

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

Факультет компьютерных систем и информационных технологий
Кафедра автоматизации и компьютерно-интегрированных технологий



УТВЕРЖДАЮ

Декан факультета компьютерных систем
и информационных технологий

Кочевский А. А.

« 19 » 04 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

«Безопасность автоматизированных систем»

15.03.04 Автоматизация технологических процессов и производств

«Компьютерные и специализированные системы автоматизации производств»

Разработчик:

доцент  Воронов А. Э.

ФОС рассмотрен и одобрен на заседании кафедры автоматизации и компьютерно-интегрированных технологий от 18 апреля 2023 г., протокол № 17

Заведующий кафедрой  Колесников А. В.

Луганск 2023 г.

**Паспорт
фонда оценочных средств по учебной дисциплине
«Безопасность автоматизированных систем»**

**Перечень компетенций (элементов компетенций),
формируемых в результате освоения учебной дисциплины**

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Контролируемые разделы (темы) учебной дисциплины	Этапы формирования (семестр изучения)
1	ПК-1	способен проводить анализ технологических процессов механосборочного производства с целью выявления операций, подлежащих автоматизации и механизации	Тема 1. Введение в безопасность автоматизированных систем Тема 2. Система информационной безопасности Тема 3. Программно-технические методы и средства защиты информации Тема 4. Криптографические механизмы защиты информации в информационных системах Тема 5. Методы криптографического закрытия информации Тема 6. Методы кодирования информации Тема 7. Методы сжатия-расширения информации Тема 8. Модели управления доступом Тема 9. Методы хранения данных Тема 10. Защита программ от изучения	8
2	ПК-4	способен осуществлять подготовку к выпуску проекта автоматизированной системы управления технологическими процессами	Тема 1. Введение в безопасность автоматизированных систем Тема 2. Система информационной безопасности Тема 3. Программно-технические методы и средства защиты информации Тема 4. Криптографические механизмы защиты информации в информационных системах Тема 5. Методы криптографического закрытия информации Тема 6. Методы кодирования информации Тема 7. Методы сжатия-расширения информации Тема 8. Модели управления доступом Тема 9. Методы хранения данных Тема 10. Защита программ от изучения	8

**Показатели и критерии оценивания компетенций, описание шкал
оценивания**

№ п/п	Код контролируемой	Показатель оценивания (знания, умения, навыки)	Контролируемые темы учебной	Наименование оценочного
-------	--------------------	--	-----------------------------	-------------------------

	компетенции		дисциплины	средства
1	ПК-1	<p>знать: методику разработки концепции автоматизированных систем управления технологическими процессами;</p> <p>уметь: разрабатывать концепции автоматизированных систем управления технологическими процессами;</p> <p>владеть навыками разработки концепции автоматизированных систем управления технологическими процессами;</p>	<p>Тема 1.</p> <p>Тема 2.</p> <p>Тема 3.</p> <p>Тема 4.</p> <p>Тема 5.</p> <p>Тема 6.</p> <p>Тема 7.</p> <p>Тема 8.</p> <p>Тема 9.</p> <p>Тема 10.</p>	Лабораторные работы, индивидуальное задание
2	ПК-4	<p>знать: правила осуществления авторского надзора за изготовлением, испытанием, внедрением и эксплуатацией автоматизированных систем управления технологическими процессами, а также методику обеспечения защиты авторских прав на решения, содержащиеся в разрабатываемых проектах;</p> <p>уметь: осуществлять авторский надзор за процессом изготовления автоматизированных систем управления технологическими процессами и обеспечивать мероприятия по защите авторских прав на решения, содержащиеся в разрабатываемых проектах;</p> <p>владеть: навыками осуществления авторского надзора за процессом изготовления автоматизированных систем управления технологическими процессами и обеспечения мероприятий по защите авторских прав на решения, содержащиеся в разрабатываемых проектах;</p>	<p>Тема 1.</p> <p>Тема 2.</p> <p>Тема 3.</p> <p>Тема 4.</p> <p>Тема 5.</p> <p>Тема 6.</p> <p>Тема 7.</p> <p>Тема 8.</p> <p>Тема 9.</p> <p>Тема 10.</p>	Лабораторные работы, индивидуальное задание

**Фонды оценочных средств по дисциплине
«Безопасность автоматизированных систем»**

Пример лабораторной работы «Криптосистема шифрования данных RSA».

Цель: получить навыки выработки и применения ключей для RSA алгоритма.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить основы работы алгоритма RSA.
2. Изучить способы проверки числа на «простоту».
3. Выполнить типовой пример, сравнить результаты.
4. Выполнить задание согласно варианта.
5. Сохранить результаты выполнения для отчета по проделанной работе.
6. Подготовить отчет по выполненной лабораторной работе.

