МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**
федеральное государственное бюджетное образовательное учреждение высшего образования
**САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ (СамГУПС)**

УТВЕРЖДЕНА:
решением Учёного совета СамГУПС
протокол №50 от 27.03.19г.
в составе основной профессиональной образовательной программы

АКТУАЛИЗИРОВАНА:
решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС .№59 от 25.02.20г.

решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС №___от_____.

решением Учёного совета СамГУПС
протокол Учёного совета СамГУПС №___от_____.

# Защита информации

## рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Мехатроника, автоматизация и управление на транспорте**

Учебный план 09.03.01-19-1-ИВТб.plm.plx
09.03.01 Информатика и вычислительная техника

Проектирование АСОИУ на транспорте

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 56
самостоятельная работа 51,75

Виды контроля в семестрах:
зачеты 8

**Распределение часов дисциплины по семестрам**

| Семестр (<Курс>.<Семестр на курсе>) | **8 (4.2)** | | Итого | |
|---|---|---|---|---|
| Недель | 7,7 | | | |
| Вид занятий | УП | РП | УП | РП |
| Лекции | 28 | 28 | 28 | 28 |
| Лабораторные | 28 | 28 | 28 | 28 |
| Контактные часы на | 0,25 | 0,25 | 0,25 | 0,25 |
| Итого ауд. | 56 | 56 | 56 | 56 |
| Контактная работа | 56,25 | 56,25 | 56,25 | 56,25 |
| Сам. работа | 51,75 | 51,75 | 51,75 | 51,75 |
| Итого | 108 | 108 | 108 | 108 |

**Самара 2019**

**Визирование РПД для исполнения в очередном учебном году**

Зав. выпускающей кафедрой **09.03.01**
к.т.н., доцент Авсиевич А.В. __ _____ 2020 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры
**Мехатроника, автоматизация и управление на транспорте**

Протокол от __ _____ 2020 г. № __
Зав. кафедрой к.т.н., доцент Авсиевич А.В.

**Визирование РПД для исполнения в очередном учебном году**

Зав. выпускающей кафедрой **09.03.01**
к.т.н., доцент Авсиевич А.В. __ _____ 2021 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры
**Мехатроника, автоматизация и управление на транспорте**

Протокол от __ _____ 2021 г. № __
Зав. кафедрой к.т.н., доцент Авсиевич А.В.

**Визирование РПД для исполнения в очередном учебном году**

Зав. выпускающей кафедрой **09.03.01**
к.т.н., доцент Авсиевич А.В. __ _____ 2022 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры
**Мехатроника, автоматизация и управление на транспорте**

Протокол от __ _____ 2022 г. № __
Зав. кафедрой к.т.н., доцент Авсиевич А.В.

**Визирование РПД для исполнения в очередном учебном году**

Зав. выпускающей кафедрой **09.03.01**
к.т.н., доцент Авсиевич А.В. __ _____ 2023 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
**Мехатроника, автоматизация и управление на транспорте**

Протокол от __ _____ 2023 г. № __
Зав. кафедрой к.т.н., доцент Авсиевич А.В.

| 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) | |
|---|---|
| 1.1 | Сформировать систему компетенций для усвоения теоретических, практических, современных представлений о основных принципах, методах и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах |

| 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ | |
|---|---|
| Цикл (раздел) ОП: | Б1.О.21 |
| **2.1** | **Требования к предварительной подготовке обучающегося:** |
| 2.1.1 | Информатика |
| 2.1.2 | Производственная практика, технологическая (проектно-технологическая) практика |
| 2.1.3 | Учебная практика, технологическая (проектно-технологическая) практика |
| **2.2** | **Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:** |
| 2.2.1 | Выпускная квалификационная работа |
| 2.2.2 | Интерфейсы периферийных устройств |
| 2.2.3 | Проектирование АСОИУ |
| 2.2.4 | Проектирование пользовательского интерфейса |
| 2.2.5 | Производственная практика, преддипломная практика |

| 3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) |
|---|
| **ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;** |

| | |
|---|---|
| Индикатор | ОПК-3.1.<br>Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. |
| Индикатор | ОПК-3.2.<br>Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. |
| Индикатор | ОПК-3.3.<br>Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. |

