

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Попов Анатолий Николаевич  
Должность: директор  
Дата подписания: 31.05.2023 17:44:35  
Уникальный программный ключ:  
1e0c38dccb0aee75cee1e5c09c1d58751c7497bc8

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА  
Федеральное государственное бюджетное образовательное учреждение высшего образования  
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

## Основы информационной безопасности

### Рабочая программа дисциплины (модуля)

Направление подготовки 09.03.03 Прикладная информатика

Направленность (профиль) Прикладная информатика на железнодорожном транспорте

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Виды контроля в семестрах:

Зачет 8

#### Распределение часов дисциплины по семестрам

Семестр (<Курс>. <Семестр на курсе>)	8 (4.2)		Итого	
	уп	рп	уп	рп
Вид занятий				
Лекции	28	28	28	28
Практические	28	28	28	28
Конт. ч. на аттест.	0,25	0,25	0,25	0,25
Конт. ч. на аттест. в период ЭС	-	-	-	-
Итого ауд.	56	56	56	56
Контактная работа	56,25	56,25	56,25	56,25
Сам. работа	51,75	51,75	51,75	51,75
Часы на контроль	-	-	-	-
Итого	108	108	108	108

**1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**

1.1	Формирование компетенций для осуществления задач профессиональной деятельности в области теории защиты компьютерной информации, а так же практических умений и навыков в использовании основных принципов, методов и алгоритмов обеспечения информационной безопасности информационно-телекоммуникационных систем.
	Задачами дисциплины являются: –раскрыть основные принципы обеспечения информационной безопасности информационно-телекоммуникационных систем; –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.22
-------------------	---------

**3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)**

УК-10	Способен формировать нетерпимое отношение к коррупционному поведению
УК-10.1	Анализирует факторы, способствующие коррупционным проявлениям, и способы противодействия им
УК-10.2	Обосновывает свою позицию по правовым вопросам, возникающим в процессе противодействия коррупции,
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
ОПК-3.3	Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

**4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Код занятия	Наименование разделов и тем /вид занятия/	Семестр /	Часов	Примечание
	<b>Раздел 1. Основные понятия информационной безопасности</b>			
1.1	Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Модели безопасности. 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/	8	2/0	
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. Лек	8	0/2	
	<b>Раздел 2. Правовые основы информационной безопасности и защита интеллектуальной собственности</b>			
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	8	2/0	
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. Лек/Лаб	8	0/2	

2.3	Всемирная конвенция об авторском праве. Основные институты и понятия международного авторского права. Произведения, пользующиеся охраной. Правовые нормы и стандарты по лицензированию и сертификацииЛек/Лаб	8	0/2	
<b>Раздел 3. Виды информационных угроз</b>				
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 обществеЛек/Лаб	8	2/0	
3.2	Классификация компьютерных преступлений. Группы компьютерных преступлений. Хакерство в мире и в России. Закрытие информации как средство ее защиты от несанкционированного доступаЛек/Лаб	8	2/2	
3.3	Угрозы информационно-психологической безопасности личности и их основные источники. Сущность и современное состояние манипуляции сознанием и поведением людей. Информационная среда иллюзии и реальностиЛек/Лаб	8	2/2	
<b>Раздел 4 Программные средства защиты персональной информации</b>				
4.1	Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов и КПКЛек	8	2/0	
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.Лек/Лаб	8	2/2	
4.3	Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. Кодирование информации. Электронная цифровая подписьЛек/Лаб	8	2/2	
4.4	Анализ программ родительского контроля. Родительский контроль в составе антивирусных программ и операционных системЛек/Лаб	8	2/2	
<b>Раздел 5 Технические средства защиты и комплексное обеспечение безопасности</b>				
5.1	Средства контроля доступа. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замкиЛек/Лаб	8	2/0	
5.2	Биометрические системы идентификацииЛек/Лаб	8	2/4	
5.3	Санитарные и гигиенические требования к работе за компьютером.Лек/Лаб	8	0/2	
<b>Раздел 6 Безопасности в сети Интернет</b>				
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/Лаб	8	2/0	
6.2	Основные психолого-педагогические приемы и средства по обеспечению информационной безопасности детей в Интернете.Лек/Лаб	8	0/2	
6.3	Технологии виртуального взаимодействия. Виды зависимостей. Интернет-зависимость как одно из негативных воздействий глобальной сети. Влияние социальных сетей на адаптацию молодежиЛек/Лаб	8	4/4	
ВСЕГО		56	ЗАЧЕТ	

## 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	Подбельский В. В.	Программирование. Базовый курс С#: учебник для вузов	Москва: Юрайт, 2020	<a href="https://urait.ru/bcode/450868">https://urait.ru/bcode/450868</a>

#### 6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
--	---------------------	----------	----------------------	-----------

	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	<a href="https://e.lanbook.com/book/152244">https://e.lanbook.com/book/152244</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	Microsoft Windows			
6.2.1.2	Code::Block			
<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	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- <a href="https://github.com/">https://github.com/</a>			
6.2.2.3	Портал для разработчиков электронной техники: <a href="http://www.espec.ws/">http://www.espec.ws/</a>			
6.2.2.4	База данных «Библиотека программиста» <a href="https://proglib.io/">https://proglib.io/</a>			
6.2.2.5	Консультантплюс			
6.2.2.6	Информационная система ГАРАНТ			
<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			
7.5	Помещения для выполнения курсовых работ укомплектованы специализированной мебелью и техническими средствами обучения (стационарными или переносными)			