

Документ подписан простой электронной подписью

Информация о владельце: **МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**

ФИО: Гаранин Максим Александрович **ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Должность: Ректор

Дата подписания: 28.08.2023 17:35:47 Федеральное государственное бюджетное образовательное учреждение высшего образования

Уникальный программный ключ:

7708e3a47e66a8ee02711b298d7c78bd1e40bf88 **САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ**

Информационная безопасность

рабочая программа дисциплины (модуля)

Направление подготовки 09.03.03 Прикладная информатика

Направленность (профиль) Управление цифровой инфраструктурой организации

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Виды контроля в семестрах:

экзамены 7

курсовые работы 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		Итого	
	УП	РП	УП	РП
Неделя	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	20	20	20	20
Лабораторные	30	30	30	30
Конт. ч. на аттест.	1,5	1,5	1,5	1,5
Конт. ч. на аттест. в период ЭС	2,35	2,35	2,35	2,35
Итого ауд.	50	50	50	50
Контактная работа	53,85	53,85	53,85	53,85
Сам. работа	137,5	137,5	137,5	137,5
Часы на контроль	24,65	24,65	24,65	24,65
Итого	216	216	216	216

Программу составил(и):

к.т.н., доцент, Гуцин А.В.

Рабочая программа дисциплины

Информационная безопасность

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана: 09.03.03-23-2-ПИБ.plm.plx

Направление подготовки 09.03.03 Прикладная информатика Направленность (профиль) Управление цифровой инфраструктурой организации

Рабочая программа одобрена на заседании кафедры

Цифровые технологии

Зав. кафедрой к.п.н., доцент Горбатов С.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.19
-------------------	---------

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-3.1	Решает стандартные задачи профессиональной деятельности на основе информационной 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
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;
ОПК-4.1	Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
ОПК-4.2	Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам

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/	7	1	
1.2	Система шифрования RSA /Лек/	7	1	
1.3	Алгоритм RSA /Лаб/	7	3	
1.4	Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел /Ср/	7	4	
1.5	Классы вычетов. Поля вычетов /Лаб/	7	3	
1.6	Проблемы теории чисел /Ср/	7	4	
1.7	НОД. Алгоритм Эвклида /Лаб/	7	3	
	Раздел 2. Фундаментальные алгоритмы			
2.1	Особенности алгоритмов в теории чисел. Алгоритм деления /Лек/	7	1	
2.2	Расширенный алгоритм Эвклида /Лаб/	7	3	
2.3	Теорема деления /Ср/	7	6	
2.4	Алгоритм Эвклида. Расширенный алгоритм Эвклида /Лек/	7	1	
2.5	Разложение на множители /Лаб/	7	3	
2.6	Алгоритм Ферма разложения на множители /Лаб/	7	3	

	Раздел 3. Факторизация чисел			
3.1	Теорема о разложении. Существование разложения /Лек/	7	1	
3.2	Модулярная арифметика и классы вычетов /Лек/	7	1	
3.3	Алгоритм Ферма разложения на множители /Лек/	7	1	
3.4	Алгоритм вероятностного теста Миллера на простоту /Лаб/	7	4	
3.5	Фундаментальное свойство простых чисел. Единственность разложения /Лек/	7	1	
3.6	Факторизация составных чисел. /Лаб/	7	4	
3.7	Числа Кармайкла и тест Миллера /Лек/	7	1	
3.8	Метод квадратичного решета /Ср/	7	6,5	
3.9	Метод Поларда /Ср/	7	6	
3.10	Тест Соловза-Штрассена /Ср/	7	6	
	Раздел 4. Простые числа			
4.1	Полиномиальная формула. Экспоненциальные формулы: числа Мерсенна, числа Ферма /Лек/	7	1	
4.2	Решето Эратосфена /Ср/	7	6	
	Раздел 5. Арифметика остатков			
5.1	Отношение эквивалентности. /Лек/	7	1	
5.2	Сравнения /Ср/	7	6	
5.3	Арифметика остатков /Лек/	7	1	
5.4	Критерий делимости /Лек/	7	1	
5.5	Степени /Лек/	7	1	
5.6	Диофантовы уравнения /Лек/	7	1	
5.7	Деление по модулю /Лек/	7	1	
5.8	Разработка ключей шифрования и передача символьной информации /Лаб/	7	4	
5.9	Теорема Ферма /Лек/	7	1	
5.10	Вычисление корней. Квадратные корни /Лек/	7	1	
5.11	Дискретное логарифмирование /Ср/	7	6,5	
	Раздел 6. Системы сравнений			
6.1	Линейные уравнения. Китайский алгоритм остатков: взаимно простые модули /Лек/	7	1	
6.2	Свойства степени. Алгоритм степени /Ср/	7	6	
	Раздел 7. Группы			
7.1	Арифметические группы. Подгруппы. Циклические подгруппы /Лек/	7	1	
7.2	Поиск подгрупп. Теорема Лагранжа /Ср/	7	6	
	Раздел 8. Контроль знаний			
8.1	Подготовка к лабораторным /Ср/	7	30	
8.2	Подготовка к лекциям /Ср/	7	10	

8.3	Подготовка к курсовой работе /Ср/	7	34,5	
8.4	Экзамен /КЭ/	7	2,35	Интерактивная беседа
8.5	Курсовая работа /КА/	7	1,5	

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	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
-----	---