**В результате освоения дисциплины (модуля) обучающийся должен**

| | |
|---|---|
| **3.1** | **Знать:** |
| 3.1.1 | правовые основы защиты компьютерной информации, модели и методы криптограффической защиты и криптоанализа; |
| **3.2** | **Уметь:** |
| 3.2.1 | Применять криптографические методы на программном уровне: создание и отладка модулей шифрования/дешифрования, подготовка к передаче и обработка приема специально структурированных данных; |
| **3.3** | **Владеть:** |
| 3.3.1 | базовыми знаниями и приемами вычислений модулярной арифметики, теории чисел для расширенного решения задач криптографической защиты информации. |

| 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Код занятия** | **Наименование разделов и тем /вид занятия/** | **Семестр / Курс** | **Часов** | **Компетен-ции** | **Литература** | **Инте ракт.** | **Примечание** |
| | **Раздел 1. Введение в криптографическую защиту информации** | | | | | | |
| 1.1 | Основные понятия криптографической защиты информации /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1.2 | Система шифрования RSA /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 1.3 | Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 1.4 | Модулярная арифметика и классы вычетов /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 1.5 | Проблемы теории чисел /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| | **Раздел 2. Фундаментальные алгоритмы** | | | | | | |
| 2.1 | Особенности алгоритмов в теории чисел /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 2.2 | Алгоритм деления /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 2.3 | Теорема деления /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 2.4 | Алгоритм Эвклида /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 2.5 | Расширенный алгоритм Эвклида /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 2.6 | Программа алгоритма Эвклида /Лаб/ | 8 | 7 | ОПК-3 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э2 Э3 | 0 | |
| | **Раздел 3. Факторизация чисел** | | | | | | |
| 3.1 | Теорема о разложении. Существование разложения /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 3.2 | Алгоритм Ферма разложения на множители /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 3.3 | Фундаментальное свойство простых чисел /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 3.4 | Единственность разложения /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 3.5 | Числа Кармайкла и тест Миллера /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 3.6 | Метод квадратичного решета /Ср/ | 8 | 2 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 3.7 | Метод Поларда /Ср/ | 8 | 2 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 3.8 | Тест Соловэа-Штрассена /Ср/ | 8 | 2 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 3.9 | Факторизация чисел /Лаб/ | 8 | 7 | ОПК-3 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э2 Э3 | 0 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3.10 | Тесты на простоту /Лаб/ | 8 | 7 | ОПК-3 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э2 Э3 | 0 | |
| | **Раздел 4. Простые числа** | | | | | | |
| 4.1 | Полиномиальная формула /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 4.2 | Экспоненциальные формулы: числа Мерсенна, числа Ферма /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 4.3 | Решето Эратосфена /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 4.4 | Генерация ключей. Шифрование RSA и подготовка данных к приему и передаче /Лаб/ | 8 | 7 | ОПК-3 | Л1.1 Л1.2Л2.1Л3.1 Э1 Э2 Э3 | 0 | |
| | **Раздел 5. Арифметика остатков** | | | | | | |
| 5.1 | Отношение эквивалентности /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.2 | Сравнения /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.3 | Арифметика остатков /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.4 | Критерий делимости /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.5 | Степени /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.6 | Диофантовы уравнения /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.7 | Деление по модулю /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.8 | Теорема Ферма /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.9 | Вычисление корней. Квадратные корни /Лек/ | 8 | 1 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 5.10 | Дискретное логарифмирование /Ср/ | 8 | 2 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| | **Раздел 6. Системы сравнений** | | | | | | |
| 6.1 | Линейные уравнения /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 6.2 | Китайский алгоритм остатков: взаимно простые модули /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 6.3 | Свойства степени. Алгоритм степени /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| | **Раздел 7. Группы** | | | | | | |
| 7.1 | Арифметические группы /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7.2 | Подгруппы /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 7.3 | Циклические подгруппы /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 7.4 | Поиск подгрупп. Теорема Лагранжа /Лек/ | 8 | 0,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| | **Раздел 8. Контроль знаний** | | | | | | |
| 8.1 | Подгоотовка к лабораторным /Ср/ | 8 | 20 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 8.2 | Подготовка к лекциям /Ср/ | 8 | 12,5 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 8.3 | Подготовка к зачету /Ср/ | 8 | 11,25 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |
| 8.4 | Интерактивная беседа /К/ | 8 | 0,25 | ОПК-3 | Л1.1 Л1.2Л2.1 Э1 Э2 Э3 | 0 | |

