МИНОБРНАУКИ РОССИИ
Кумертауский филиал
федерального государственного
бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»
(Кумертауский филиал ОГУ)

Кафедра электроснабжения промышленных предприятий

Фонд
оценочных средств

по дисциплине *«Защита информационных процессов в автоматизированных системах»*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки)

Автоматизированные системы обработки информации и управления
(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Заочная

Кумертау 2022

Фонд оценочных средств предназначен для контроля знаний обучающихся по направлению подготовки 09.03.01 Информатика и вычислительная техника по дисциплине «*Защита информационных процессов в автоматизированных системах*», рабочая программа по которой зарегистрирована под учетным номером

Фонд оценочных средств рассмотрен и утвержден на заседании
кафедры ЭПП
наименование кафедры

протокол № 1 от "30" августа 2022г.

И.о.зав. кафедрой
ЭПП _____ А.В.Богданов
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры ЭПП _____ Л.Ю.Полякова
должность *подпись* *расшифровка подписи*

Раздел 1. Перечень компетенций, с указанием этапов их формирования в процессе освоения дисциплины

Формируемые компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Виды оценочных средств/ шифр раздела в данном документе
ПК*-2 Способен применять методы моделирования в профессиональной деятельности	ПК*-2-В-5 Использует методы автоматизированного проектирования с использованием современных программных средств	**Знать:** методы автоматизированного проектирования с использованием современных программных средств **Владеть:** способами автоматизированного проектирования с использованием современных программных средств	**Блок А –** задания репродуктивного уровня А.0 Фонд тестовых заданий А.1 Вопросы для опроса на практических занятиях
		Уметь: применять методы автоматизированного проектирования с использованием программных средств	**Блок В –** задания реконструктивного уровня В.1 Типовые задания на практические занятия
		Владеть: способами автоматизированного проектирования с использованием современных программных средств	**Блок С –** задания практико-ориентированного и/или исследовательского уровня С1.индивидуальные творческие задания
ПК*-5 Способен оформлять техническую документацию на различных стадиях разработки проекта автоматизированных систем	ПК*-5-В-1 Понимает принципы оформления технической документации на различных стадиях разработки проекта ПК*-5-В-4 Составляет аналитическое описание систем автоматического управления, выбирает способ представления модели системы управления, оформляет техническую документацию в виде функциональных и структурных схем систем автоматического управления	**Знать:** принципы оформления технической документации на различных стадиях разработки проекта	**Блок А –** задания репродуктивного уровня А.0 Фонд тестовых заданий А.1 Вопросы для опроса на практических занятиях
		Уметь: составлять аналитическое описание систем автоматического управления	**Блок В –** задания реконструктивного уровня В.1 Типовые задания на практические занятия
		Владеть: навыками оформле-	**Блок С –** задания практико-

Формируемые компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Виды оценочных средств/ шифр раздела в данном документе
		ния технической документации на различных стадиях разработки проекта автоматизированных систем	ориентированного и/или исследовательского уровня С1.индивидуальные творческие задания

Раздел 2. Типовые контрольные задания и иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (оценочные средства). Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Блок А - Оценочные средства для диагностирования сформированности уровня компетенций – «знать»

А.1 Фонд тестовых заданий по дисциплине, разработанный и утвержденный в соответствии с Положением о Фонде тестовых заданий 14.03.2017 г.

Пример теста, предъявляемого студенту, изучившему все темы дисциплины (время выполнения теста – не более 40 минут)**:**

Выберите один правильный ответ:

Пример варианта тестов

1. **Как называется внешняя или внутренняя по отношению к атакуемой компьютерной системе программа, обладающая определенными деструктивными функциями по отношению к этой системе?**
1. Компьютерный вирус
2. Программная закладка
3. Аппаратная закладка

2. **Как называется несаморазмножающаяся программа, обеспечивающая злоумышленнику возможности несанкционированного доступа к защищаемой информации?**
1. Компьютерный вирус
2. Ловушка
3. Люк
4. Логическая бомба

3. **Какие из перечисленных свойств присущи компьютерным вирусам?**

1. Способность к включению своего кода в тела других файлов и системных областей памяти компьютера
2. Способность к последующему самостоятельному выполнению и самовоспроизведению
3. Способность к самостоятельному распространению в КС
4. Все перечисленные свойства
5. Только 1 и 3 свойство
6. Только 2 и 3 свойство

4. В чем принципиальное отличие компьютерного вируса от программной закладки?

