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	
Недель	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, Гущин 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: 09.03.01-23-4-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.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.22

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
3.2	**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	2	
1.2	Система шифрования RSA /Лек/	8	2	
1.3	Алгоритм RSA /Лаб/	8	3	
1.4	Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел /Лек/	8	2	
1.5	Модулярная арифметика и классы вычетов /Лек/	8	1	
1.6	Классы вычетов. Поля вычетов /Лаб/	8	3	
1.7	НОД. Алгоритм Эвклида /Лаб/	8	3	
	Раздел 2. Фундаментальные алгоритмы			
2.1	Алгоритм деления /Лек/	8	2	
2.2	Расширенный алгоритм Эвклида /Лаб/	8	4	
2.3	Теорема деления /Лек/	8	1	
2.4	Алгоритм Эвклида /Лек/	8	1	
2.5	Разложение на множители /Лаб/	8	4	
2.6	Расширенный алгоритм Эвклида /Лек/	8	1	
2.7	Алгоритм Ферма разложения на множители /Лаб/	8	4	

	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	4	
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 Соловэа-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 подгрупп. Теорема Лагранжа /Лек/	8	0,5	
	Раздел 8. Самостоятельная работа			
8.1	Подгоотовка к лабораторным /Ср/	8	16	
8.2	Подготовка к лекциям /Ср/	8	11	
	Раздел 9. Контактная работа			
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: чебник для вузов	Москва: Юрайт, 2021	tps://urait.ru/bcode/46986

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	tps://urait.ru/bcode/47013

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	CodeBlock C++ Свободная лицензия (не ограничено)

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/

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