## 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 5.1. Структура и содержание ФОС

Структура и содержание ФОС привидены в Приложении 1 к РПД
Включает оценочные средства по следующим формам контроля:
Выполнение лабораторных работ
Тестирование
Зачет

### 5.2. Показатели и критерии оценивания компетенций

Критерии формирования оценок по выполнению тестовых заданий
«Отлично» (5 баллов) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 100 – 80% от общего объёма заданных тестовых вопросов.
«Хорошо» (4 балла) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 79 – 60% от общего объёма заданных тестовых вопросов.
«Удовлетворительно» (3 балла) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 59 – 51% от общего объёма заданных тестовых вопросов.
«Неудовлетворительно» (0 баллов) - получают обучающиеся с правильным количеством ответов на тестовые вопросы – 50% и менее от общего объёма заданных тестовых вопросов.

Критерии формирования оценок по зачету
«Зачтено»» - обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности.
«Не зачтено» - выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У экзаменуемого слабо выражена способность к самостоятельному аналитическому мышлению, имеются затруднения в изложении материала, отсутствуют необходимые умения и навыки, допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения положительной оценки.

Критерии формирования оценок по отчетам выполненных лабораторных работ
«Зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов в соответствии с заданием, выданным для выполнения лабораторной работы. Обучающийся полностью владеет информацией по теме работы, решил все поставленные в задании задачи.
«Не зачтено» - ставится за работу, если обучающийся правильно выполнил менее 2/3 всей работы, использовал при выполнении работы неправильные алгоритмы, допустил грубые ошибки при программировании, сформулировал неверные выводы по результатам работы.

Критерии и шкала оценивания уровней освоения компетенций:
Оценка «неудовлетворительно» (не зачтено) или отсутствие сформированности компетенции
Неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были

представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу свидетельствуют об отсутствии сформированной компетенции. Отсутствие подтверждения наличия сформированности компетенции свидетельствует об отрицательных результатах освоения учебной дисциплины. Уровень освоения дисциплины, при котором у обучаемого не сформировано более 50% компетенций. Если же учебная дисциплина выступает в качестве итогового этапа формирования компетенций (чаще всего это дисциплины профессионального цикла) оценка «неудовлетворительно» должна быть выставлена при отсутствии сформированности хотя бы одной компетенции.

Оценка «удовлетворительно» (зачтено) или низкий уровень освоения компетенции
Если обучаемый демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий в полном соответствии с образцом, данным преподавателем, по заданиям, решение которых было показано преподавателем, следует считать, что компетенция сформирована, но ее уровень недостаточно высок. Поскольку выявлено наличие сформированной компетенции, ее следует оценивать положительно, но на низком уровне. При наличии более 50% сформированных компетенций по дисциплинам, имеющим возможность доформирования компетенций на последующих этапах обучения. Для дисциплин итогового формирования компетенций естественно выставлять оценку «удовлетворительно», если сформированы все компетенции и более 60% дисциплин профессионального цикла «удовлетворительно».

Оценка «хорошо» (зачтено) или повышенный уровень освоения компетенции
Способность обучающегося продемонстрировать самостоятельное применение знаний, умений и навыков при решении заданий, аналогичных тем, которые представлял преподаватель при потенциальном формировании компетенции, подтверждает наличие сформированной компетенции, причем на более высоком уровне. Наличие сформированной компетенции на повышенном уровне самостоятельности со стороны обучаемого при ее практической демонстрации в ходе решения аналогичных заданий следует оценивать как положительное и устойчиво закрепленное в практическом навыке. Для определения уровня освоения промежуточной дисциплины на оценку «хорошо» обучающийся должен продемонстрировать наличие 80% сформированных компетенций, из которых не менее 1/3 оценены отметкой «хорошо». Оценивание итоговой дисциплины на «хорошо» обуславливается наличием у обучаемого всех сформированных компетенций причем общепрофессиональных компетенции по учебной дисциплине должны быть сформированы не менее чем на 60% на повышенном уровне, то есть с оценкой «хорошо»

Оценка «отлично» (зачтено) или высокий уровень освоения компетенции
Обучаемый демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин, следует считать компетенцию сформированной на высоком уровне. Присутствие сформированной компетенции на высоком уровне, способность к ее дальнейшему саморазвитию и высокой адаптивности практического применения к изменяющимся условиям профессиональной задачи. Оценка «отлично» по дисциплине с промежуточным освоением компетенций, может быть выставлена при 100% подтверждении наличия компетенций, либо при 90% сформированных компетенций, из которых не менее 2/3 оценены отметкой «хорошо». В случае оценивания уровня освоения дисциплины с итоговым формированием компетенций оценка «отлично» может быть выставлена при подтверждении 100% наличия сформированной компетенции у обучаемого, выполнены требования к получению оценки «хорошо» и освоены на «отлично» не менее 50% общепрофессиональных компетенций.