1. Сложностью написания
2. Возможностью деструктивного воздействия
3. Способностью к саморазмножению и модификации
4. Всеми вышеперечисленными свойствами

5. Что понимается под термином «иерархия доверия»?

1 система проверки цифровых сертификатов
2 система проверки цифровых подписей
3 система аннулирования сертификатов
4 доверенный центр

6. Протокол распределения симметричных ключей

1. Протокол X.509
2. Протокол широкоротой лягушки
3. Протокол S/key
4. Протокол Нидхейма-Шредера
5. Протокол Цербер

7. Какие алгоритмы используют один и тот же ключ для шифрования и дешифровки?

1 асимметричный
2 симметричный
3 правильного ответа нет
4 и ассиметричный и симметричный

8. По какому критерию классифицируется удаленная атака, приводящая к искажению информации?

1. По цели воздействия
2. По характеру воздействия
3. По расположению субъекта атаки относительно атакуемого объекта

9. Как называются СОА обнаруживающие атаки, направленные на всю сеть или сегмент?

1. host-based
2. network-based
3. Системы обнаружения атак на уровне хоста
4. Нет правильных ответов

10. Межсетевой экран предназначен:

1. Для защиты программ от несанкционированного копирования
2. Для обеспечения безопасного доступа к внешней сети и ограничения доступа внешних пользователей к внутренней сети.
3. Для защиты экрана монитора от несанкционированного снятия информации с помощью технических средств разведки.
4. Нет правильных ответов.

А.1 Вопросы для опроса и собеседования

Вопросы для устного опроса, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, факты) и умение правильно использовать специальные термины и понятия дисциплины.

Раздел 1 Введение. Проблемы безопасности информации. Математические основы криптографии. Вычислительна сложность

1. Основные тенденции технологий защиты информации
2. Проблемы безопасности мобильных устройств
3. Проблемы обеспечения безопасности информации
4. Информационная война
5. Какой шифр называют комбинированным или композиционным шифром?
6. Какие факторы влияют на стойкость блочного алгоритма шифрования?
7. Какие простейшие операции применяются в блочных алгоритмах шифрования?
8. В чем отличие блочных алгоритмов шифрования от поточных?
9. Что понимается под "раундом" алгоритма шифрования?
10. Каковы требования к блочному алгоритму шифрования?
11. Почему блочный алгоритм шифрования должен иметь простую и понятную структуру?
12. Что понимается под требованием "высокой криптостойкости" алгоритма шифрования?

Раздел 2 Криптографические методы защиты информации

1. Чем асимметричные алгоритмы шифрования отличаются от симметричных?
2. Для решения каких задач могут на практике применяться алгоритмы шифрования с открытым ключом?
3. Какие математические функции называются односторонними? Для чего они могут применяться в криптографии?
4. Что такое цифровая подпись?
5. Каков алгоритм формирования цифровой подписи при использовании алгоритмов шифрования с открытым ключом?
6. Каким образом алгоритмы шифрования с открытым ключом могут использоваться для формирования общего секретного ключа у группы пользователей?
7. Какие требования предъявляются к асимметричным алгоритмам?
8. Для каких целей может применяться алгоритм RSA?
9. Опишите процесс шифрования с использованием алгоритма RSA.
10. Для каких целей может применяться алгоритм Диффи-Хеллмана?

11. Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана.
12. Для каких целей может применяться алгоритм Эль-Гамаля?.
13. Опишите последовательность действий при использовании алгоритма Эль-Гамаля.

Раздел 3 Технологии аутентификации.

1. Протоколы обмена ключами.
2. Шифрование сетевого трафика.
3. Анализ протоколов распределения ключей.
4. BAN –логика.Какие цифровые подписи называются рандомизированными?
5. В чем заключается проблема сертификации открытых ключей?
6. Что включается в понятие инфраструктуры открытых ключей?
7. Каковы функции центра сертификации открытых ключей?
8. Что такое сертификат открытого ключа?
9. Какая схема распределения открытых ключей абонентов может использоваться в системе связи, имеющей в своем составе центр сертификации открытых ключей?

