

Документ подписан простой электронной подписью
Информация о владельце: **МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**
ФИО: Маланичева Наталья Николаевна
Должность: директор филиала
Дата подписания: 11.05.2024 13:50:52
Уникальный программный ключ:
94732c3d953a82d495dcc3155d5c573883fedd18

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение высшего образования
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		
Неделя	16,7			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	48	48	48	48
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.	64	64	64	64
Контактная работа	67,85	67,85	67,85	67,85
Сам. работа	123,5	123,5	123,5	123,5
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: 09.03.03-24-1-ПИБ-ННлиценз.plm.plx

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

Рабочая программа одобрена на заседании кафедры «Общеобразовательные и профессиональные дисциплины»

И.о. зав. кафедрой к. соц. н., доцент Чистяков В. А.

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.20

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	принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, основные стандарты оформления технической документации на различных стадиях жизненного цикла
3.2 Уметь:	
3.2.1	решать стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; применять стандарты оформления технической документации на различных стадиях жизненного цикла
3.3 Владеть:	
3.3.1	методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации; навыками составления технической документации

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	0,5	
1.2	Система шифрования RSA /Лек/	7	1	
1.3	Алгоритм RSA /Лаб/	7	6	
1.4	Основы теории чисел. Теоремы Ферма, Эйлера и Гаусса в теории чисел /Ср/	7	4	
1.5	Классы вычетов. Поля вычетов /Лаб/	7	6	
1.6	Проблемы теории чисел /Ср/	7	2	
1.7	НОД. Алгоритм Эвклида /Лаб/	7	4	
	Раздел 2. Фундаментальные алгоритмы			
2.1	Особенности алгоритмов в теории чисел.Алгоритм деления /Лек/	7	1	
2.2	Расширенный алгоритм Эвклида /Лаб/	7	4	
2.3	Теорема деления /Ср/	7	6	

2.4	Алгоритм Эвклида.Расширенный алгоритм Эвклида /Лек/	7	1	
2.5	Разложение на множители /Лаб/	7	4	
2.6	Алгоритм Ферма разложения на множители /Лаб/	7	4	
	Раздел 3. Факторизация чисел			
3.1	Теорема о разложении. Существование разложения /Лек/	7	0,5	
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	6	
3.5	Фундаментальное свойство простых чисел. Единственность разложения /Лек/	7	0,5	
3.6	Факторизация составных чисел. /Лаб/	7	6	
3.7	Числа Кармайкла и тест Миллера /Лек/	7	0,5	
3.8	Метод квадратичного решета /Ср/	7	4	
3.9	Метод Поларда /Ср/	7	4	
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	4	
	Раздел 5. Арифметика остатков			
5.1	Отношение эквивалентности. /Лек/	7	0,5	
5.2	Сравнения /Ср/	7	6	
5.3	Арифметика остатков /Лек/	7	0,5	
5.4	Критерий делимости /Лек/	7	1	
5.5	Степени /Лек/	7	0,5	
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	8	
5.9	Теорема Ферма /Лек/	7	1	
5.10	Вычисление корней. Квадратные корни /Лек/	7	0,5	
5.11	Дискретное логарифмирование /Ср/	7	4,5	
	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	5	
	Раздел 7. Группы			
7.1	Арифметические группы. Подгруппы. Циклические подгруппы /Лек/	7	1	
7.2	Поиск подгруп. Теорема Лагранжа /Ср/	7	3,5	

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	Казарин О. В., Забабурин А. С.	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов	Москва: Юрайт, 2023	https://urait.ru/bcode/513300
Л1.2	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: учебник для вузов	Москва: Юрайт, 2021	https://urait.ru/bcode/469866
Л1.3	Мойзес О. Е., Кузьменко Е. А.	Информатика. Углубленный курс: учебное пособие для вузов	Москва: Юрайт, 2022	https://urait.ru/bcode/490342

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

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.2	Гущин А. В.	Защита информации: метод. указ. к вып. лаб. работ для обуч. по напр. подгот. 09.03.01 Информатика и выч. техника очн. формы обуч.	Самара: СамГУПС, 2020	https://you.samgups.ru/irbis
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	Установлено программное обеспечение:			
6.2.1.2	Операционная система Ubuntu (свободно распространяемое ПО)			
6.2.1.3	Code::Blocks (свободно распространяемое ПО)			
6.2.2 Перечень профессиональных баз данных и информационных справочных систем				
6.2.2.1	ЭБС ЮРАЙТ https://urait.ru/			
6.2.2.2	Электронная библиотека Учебно-методического центра по образованию на железнодорожном транспорте (ЭБ УМЦ ЖДТ) https://umczdt.ru/			
6.2.2.3	ЭБС BOOK.RU https://book.ru/			
6.2.2.4	ЭОИС "Moodle" http://moodle.nnsamgups.ru/moodle/			
6.2.2.5	База книг и публикаций Электронной библиотеки "Наука и Техника"- http://www.n-t.ru			
6.2.2.6	Портал для разработчиков электронной техники: http://www.espec.ws/			
6.2.2.7	База данных «Библиотека программиста» https://proglib.io/			
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
7.1	Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата: лекций - аудитория № 401			
7.2	Оборудование: Специализированная мебель: столы ученические - 29 шт., стулья ученические – 57 шт., доска настенная – 1 шт., стол преподавателя – 1 шт., стул преподавателя – 1 шт.			
7.3	Технические средства обучения: (переносной экран, переносной проектор, ноутбук)			
7.4	Учебная аудитория для проведения учебных занятий, предусмотренных программой бакалавриата: лабораторных работ - лаборатория Компьютерный класс №3 (аудитория № 412)			
7.5	Оборудование: Специализированная мебель: столы ученические – 25 шт., стулья ученические – 37 шт., доска настенная – 1 шт., стол преподавателя – 1 шт., стул преподавателя – 1 шт.			
7.6	Технические средства обучения: компьютеры – 16 шт., видеопанель – 1шт., компьютер преподавателя 1 шт.			
7.7	Лаборатории, оснащенные специальным лабораторным оборудованием: компьютерной техникой с установленным ПО: Операционная система Ubuntu (свободно распространяемое ПО), Code::Blocks (свободно распространяемое ПО)			
7.8	Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.			