

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Гаранин Максим Александрович  
Должность: Ректор  
Дата подписания: 06.05.2024 15:16:51  
Уникальный программный ключ:  
7708e3a47e66a8ee02711b298d7c78bd1e40bf88

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	
	8			
Неделя	8			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	32	32	32	32
Конт. ч. на аттест. в период ЭС	0,25	0,25	0,25	0,25
Итого ауд.	64	64	64	64
Контактная работа	64,25	64,25	64,25	64,25
Сам. работа	35	35	35	35
Часы на контроль	8,75	8,75	8,75	8,75
Итого	108	108	108	108

Программу составил(и):

*к.т.н., доцент, Припутников А.П.*

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: 09.03.01-24-1-ИВТб.plm.plx

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Проектирование АСОИУ на транспорте

Рабочая программа одобрена на заседании кафедры

**Цифровые технологии**

Зав. кафедрой к.э.н., доцент Ефимова Т.Б.

**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
- УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности
- УК-10.1 Раскрывает механизм проявления коррупционного поведения и определяет способы противодействия ему в профессиональной деятельности
- УК-10.2 Обосновывает правовыми средствами свою гражданскую позицию в отношении терроризма и экстремизма и применяет способы противодействия им в профессиональной сфере

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

**3.1 Знать:**

- |       |   |
|-------|---|
| 3.1.1 | - основы теории чисел;  |
| 3.1.2 | - правовые основы защиты компьютерной информации, модели и методы криптографической защиты и криптоанализа; |

**3.2 Уметь:**

- |       |   |
|-------|---|
| 3.2.1 | - производить вычисления с большими числами;  |
| 3.2.2 | - 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 | - методами модальной арифметики;  |
| 3.3.2 | - 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	Примечание
	<b>Раздел 1. Введение в криптографическую защиту информации</b>			
1.1	Основные понятия криптографической защиты, Система шифрования RSA информации /Лек/	8	4	
1.2	Криптография с открытым ключом /Лаб/	8	4	
1.3	Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел, Модулярная арифметика и классы вычетов. Проблемы теории чисел /Лек/	8	4	
	<b>Раздел 2. Фундаментальные алгоритмы</b>			
2.1	Особенности алгоритмов в теории чисел. Алгоритм деления. Теорема деления. Алгоритм Эвклида. /Лек/	8	4	
2.2	Факторизация (p-1) – метод Полларда /Лаб/	8	4	
2.3	Расширенный алгоритм Эвклида /Лек/	8	4	
2.4	Вычисление символа Якоби /Лаб/	8	4	
	<b>Раздел 3. Факторизация чисел</b>			
3.1	Теорема о разложении. Существование разложения. Алгоритм Ферма разложения на множители /Лек/	8	2	
3.2	Алгоритм Ферма разложения на множители /Лек/	8	2	

3.3	Фундаментальное свойство простых чисел. Единственность разложения. Числа Кармайкла и тест Миллера /Лек/	8	2	
3.4	Тест Миллера-Рабина /Лаб/	8	4	
3.5	Тест Соловья-Штрассена /Лаб/	8	4	
<b>Раздел 4. Простые числа</b>				
4.1	Полиномиальная формула /Лек/	8	2	
4.2	Экспоненциальные формулы: числа Мерсенна, числа Ферма. Решето Эратосфена /Лек/	8	2	
4.3	Метод квадратичного решета /Лаб/	8	6	
<b>Раздел 5. Арифметика остатков</b>				
5.1	Отношение эквивалентности. Сравнения. Арифметика остатков /Лек/	8	1	
5.2	Критерий делимости. Степени. Диофантовы уравнения /Лек/	8	2	
5.3	Деление по модулю. Теорема Ферма. Вычисление корней. Квадратные корни. /Лаб/	8	2	
<b>Раздел 6. Системы сравнений</b>				
6.1	Линейные уравнения. Китайский алгоритм остатков: взаимно простые модули /Лек/	8	2	
6.2	Свойства степени. Алгоритм степени /Лек/	8	1	
<b>Раздел 7. Группы</b>				
7.1	Арифметические группы, подгруппы /Лаб/	8	2	
7.2	Циклические подгруппы, Поиск подгрупп. Теорема Лагранжа /Лаб/	8	2	
<b>Раздел 8. Самостоятельная работа</b>				
8.1	Подготовка к лабораторным /Ср/	8	19	
8.2	Подготовка к лекциям /Ср/	8	16	
<b>Раздел 9. Контактные часы</b>				
9.1	Зачет /КЭ/	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	<a href="https://urait.ru/bcode/469866">https://urait.ru/bcode/469866</a>

<b>6.1.2. Дополнительная литература</b>				
	Авторы, составители	Заглавие	Издательс тво, год	Эл. адрес
Л2.1	Внуков А. А.	Защита информации: учебное пособие для вузов	Москва: Юрайт, 2021	<a href="https://urait.ru/bcode/470131">https://urait.ru/bcode/470131</a>
<b>6.2 Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине (модулю)</b>				
<b>6.2.1 Перечень лицензионного и свободно распространяемого программного обеспечения</b>				
6.2.1.1	Операционная система Microsoft Windows10 Pro Договор №034210000481700004 Номер лицензии 68383602 (не ограничено)			
6.2.1.2	C++ CodeBlock - свободная лицензия, срок не ограничен			
<b>6.2.2 Перечень профессиональных баз данных и информационных справочных систем</b>				
6.2.2.1	База книг и публикаций Электронной библиотеки "Наука и Техника" - <a href="http://www.n-t.ru">http://www.n-t.ru</a>			
6.2.2.2	База данных «Библиотека программиста» <a href="https://proglib.io/">https://proglib.io/</a>			
<b>7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>				
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			