Раздел 5 Программные средства защиты информации в компьютерных системах

1. Классификация средств защиты информации.
2. Антивирусы.
3. Межсетевые экраны.
4. VPN.
5. Системы обнаружения вторжений.
6. Проблемы и технологии обеспечения безопасности баз данных
7. Проблемы и технологии обеспечения безопасности электронной почты
8. Проблемы и технологии обеспечения безопасности социальных сетей
9. Проблемы и технологии обеспечения безопасности платежных систем
10. Проблемы и технологии обеспечения безопасности облачных сред

Блок Б - Оценочные средства для диагностирования сформированности уровня компетенций – «уметь»

В.0 Варианты заданий на выполнение ПЗ

Ссылка на источники, указанные в списках основной и дополнительной литературы в рабочей программе:

1. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие [Электронный ресурс] / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с.: ил.; 70x100 1/16. - (Высшее образование). (переплет) ISBN 978-5-8199-0411-4. – Режим доступа: http://znanium.com/bookread2.php?book=402686
2. Смарт, Н. Криптография / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. - Москва: Техносфера, 2006. - 528 с. (22)
3. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: учеб. пособие для студентов вузов, обучающихся по направлению 230100

"Информатика и вычислительная техника" / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с. (12)

B.2 Типовые задачи на практические занятия:

Раздел 2 Криптографические методы защиты информации

1.Сложите по модулю 2:

- двоичные числа 10101100 и 11001010 ;
- десятичные числа 15 и 10 ;
- шестнадцатеричные числа 0B5 и 37.

Примечание: десятичные и шестнадцатеричные числа необходимо сначала перевести в двоичный вид.

2.Сложите по модулю 2^8:

- двоичные числа 10101100 и 11001010 ;
- десятичные числа 155 и 100 ;
- шестнадцатеричные числа 0B5 и 37.

Примечание: десятичные числа необходимо сначала перевести в двоичный вид.

3.Являются ли простыми числа 37, 59, 67, 93, 101, 111, 231?

4.Являются ли взаимно простыми числа:

- 16 и 37
- 16, 37 и 38

Блок C - Оценочные средства для диагностирования сформированности уровня компетенций – «владеть»

C.0 Индивидуальные творческие задания

1. Пусть пользователь А хочет передать пользователю Б сообщение m=10, зашифрованное с помощью алгоритма RSA. Пользователь Б имеет следующие параметры: P=7, Q=11, d=47. Опишите процесс передачи сообщения m пользователю Б.
2. Вычислите закрытые ключи Y_1, Y_2 и общий ключ Z для системы Диффи-Хеллмана с параметрами A=3, P=7, X_1=3, X_2=6.
3. В системе связи, применяющей шифр Эль-Гамаля, пользователь 1 желает передать сообщение m пользователю 2. Найдите недостающие параметры при следующих заданных параметрах P = 19, A = 2, X_2 = 3, k = 5, m = 10.
4. Абоненты некоторой сети применяют цифровую подпись по стандарту ГОСТ Р34.10-94 с общими параметрами p = 47, q = 23, a = 37. Найдите открытый ключ абонента Петрова для X = 8.
5. Абоненты некоторой сети применяют цифровую подпись по алгоритму Эль-Гамаля с общими параметрами P = 17, A = 3. Найдите открытый ключ абонента Петрова для X = 11.

Блок D - Оценочные средства, используемые в рамках промежуточного контроля знаний, проводимого в форме экзамена

Вопросы к экзамену

1. Информационная безопасность: понятие, цель, задачи, методы обеспечения безопасности.
2. Содержание и структура понятия компьютерной безопасности
3. Общие принципы обеспечения компьютерной безопасности
4. Криптография. Основные понятия. Шифры замены. Шифры перестановки.
5. Классификация криптоалгоритмов. Обобщенная схема криптосистемы
6. Блочные шифры: понятия, сеть Фейстеля.
7. Симметричные шифры. Принцип Кирхгофа. Условия стойкости
8. Блочные шифры. Архитектура блочных шифров
9. Шифр Магма. Шифр Кузнечик.
10. Режимы блочного шифра. Алгоритм Диффи-Хелмана.
11. Ассиметричные криптоалгоритмы. Концепция криптосистемы с открытым ключом. Односторонние функции.
12. Алгоритм RSA.
13. Электронная цифровая подпись: понятие, отличия от рукописной подписи. Подходы к созданию схем цифровой подписи.
14. Понятия идентификации, аутентификации, авторизации. Принципы аутентификации. Классификация методов аутентификации.
15. Управление криптографическими ключами. Криптографические протоколы.
16. Распределение секретных ключей с помощью системы с открытым ключом.
17. Авторизация. Основные понятия. Политика разграничения доступа. Типы (модели) политики безопасности. Единый диспетчер доступа.
18. Понятия: межсетевые экраны, VPN.
19. Классификация систем обнаружения атак
20. Классическая архитектура системы обнаружения атак
21. Подходы к обнаружению атак

Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Оценивание выполнения тестов

4-балльная шкала	Показатели	Критерии
Отлично	1. Полнота выполнения тестовых заданий; 2. Своевременность выполнения; 3. Правильность ответов на вопросы; 4. Самостоятельность тестирования.	Выполнено 90% и более заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос.
Хорошо		Выполнено 75 - 89 % заданий предложенного теста, в заданиях открытого типа дан полный, развернутый ответ на поставленный вопрос; однако были допущены неточности в определении понятий, терминов и др.
Удовлетвори-		Выполнено 60 -74% % заданий

4-балльная шкала	Показатели	Критерии
тельно		предложенного теста, в заданиях открытого типа дан неполный ответ на поставленный вопрос, в ответе не присутствуют доказательные примеры, текст со стилистическими и орфографическими ошибками.
Неудовлетвори-тельно		Выполнено <59% заданий предложенного теста, на поставленные вопросы ответ отсутствует или неполный, допущены существенные ошибки в теоретическом материале (терминах, понятиях).

Оценивание выполнения практических заданий

4-балльная шкала	Показатели	Критерии
Отлично	1. Полнота выполнения практического задания; 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения задания; 4. Самостоятельность решения; 5. Аргументирование обоснование алгоритма решения задачи (выбора программного средства).	Задание решено самостоятельно. Студент владеет необходимыми навыками и приемами решения задач, материал в точности соответствует выбранной теме, студент последовательно, четко и логически может пояснить ход выполнения работы, причем не затрудняется с ответами на дополнительные вопросы.
Хорошо		Задание решено с подсказками преподавателя. Материал соответствует выбранной теме, студент владеет необходимыми навыками и приемами решения задач, но при защите работы допускаются незначительные неточности. Способен решить задачу при изменении ее контекста.
Удовлетвори-тельно		Задание решено с помощью преподавателя. Материал не является полным, решение задачи реализовано частично и при этом студент не всегда может пояснить ход выполнения работы. Затрудняется дать ответы на дополнительные вопросы. Не способен решить задачу при изменении ее контекста.
Неудовлетвори-тельно		Студент не может пояснить ход выполнения работы; материал не соответствует выбранной теме или задание не решено.

Оценивание выполнения творческого задания

4-балльная шкала	Показатели	Критерии
Отлично	1. Полнота выполнения практического задания; 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения задания; 4. Самостоятельность решения; 5. Аргументирование обоснование алгоритма решения задачи (выбора программного средства).	Задание выполнено самостоятельно. Студент владеет необходимыми навыками и приемами решения задач, материал в точности соответствует выбранной теме, студент последовательно, четко и логически может пояснить ход выполнения работы, причем не затрудняется с ответами на дополнительные вопросы.
Хорошо		Задание выполнено с подсказками преподавателя. Материал соответствует выбранной теме, студент владеет необходимыми навыками и приемами решения задач, но при защите работы допускаются незначительные неточности. Способен решить задачу при изменении ее контекста.
Удовлетвори-тельно		Задание выполнено с помощью преподавателя. Материал не является полным, решение задачи реализовано частично и при этом студент не всегда может пояснить ход выполнения работы. Затрудняется дать ответы на дополнительные вопросы. Не способен решить задачу при изменении ее контекста.
Неудовлетвори-тельно		Студент не может пояснить ход выполнения работы; материал не соответствует выбранной теме или задание не выполнено.

Оценивание ответа на зачете

Бинарная шкала	Показатели	Критерии
Зачтено	1. Полнота изложения теоретического материала; 2. Полнота и правильность решения практического задания; 3. Самостоятельность ответа; 4. Культура речи.	Дан развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в объеме учебной программы, осмысливает дисциплину, самостоятельно, и отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания (допускается небольшими неточности)

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

Раздел 3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Процедура проведения тестирования

Тестирование проводится по тестам на электронном или бумажном носителе по отдельным темам, ответы на тестовые задания студент оформляет на листе и сдает преподавателю. На тестирование отводится 30 минут. Вариант тестовых заданий включает в себя 15 вопросов. При тестировании используются следующие варианты ответов на тестовое задание: один из нескольких, несколько из нескольких, выбор из списка, ответ текстом, графический ответ. Критерии оценивания соответствуют приведенной шкале.

