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)[1]

Закреплена за кафедрой	**Логистика и транспортные технологии**
Учебный план	27.03.05-24-1-ИУб-ОрИПС.plm.plx Направление подготовки: 27.03.05 Инноватика Направленность (профиль): Управление инновациями на транспорте
Квалификация	**бакалавр**
Форма обучения	**очная**
Общая трудоемкость	**6 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	48	48	48	48
Конт. ч. на аттест.	1	1	1	1
Конт. ч. на аттест. в период ЭС	2,3	2,3	2,3	2,3
Итого ауд.	64	64	64	64
Контактная работа	67,3	67,3	67,3	67,3
Сам. работа	124	124	124	124
Часы на контроль	24,7	24,7	24,7	24,7
Итого	216	216	216	216

Оренбург

[1] Рабочая программа подлежит ежегодной актуализации в составе основной профессиональной образовательной программы (ОПОП).
Сведения об актуализации ОПОП вносятся в лист актуализации ОПОП.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Формирование компетенций для осуществления задач профессиональной деятельности в областитеории защиты компьютерной информации, а так же практических умений и навыков в использовании основных принципов, методов и алгоритмов обеспечения информационной безопасности информационно-телекоммуникационных систем.
1.2	Задачами дисциплины являются: –раскрыть основные принципы обеспечения информационной безопасности информационно-телекоммуникационныхсистем; –сформировать компетентности в области информационной безопасности; –обучить студентов проектировать и разрабатывать программное обеспечение, обеспечивающее информационную безопасность существующих систем; –ознакомить с современными тенденциями в области защиты информации (в том числе и криптографией).

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О.24

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ОПК-3 Способен использовать фундаментальные знания для решения базовых задач управления в технических системах с целью совершенствования в профессиональной деятельности
ОПК-3.3 Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-5 Способен решать задачи в области инновационных процессов в науке, технике и технологии с учетом нормативно-правового регулирования в сфере интеллектуальной собственности
ОПК-5.1 Оформлеет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр /	Часов	Примечание
	Раздел 1. Основные понятия информационной безопасности			
1.1	Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Модели безопасности. Понятие «национальная безопасность». Доктрина безопасности Российской Федерации Понятия информации. Классификация информации по категории доступа. Виды информации. Понятие ценности информации. Перечень сведений, доступ к которым не может быть ограничен. Понятие конфиденциальной информации, ее виды/Лек/Ср	7	2/7	
1.2	Концепция информационной безопасности. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры по защите информации. Ср	7	7	
	Раздел 2. Правовые основы информационной безопасности и защита интеллектуальной собственности	7		
2.1	Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание. Лек/Ср	7	2/7	
2.2	История создания правового института по охране авторского права. Субъекты авторского права. Права обладателей авторских прав. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность. Ср	7	7	

2.3	Всемирная конвенция об авторском праве. Основные институты и понятия международного авторского права. Произведения, пользующиеся охраной. Правовые нормы и стандарты по лицензированию и сертификации Ср	7	7	
	Раздел 3. Виды информационных угроз	7		
3.1	Факторы, риски угроз информационным ресурсам. Виды угроз и типы атак. Информационные войны. Информационное оружие. Анализ и оценивание угроз информационной безопасности личности в современном информационном обществе Лек/Ср	7	2/7	
3.2	Классификация компьютерных преступлений. Группы компьютерных преступлений. Хакерство в мире и в России. Закрытие информации как средство ее защиты от несанкционированного доступа Лек/ Ср	7	2/7	
3.3	Угрозы информационно-психологической безопасности личности и их основные источники. Сущность и современное состояние манипуляции сознанием и поведением людей. Информационная среда иллюзии и реальности Ср	7	7	
	Раздел 4Программные средства защиты персональной информации	7		
4.1	Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов и КПК Лек/Ср	7	2/7	
4.2	Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Л/СР	7	2/7	
4.3	Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. Кодирование информации. Электронная цифровая подпись Ср	7	7	
4.4	Анализ уязвимостей компьютерной системы с использованием программных средств Лаб	7	2	
4.5	Исследование и настройка межсетевого экрана Лаб	7	2	
4.6	Резервное копирование программ, системных параметров и файлов Лаб	7	2	
4.7	Использование методов замены для шифрования данных Лаб	7	4	
4.8	Использование методов перестановки для шифрования данных Лаб	7	4	
4.9	Методы криптоанализа классических шифров Лаб	7	4	
4.10	Криптосистемы с открытым ключом. Методы ЭЦП Лаб	7	4	
4.11	Методы сжатия. АЛгоритм Шеннона - Фано Лаб	7	4	
4.12	Методы сжатия. АЛгоритм Хаффмена Лаб	7	4	
4.13	Корректирующие коды. Коды Хэмминга Лаб	7	4	
4.14	Защита файлов от несанкционированного доступа с помощью архиваторов и средств Microsoft Office. Лаб	7	2	
4.15	Восстановление удаленных файлов и необратимое удаление информации. Лаб	7	2	
4.16	Защита папок и файлов Лаб	7	2	
4.17	Обеспечение безопасности локальных сетей Лаб	7	2	
	Раздел 5Технические средства защиты и комплексное обеспечение безопасности	7		

5.1	Средства контроля доступа. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки Лек/Ср	7	2/7	
5.2	Биометрические системы идентификации Ср	7	7	
5.3	Защита программ от несанкционированного использования с помощью USB-ключей и программного обеспечения производителя. Лаб	7	2	
5.4	Защита программ от несанкционированного использования с помощью USB-ключей и средств разработчика. Лаб	7	2	
	Раздел 6Безопасности в сети Интернет	7		
6.1	Классификация Интернет-угроз. Роль Интернета в мировом информационном пространстве. Понятие и виды сетевых атак. Основные угрозы в Интернете для детей и подростков. Защита и управление репутацией в Интернете. Антиспамовые средства. Лек/ Ср	7	2/7	
6.2	Настройка параметров безопасности браузера Лаб	7	2	
	Раздел 7. Самостоятельная работа	7		
7.1	Выполнение курсовой работы	7	21	
7.2	Подготовка к экзамену		5	
	Раздел 7Контактные часы на аттестацию	7		
8.1	Защита курсовой работы /КА/	7	1	
8.2	Экзамен /КЭ/	7	2,3	

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	Нестеров, С. А.	Основы информационной безопасности	Санкт-Петербург : Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст : электронный	https://e.lanbook.com/book/370967

6.1.2. Дополнительнаялитература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Артюшенко В. В., Никулин А. В.	Компьютерные сети и телекоммуникации: учебно- методическое пособие	Новосибирск: НГТУ, 2020	https://e.lanbook.com/book/152244

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	Microsoft Windows
6.2.1.2	Code::Block

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	Консультантплюс
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	Помещения для выполнения курсовых работ укомплектованы специализированной мебелью и техническими средствами обучения (стационарными или переносными)