

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гнатюк Максим Александрович
Должность: Первый проректор
Дата подписания: 11.07.2022 09:51:21
Уникальный программный ключ:
8873f497f100e798ae8c92c0d38e105c818d5410

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение высшего образования
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

Защита информации

рабочая программа дисциплины (модуля)

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Проектирование АСОИУ на транспорте

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Виды контроля в семестрах:

зачеты 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	8 (4.2)		Итого	
	Неделя			
Неделя	7,7			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Лабораторные	28	28	28	28
Конт. ч. на аттест.	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

Программу составил(и):

к.т.н., доцент, Гуцин А.В.

Рабочая программа дисциплины

Защита информации

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 929)

составлена на основании учебного плана: 09.03.01-20-12-ИВТб изм1.plm.plx

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Проектирование АСОИУ на транспорте

Рабочая программа одобрена на заседании кафедры

Мехатроника, автоматизация и управление на транспорте

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.23
-------------------	---------

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;

ОПК-3.2 Применяет методы защиты информации при выполнении задач профессиональной деятельности

В результате освоения дисциплины (модуля) обучающийся должен

3.1 Знать:	
3.1.1	основы теории чисел
3.2 Уметь:	
3.2.1	производить вычисления с большими числами
3.3 Владеть:	
3.3.1	методами модальной арифметики

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Примечание
	Раздел 1. Введение в криптографическую защиту информации			
1.1	Основные понятия криптографической защиты информации /Лек/	8	0,5	
1.2	Система шифрования RSA /Лек/	8	1	
1.3	Алгоритм RSA /Лаб/	8	3	
1.4	Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел /Лек/	8	0,5	
1.5	Модулярная арифметика и классы вычетов /Лек/	8	1	
1.6	Классы вычетов. Поля вычетов /Лаб/	8	3	
1.7	Проблемы теории чисел /Лек/	8	0,5	
1.8	НОД. Алгоритм Эвклида /Лаб/	8	3	
	Раздел 2. Фундаментальные алгоритмы			
2.1	Особенности алгоритмов в теории чисел /Лек/	8	0,5	
2.2	Алгоритм деления /Лек/	8	1	
2.3	Расширенный алгоритм Эвклида /Лаб/	8	3	
2.4	Теорема деления /Лек/	8	1	
2.5	Алгоритм Эвклида /Лек/	8	1	
2.6	Разложение на множители /Лаб/	8	3	
2.7	Расширенный алгоритм Эвклида /Лек/	8	1	
2.8	Алгоритм Ферма разложения на множители /Лаб/	8	3	
	Раздел 3. Факторизация чисел			
3.1	Теорема о разложении. Существование разложения /Лек/	8	1	

3.2	Алгоритм Ферма разложения на множители /Лек/	8	1	
3.3	Алгоритм вероятностного теста Миллера на простоту /Лаб/	8	3	
3.4	Фундаментальное свойство простых чисел /Лек/	8	1	
3.5	Единственность разложения /Лек/	8	0,5	
3.6	Факторизация составных чисел. /Лаб/	8	3	
3.7	Числа Кармайкла и тест Миллера /Лек/	8	1	
3.8	Метод квадратичного решета /Ср/	8	2	
3.9	Метод Поларда /Ср/	8	2	
3.10	Тест Соловза-Штрассена /Ср/	8	2	
	Раздел 4. Простые числа			
4.1	Полиномиальная формула /Лек/	8	1	
4.2	Экспоненциальные формулы: числа Мерсенна, числа Ферма /Лек/	8	1	
4.3	Решето Эратосфена /Лек/	8	1	
	Раздел 5. Арифметика остатков			
5.1	Отношение эквивалентности /Лек/	8	1	
5.2	Сравнения /Лек/	8	1	
5.3	Арифметика остатков /Лек/	8	1	
5.4	Критерий делимости /Лек/	8	1	
5.5	Степени /Лек/	8	1	
5.6	Диофантовы уравнения /Лек/	8	1	
5.7	Деление по модулю /Лек/	8	1	
5.8	Разработка ключей шифрования и передача символьной информации /Лаб/	8	4	
5.9	Теорема Ферма /Лек/	8	1	
5.10	Вычисление корней. Квадратные корни /Лек/	8	1	
5.11	Дискретное логарифмирование /Ср/	8	2	
	Раздел 6. Системы сравнений			
6.1	Линейные уравнения /Лек/	8	0,5	
6.2	Китайский алгоритм остатков: взаимно простые модули /Лек/	8	0,5	
6.3	Свойства степени. Алгоритм степени /Лек/	8	0,5	
	Раздел 7. Группы			
7.1	Арифметические группы /Лек/	8	0,5	
7.2	Подгруппы /Лек/	8	0,5	
7.3	Циклические подгруппы /Лек/	8	0,5	
7.4	Поиск подгруп. Теорема Лагранжа /Лек/	8	0,5	
	Раздел 8. Контроль знаний			

8.1	Подготовка к лабораторным /Ср/	8	28	
8.2	Подготовка к лекциям /Ср/	8	7	
8.3	Подготовка к зачету /Ср/	8	8,75	
8.4	Зачет /КА/	8	0,25	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Оценочные материалы для проведения промежуточной аттестации обучающихся приведены в приложении к рабочей программе дисциплины.

Формы и виды текущего контроля по дисциплине (модулю), виды заданий, критерии их оценивания, распределение баллов по видам текущего контроля разрабатываются преподавателем дисциплины с учетом ее специфики и доводятся до сведения обучающихся на первом учебном занятии.

Текущий контроль успеваемости осуществляется преподавателем дисциплины (модуля), как правило, с использованием ЭИОС или путем проверки письменных работ, предусмотренных рабочими программами дисциплин в рамках контактной работы и самостоятельной работы обучающихся. Для фиксирования результатов текущего контроля может использоваться ЭИОС.

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л1.1	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: учебник для вузов	Москва: Юрайт, 2021	https://urait.ru/bcode/469866

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Внуков А. А.	Защита информации: учебное пособие для вузов	Москва: Юрайт, 2021	https://urait.ru/bcode/470131

6.2 Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине (модулю)

6.2.1 Перечень лицензионного и свободно распространяемого программного обеспечения

6.2.1.1	Операционная система Microsoft Windows10 Pro Договор №034210000481700004 Номер лицензии 68383602 (не ограничено)
6.2.1.2	Code::Blocks (Свободно распространяемое ПО) https://ru.wikipedia.org/wiki/Code_Blocks

6.2.2 Перечень профессиональных баз данных и информационных справочных систем

6.2.2.1	База книг и публикаций Электронной библиотеки "Наука и Техника" - http://www.n-t.ru
6.2.2.2	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- https://github.com/
6.2.2.3	Портал для разработчиков электронной техники: http://www.espec.ws/
6.2.2.4	База данных «Библиотека программиста» https://proglib.io/
6.2.2.5	Консультант плюс
6.2.2.6	Информационная система ГАРАНТ

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Учебные аудитории для проведения занятий лекционного типа, укомплектованные специализированной мебелью и техническими средствами обучения: мультимедийное оборудование для предоставления учебной информации большой аудитории и/или звукоусиливающее оборудование (стационарное или переносное).
7.2	Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения: мультимедийное оборудование и/или звукоусиливающее оборудование (стационарное или переносное)

7.3	Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.
7.4	Помещения для хранения и профилактического обслуживания учебного оборудования
7.5	Учебные аудитории для проведения лабораторных работ укомплектованы специализированной мебелью и техническими средствами обучения: ноутбуки или компьютеры, подключенные к локальной сети СамГУПС.