Процедура выполнения практических заданий

Практическое задание выполняется студентом в аудиторное время или во внеаудиторное время самостоятельно согласно сформулированному заданию. Выполнение практического задания предполагает применение методологических знаний и умений, накопленного опыта творческой деятельности, использование эвристических методов. Студент может выполнить задание в изучаемом программном средстве или использовать его аналог. Выполненное задание студент сохраняет в файле соответствующего типа, отправляет преподавателю по почте или приносит лично. Выполнение задания осуществляется студентом весь период времени между сессиями. При проверке задания студент объясняет ход выполнения задания, отвечает на вопросы. Оценивание задания производится по четырехбалльной шкале.

Методика выполнения индивидуального творческого задания

Творческое задание выполняется на занятии или дома. Творческое задание требует использования дополнительного материала по изучаемой теме. Выполнение комплексного задания предполагает применение методологических знаний и умений, накопленного опыта творческой деятельности, использование эвристических методов. Студент может выполнить задание в изучаемом

программном средстве или использовать его аналог. Выполненное задание студент сохраняет в файле соответствующего типа, отправляет преподавателю по почте или приносит лично. На выполнение задания отводится 1-2 недели. При проверке задания студент объясняет ход выполнения задания, отвечает на вопросы. Оценивание задания производится по четырехбалльной шкале.

Методические материалы, определяющие процедуру оценивания при зачете

Зачет может быть проведен в устной форме, в форме письменной работы или тестирования. Вопросы на зачет утверждаются на заседании кафедры текущего учебного года и подписываются заведующим кафедрой. Форма проведения зачета, содержание заданий определяется преподавателем, читающим лекции по данной дисциплине.

Перечень примерных вопросов, заданий и критерии оценки доводятся до сведения обучающихся в начале изучения дисциплины. Число вопросов, включаемых в задание, должно быть не менее двух и не более пяти, при этом вопросы могут носить как теоретический, так и прикладной характер. На зачет могут выноситься типовые задачи, проработанные в течение семестра на аудиторных занятиях и в процессе самостоятельной работы. Содержание вопросов и задач, включаемых в задание, должно соответствовать учебной программе дисциплины.

Зачет проводится в соответствии с утвержденным расписанием, определяющим время и место его проведения.

При проведении устного зачета обучающийся получает вопросы к зачету. Преподаватель, проводящий зачет имеет право с целью выяснения глубины знаний задавать обучающимся не более 2-3 дополнительных вопросов в рамках тем. Зачет должен быть методически обеспечен (программа курса и критерии оценок, утвержденные на заседании кафедры). Во время зачета обучающийся имеет право пользоваться словарями, таблицами и другой справочной литературой только при наличии соответствующего разрешения кафедры.

При подготовке к устному зачету обучающийся ведет записи на листе подготовки к ответу, который затем сдает преподавателю, проводящему зачет. Лист подготовки к ответу может быть рассмотрен в случае подачи обучающимся апелляции.

Зачет в форме письменной работы выполняется под наблюдением преподавателя.

Зачет в форме тестирования (зачет в письменном виде) включает вопросы и (или) задачи по всему курсу. Продолжительность тестирования должна быть не менее одного, но не более трех академических часов. Продолжительность зачета в форме компьютерного тестирования должна быть не менее одного, но не более двух академических часов.

Проверка письменных работ и тестов осуществляется преподавателем, на последней странице письменной работы и теста ставится дата проверки и подпись преподавателя.

Результаты письменной работы и теста должны быть объявлены в течение 24 часов после завершения зачета. Листы подготовки к устному зачету, письменные работы и результаты тестирования должны храниться на кафедре до окончания срока апелляции.

Неявка на зачет отмечается в зачетно-экзаменационной ведомости словами «не явился» и заверяется подписью преподавателя.

Если во время сдачи или пересдачи зачета со стороны обучающегося допущены нарушения учебной дисциплины (списывание, использование средств мобильной

связи, ПК, аудиоплейеров, других технических устройств), нарушения Правил внутреннего распорядка Кумертауского филиала ОГУ, предпринята попытка подлога документов, преподаватель вправе удалить обучающего с зачета с выставлением в ведомости отметки «не зачтено».

Компетенции, знания, умения и навыки обучающихся оцениваются оценками: «зачтено», «не зачтено».