Шифрограмма (вес ранца), C
Символ	Bin-код		
А	1100 0000	62+93	155
Б	1100 0001	62+93+210	365
Р	1101 0000	62+93+403	558
А	1100 0000	62+93	155
М	1100 1100	62+93+417+352	924

О	1100 1110	62+93+417+352+315	1239
В	1100 0010	62+93+315	470

Правильный ответ: 155, 365, 558,155,924, 1239, 470

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

2. Зашифровать текст, используя алгоритм RSA:

Привести расширенное решение.

Время выполнения – 60 мин.

Ожидаемый результат:

Шифрование:

Выбираем простые числа:

p= 3, q=11

Вычисляем модуль $n = p \cdot q = 3 \cdot 11 = 33$

Вычисляем функцию Эйлера от модуля n : $\varphi(N) = (p-1)(q-1) = = 2 \cdot 10 = 20.$

4. Выбираем открытую экспоненту e=7

5. Определяем закрытую экспоненту d: $d * e = 1\big(mod\varphi(N)\big) \Longrightarrow d = 3$

Будем шифровать сообщение RSA, пусть букве А соответствует цифра 1, В – 2, С - 3 и т.д., тогда:

R=18; S=19; A=1;

Открытый ключ: $(e, n) = (7{,}33)$

$$C_1 = (18^7) mod 33 = 6$$
$$C_2 = (19^7) mod 33 = 13$$
$$C_3 = (1^7) mod 33 = 1$$

Правильный ответ: 6,13,1

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

3. Зашифровать текст, используя Шифр Playfair:

Привести расширенное решение.

Время выполнения – 60 мин.

Ожидаемый результат:

Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 х 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста.

Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – X, для русского алфавита - Я). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес оЯ об ще ни еЯ». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА»

Д	Я	И	Н	А	Б
В	Г	Е	Ё	Ж	З
Й	К	Л	М	О	П
Р	С	Т	У	Ф	Х
Ц	Ч	Ш	Щ	Ы	Ь
Ъ	Э	Ю	-	1	2

Ключевая таблица для шифра Playfair

Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста:

1) Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

2) Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

3) Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Пример шифрования.

- биграмма «за» формирует прямоугольник – заменяется на «жб»;
- биграмма «ши» находятся в одном столбце – заменяется на «юе»;
- биграмма «фр» находятся в одной строке – заменяется на «хс»;
- биграмма «ов» формирует прямоугольник – заменяется на «йж»;
- биграмма «ан» находятся в одной строке – заменяется на «ба»;
- биграмма «но» формирует прямоугольник – заменяется на «ам»;
- биграмма «ес» формирует прямоугольник – заменяется на «гт»;
- биграмма «оя» формирует прямоугольник – заменяется на «ка»;
- биграмма «об» формирует прямоугольник – заменяется на «па»;
- биграмма «ще» формирует прямоугольник – заменяется на «шё»;
- биграмма «ни» формирует прямоугольник – заменяется на «ан»;

- биграмма «ея» формирует прямоугольник – заменяется на «ги».

Правильный ответ: жб юе хс йж ба ам гт ка па шё ан ги

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

4. Имеется криптограмма

HFPSHJB

Найдите исходное сообщение, если известно, что шифрпреобразование заключалось в следующем. Пусть x_1, x_2 - корни трехчлена $x^2 + 5x + 4$. К порядковому номеру каждой буквы в английском алфавите прибавлялось значение многочлена

$$f(x) = x^6 + 5x^5 + 4x^4 + x^3 + 6x^2 + 9x + 5$$

вычисленное либо при $x = x_1$, либо при $x = x_2$ (в неизвестном порядке), а затем полученное число заменялось соответствующей ему буквой.

Привести расширенное решение.

Время выполнения – 60 мин.

Ожидаемый результат:

Для данного многочлена верно разложение:

$f(x) = (x^2 + 5x + 4)(x^4 + x + 1) + 1$.

Это легко проверить просто разделив «столбиком» $f(x)$ на $x^2 + 5x + 4$ с остатком.

Поэтому, и при $x = x_1$, и при $x = x_2$ значение $f(x) = 1$. Таким образом, данное преобразование осуществляет не что иное, как сдвиговый шифр с параметром k=1. Если теперь шифрованное сообщение представить в виде цифровом виде, получим

8 6 16 19 8 10 2

Отнимем от каждого значение 1, получим:

7 5 15 18 7 9 1,

приводим обратно к буквенному виду, получаем ответ.

Правильный ответ: GEORGIA

Компетенции (индикаторы): УК-1, УК-6, ОПК-1, ПК-5

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Защита информации» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки: 09.03.01 Информатика и вычислительная техника.

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины представлены в полном объеме.

Виды оценочных средств, включенные в представленный фонд, отвечают основным принципам формирования ФОС.

Разработанный и представленный для экспертизы фонд оценочных средств рекомендуется к использованию в процессе подготовки обучающихся по указанному направлению.

Председатель учебно-методической комиссии института компьютерных систем и информационных технологий — Ветрова Н.Н.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)