**5.3. Типовые контрольные задания для оценки знаний, умений, навыков и (или) опыта деятельности**

Вопросы к зачету:

I. Введение в криптографическую защиту информации
1. Основные понятия криптографической защиты информации
2. Система шифрования RSA
3. Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел
4. Модулярная арифметика и классы вычетов
5. Проблемы теории чисел

II. Фундаментальные алгоритмы

6. Особенности алгоритмов в теории чисел
7. Алгоритм деления
8. Теорема деления
9. Алгоритм Эвклида
10. Расширенный алгоритм Эвклида

III. Факторизация чисел

11. Теорема о разложении
12. Существование разложения
13. Алгоритм Ферма разложения на множители
14. Фундаментальное свойство простых чисел

15. Единственность разложения
16. Числа Кармайкла и тест Миллера

IV. Простые числа

17. Полиномиальная формула
18. Экспоненциальные формулы: числа Мерсенна, числа Ферма
19. Решето Эратосфена

V. Арифметика остатков

20. Отношение эквивалентности
21. Сравнения
22. Арифметика остатков
23. Критерий делимости
24. Степени
25. Диофантовы уравнения
26. Деление по модулю
27. Теорема Ферма
28. Вычисление корней. Квадратные корни

VI. Системы сравнений

29. Линейные уравнения
30. Китайский алгоритм остатков: взаимно простые модули
31. Свойства степени. Алгоритм степени

VII. Группы

32. Арифметические группы
33. Подгруппы
34. Циклические подгруппы
35. Поиск подгрупп. Теорема Лагранжа
Примечание: по усмотрению преподавателя, вопросы на зачете могут быть заменены требованием решения практических задач, аналогичных примерам лабораторных работ.

Примерные тесты с ответами:
1. Кто является основным ответственным за определение уровня классификации информации?

A. Руководитель среднего звена
B. Высшее руководство
C. Владелец
D. Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
A. Сотрудники
B. Хакеры
C. Атакующие
D. Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
C. Улучшить контроль за безопасностью этой информации
D. Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
B. Необходимый уровень доступности, целостности и конфиденциальности
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных
B. Пользователи
C. Администраторы
D. Руководство

6. Что такое процедура?

A. Правила использования программного и аппаратного обеспечения в компании
B. Пошаговая инструкция по выполнению задачи
C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

A. Поддержка высшего руководства
B. Эффективные защитные меры и методы их внедрения
C. Актуальные и адекватные политики и процедуры безопасности
D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
B. Когда риски не могут быть приняты во внимание по политическим соображениям
C. Когда необходимые защитные меры слишком сложны
D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности
B. Общие руководящие требования по достижению определенного уровня безопасности
C. Широкие, высокоуровневые заявления руководства
D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

A. Анализ рисков
B. Анализ затрат / выгоды
C. Результаты ALE
D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды
B. Оценить возможные потери для каждой контрмеры
C. Количественно оценить затраты / выгоды
D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

A. Среднесрочное планирование
B. Долгосрочное планирование
C. Ежедневное планирование
D. Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?

A. Нечто, приводящее к ущербу от угрозы
B. Любая потенциальная опасность для информации или систем
C. Любой недостаток или отсутствие информационной безопасности
D. Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов
B. Контрмер и защитных механизмов
C. Физической безопасности и технических средств защиты
D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности
B. Классификацию данных после внедрения механизмов безопасности
C. Уровень доверия, обеспечиваемый механизмом безопасности
D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность
B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

A. Угрозы х Риски х Ценность актива
B. (Угрозы х Ценность актива х Уязвимости) х Риски
C. SLE х Частоту = ALE
D. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий
B. Количественная оценка воздействия потенциальных угроз
C. Выявление рисков
D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка
B. Выполнение анализа рисков
C. Определение цели и границ
D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка
B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Что является наилучшим описанием количественного анализа рисков?

A. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
B. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
C. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
D. Метод, основанный на суждениях и интуиции

22. Почему количественный анализ рисков в чистом виде не достижим?

A. Он достижим и используется
B. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
C. Это связано с точностью количественных элементов
D. Количественные измерения должны применяться к качественным элементам

23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

A. Много информации нужно собрать и ввести в программу
B. Руководство должно собрать и оценить риски

C. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
D. Множество людей должно одобрить данные

24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

A. Стандарты
B. Должный процесс (Due process)
C. Должная забота (Due care)
D. Снижение обязательств

25. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

A. Список стандартов, процедур и политик для разработки программы безопасности
B. Текущая версия ISO 17799
C. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
D. Открытый стандарт, определяющий цели контроля
26. Из каких четырех доменов состоит CobiT?

A. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
B. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
C. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
D. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

27. Что представляет собой стандарт ISO/IEC 27799?

A. Стандарт по защите персональных данных о здоровье
B. Новая версия BS 17799
C. Определения для новой серии ISO 27000
D. Новая версия NIST 800-60

28. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

A. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
B. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
C. COSO учитывает корпоративную культуру и разработку политик
D. COSO – это система отказоустойчивости

29. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

A. NIST и OCTAVE являются корпоративными
B. NIST и OCTAVE ориентирован на ИТ
C. AS/NZS ориентирован на ИТ
D. NIST и AS/NZS являются корпоративными

30. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

A. Анализ связующего дерева
B. AS/NZS
C. NIST
D. Анализ сбоев и дефектов

31. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

A. Безопасная OECD
B. ISO\IEC
C. OECD
D. CPTED

32. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. [illegible]

5. аналитических преобразований.

33. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
1. Гаммирования
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

34. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

35. Защита информации от утечки это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
5. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

36. Защита информации это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

37. Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

38 Икусственные угрозы безопасности информации вызваны:

1. деятельностью человека;
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
4. корыстными устремлениями злоумышленников;
5. ошибками при действиях персонала.

39 К основным непреднамеренным искусственным угрозам АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.;
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

40. К посторонним лицам нарушителям информационной безопасности относится:

1. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
2. персонал, обслуживающий технические средства;
3. технический персонал, обслуживающий здание;
4. пользователи;
5. сотрудники службы безопасности.
6. представители конкурирующих организаций.
7. лица, нарушившие пропускной режим;

41. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

42. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

43. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

44. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

45. Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

46. Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

47. Активный перехват информации это перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

48. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

49. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

50. Перехват, который осуществляется путем использования оптической техники называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

Ответы:

1)C

2)A

3)C

4)B

5)D

6)B

7)A

8)D

9)C

10)B

11)D

12)A

13)A

14)A

16)C

17)D

18)A

19)B

20)C

21)C

22)D

23)A

24)C

25)D

2-ВАРИАНТ

26)A

27)A

28)B

29)B

30)D

31)C

32)4

33)1

34)1

35)4

36)5

37)3

38)1

39)5

40)6

41)1

42)2

43)1

44)2

45)4

46)5

48)3

49)2

50)4

**5.4. Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности**

Описание процедуры оценивания «Тестирование»
Тестирование по дисциплине проводится с использованием ресурсов электронной образовательной среды – ЭОС (доступ: http://samgups.org.ru). Количество тестовых заданий и время задается системой. Во время проведения тестирования обучающиеся могут пользоваться программой дисциплины, справочной литературой, калькулятором. Результат каждого обучающегося оценивается в соответствии с универсальной шкалой, приведенной в пункте 2.

Описание процедуры оценивания «Зачет»
При проведении зачета в форме устного ответа на 2 вопроса, выбранных преподавателем из перечня вопросов, обучающемуся предоставляется 20 минут на подготовку. Опрос обучающегося не должен превышать 0,25 часа. Ответ обучающегося оценивается в соответствии с критериями, описанными в пункте 2.
При проведении зачета в форме тестирования в ЭОС (доступ: http://samgups.org.ru) количество тестовых заданий и время задается системой. Во время проведения зачета обучающиеся могут пользоваться программой дисциплины, справочной литературой, калькулятором. Результат каждого обучающегося оценивается в соответствии с универсальной шкалой, приведенной в пункте 2.