ПРИМЕР ВАРИАНТА ЗАДАНИЯ

1. Зашифровать текст, используя RSA-метод (заполнить пустые поля таблицы по вариантам).
2. Расшифровать полученную криптограмму.
3. Выработать ключ длины 2048 бит. Зашифровать и расшифровать произвольное сообщение.

СОДЕРЖАНИЕ ОТЧЕТА

1. Название и цель работы.
2. Общие теоретические сведения.
3. Исходные коды реализации задания по варианту.
4. Анализ результатов и выводы.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Основные требования к ключам алгоритма RSA, обеспечивающие криптостойкость.
2. Методы проверки простоты числа.
3. Определение взаимопростоты чисел.
4. Китайская теорема об остатках.
5. Быстрое возведение числа в степень по модулю.
6. Последовательность выработки ключей для алгоритма RSA.
7. Шифрование текстовой и битовой информации алгоритмом RSA.
8. Доказательство корректности схемы RSA.
9. Цифровая подпись алгоритмом RSA.
10. Малая теорема ферма.

Критерии и шкала оценивания по оценочному средству «Лабораторная работа»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Лабораторная работа выполнена самостоятельно на высоком уровне и в полном объеме, отчет оформлен в соответствии с требованиями, сделаны правильные выводы по проведенным экспериментам.
4	Лабораторная работа выполнена самостоятельно на среднем уровне и в полном объеме, отчет оформлен с незначительными отклонениями от требований, допущены незначительные неточности в выводах по проведенным экспериментам
3	Лабораторная работа выполнена на низком уровне и не полностью, отчет оформлен с отклонениями от требований, выводы по экспериментам сделаны не в полном объеме.
2	Лабораторная работа не выполнена, отчет не оформлен, или представленный отчет не соответствует варианту задания.

Индивидуальные задания

Используя алгоритмы «шифрование данных RSA», «перестановка гиперкуб Гамильтона», «XOR шифрование» зашифровать, передать по информационной сети, и расшифровать сообщение, составленное из следующих данных:

- Ваши Фамилия Имя Отчество;
- Номер зачетной книжки;
- Текущий учебный год обучения (например, 2023-2024);
- Название академической группы;
- Шифр и название направления подготовки;
- Название специальности;
- Название кафедры;
- Название факультета;
- Название университета.

Для решения задания должны быть применены все три алгоритма в порядке выбранном самостоятельно (в пояснительной записке необходимо обосновать выбранную последовательность).

Задание должно быть решено, как минимум, двумя способами: вручную, программой на языке C++ (или другом языке программирования по согласованию с преподавателем).

Критерии и шкала оценивания по оценочному средству «Индивидуальное задание»

Шкала оценивания	Критерий оценивания
5	Индивидуальное задание выполнено самостоятельно на высоком уровне и в полном объеме, отчет оформлен в соответствии с требованиями, сделаны правильные выводы по проведенным экспериментам и\или полученным результатам
4	Индивидуальное задание выполнено самостоятельно на среднем уровне и в полном объеме (более 90% задач), отчет оформлен с незначительными отклонениями от требований, допущены незначительные неточности в выводах по проведенным экспериментам и\или полученным результатам.
3	Индивидуальное задание выполнено на низком уровне и\или не полностью (более 50% задач), отчет оформлен с отклонениями от требований, выводы по экспериментам и\или полученным результатам сделаны не в полном объеме.
2	Индивидуальное задание не выполнено (менее 50% задач), отчет не оформлен, или представленный отчет не соответствует варианту задания

Оценочные средства для промежуточной аттестации

Зачет выставляется автоматически при условии защиты всех лабораторных работ и индивидуального задания на оценку не ниже 3 балла.

Критерии и шкала оценивания по оценочному средству «зачет»

Шкала оценивания	Характеристика знания предмета и ответов
зачтено	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач. Успешно выполняющий предусмотренные в программе задания.
не зачтено	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы. Предусмотренные в программе задания выполнены не полностью.

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)

Экспертное заключение

Представленный фонд оценочных средств (далее – ФОС) по дисциплине «Безопасность автоматизированных систем» соответствует требованиям ФГОС ВО.

Предлагаемые формы и средства текущего и промежуточного контроля адекватны целям и задачам реализации основной профессиональной образовательной программы по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств.

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 факультета компьютерных
систем и информационных технологий



Ветрова Н. Н.