Описание процедуры оценивания «Результат выполнения лабораторной работы»
Оценивание итогов лабораторной работы проводится преподавателем, ведущим лабораторные работы.
По результатам проверки лабораторной работы обучающийся допускается к оценке работы при условии соблюдения перечисленных условий:
– выполнены все задания;
– отсутствуют ошибки;
– оформлено в соответствии с требованиями.
В том случае, если содержание выполненной работы не отвечает предъявляемым требованиям, то он возвращается автору на доработку. Обучающийся должен переделать отчет с учетом замечаний. Если сомнения вызывают отдельные аспекты отчета, то в этом случае они рассматриваются во время устной защиты.
Отчет по лабораторной работе представляет собой устный публичный отчет обучающегося о результатах выполнения, ответы на вопросы преподавателя.
Ответ обучающегося оценивается преподавателем в соответствии с критериями, описанными в пункте 5.2.

**6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**6.1. Рекомендуемая литература**

**6.1.1. Основная литература**

| | Авторы, составители | Заглавие | Кол-во | Издательство, год |
|---|---|---|---|---|
| Л1.1 | Корниенко А. А. | Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте: учебник для вузов | 45 | Москва: УМЦ по образованию на железнодорожном транспорте, 2014 |
| Л1.2 | Корниенко А. А. | Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте: учебник для вузов | 45 | Москва: УМЦ по образованию на железнодорожном транспорте, 2014 |

**6.1.2. Дополнительная литература**

| | Авторы, составители | Заглавие | Кол-во | Издательство, год |
|---|---|---|---|---|
| Л2.1 | Бурова М. А., Овсянников А. С. | Информационная безопасность и защита информации: конспект лекций | 1 Электронное издание | Самара: СамГУПС, 2012 |

**6.1.3. Методические разработки**

| | Авторы, составители | Заглавие | Кол-во | Издательство, год |
|---|---|---|---|---|
| Л3.1 | Тюмиков Д. К. | Защита информации в WINDOWS: метод. указ. к вып. лаб. работ по дисц. Защита информации для обуч. по напр. подгот. 09.03.01 ИВТ очн. формы обуч. | 20 | Самара: СамГУПС, 2015 |

**6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"**

| | |
|---|---|
| Э1 | http://www.exponenta.ru/ |
| Э2 | http://matlab.ru/products/matlab |
| Э3 | http://www.scilab.org |
| **6.3.1 Перечень программного обеспечения** | |
| 6.3.1.1 | Лицензионное ПО: Windows XP |
| 6.3.1.2 | C++ CodeBlock |
| **6.3.2 Перечень информационных справочных систем** | |
| 6.3.2.1 | Дистанционные образовательные ресурсы СамГУПС http://samgups.org.ru |
| 6.3.2.2 | Рекомендуемые поисковые системы http://www.yandex.ru/, http://www.google.ru/, http://www.google.com/ |

| **7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** | |
|---|---|
| 7.1 | Лекционная аудитория (20 и более посадочных мест) и аудитория для проведения лабораторных занятий (25 и более посадочных мест) оборудованные учебной мебелью; неограниченный доступ к электронно-библиотечным системам (через ресурсы библиотеки СамГУПС), к электронной информационно-образовательной среде moodle и к информационно-телекоммуникационной сети «Интернет» в рамках самостоятельной работы обучающегося. |
| 7.2 | Для проведения лабораторных работ по дисциплине «Защита информации» необходимо: мультимедийное оборудование (проектор, экран, ноутбук или компьютер). |

**8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Для освоения дисциплины «Защита информации» обучающемуся необходимо: выполнять лабораторные задания; успешно пройти все формы текущего контроля; успешно пройти промежуточную аттестацию (вопросы прилагаются п.6.4).
Для теоретического и практического усвоения дисциплины большое значение имеет самостоятельная работа обучающихся, которая может осуществляться как индивидуально, так и под руководством. Данная работа предполагает самостоятельное изучение обучающимся отдельных тем, дополнительную подготовку к каждому лабораторному занятию.
Самостоятельная работа обучающихся является важной формой образовательного процесса. Она реализуется вне рамок расписания, а также в библиотеке, дома, при выполнении учебных задач.
Цель самостоятельной работы - научить обучающегося осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы повысить уровень освоения компетенций, а также привить умение в дальнейшем непрерывно повышать свою квалификацию