

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Попов Анатолий Николаевич

Должность: директор

Дата подписания: 16.05.2024 11:19:17

Уникальный программный ключ:

1e0c38dcc0aee73cee1e5c09c1d5875fc7497dc8

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) Прикладная информатика на железнодорожном транспорте

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Виды контроля в семестрах:

Экзамен 7

Курсовая работа 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	8 (4.2)		Итого	
	уп	рп	уп	рп
Лекции	16	16	16	16
Лабораторные	48	48	48	48
КЭ	2,3	2,3	2,3	2,3
КА	1	1	1	1
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

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.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-3.3	Составляет обзоры, аннотации, рефераты, научные доклады, публикации и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
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

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
Кодзанятия	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/	7	1	
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	7	1	
	Раздел 2. Правовые основы информационной безопасности и защита интеллектуальной собственности			

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	7	1	
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	7	1	
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 Лаб	7	2	
	Раздел 3. Виды информационных угроз			
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	7	1	
3.2	Классификация компьютерных преступлений. Группы компьютерных преступлений. Хакерство в мире и в России. Закрытие информации как средство ее защиты от несанкционированного доступа Лек/Лаб	7	1/4	
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 Лек/Лаб	7	1/4	
	Раздел 4 Программные средства защиты персональной информации			
4.1	Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов и КПК Лек/лаб	7	1/4	
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	7	1/4	
4.3	Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. Кодирование информации. Электронная цифровая подпись Лек/Лаб	7	1/4	
4.4	Анализ программ родительского контроля. Родительский контроль в составе антивирусных программ и операционных систем Лек/Лаб	7	1/4	
	Раздел 5 Технические средства защиты и комплексное обеспечение безопасности			
5.1	Средства контроля доступа. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки Лек/Лаб	7	1/4	
5.2	Биометрические системы идентификации Лек/Лаб	7	1/4	
5.3	Санитарные и гигиенические требования к работе за компьютером. Лаб	7	4	
	Раздел 6 Безопасности в сети Интернет			

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	7	1	
6.2	Основные психолого-педагогические приемы и средства по обеспечению информационной безопасности детей в Интернете. Лаб	7	4	
6.3	Технологии виртуального взаимодействия. Виды зависимостей. Интернет-зависимость как одно из негативных воздействий глобальной сети. Влияние социальных сетей на адаптацию молодежи Лек/Лаб	7	2/6	
6.4	Подготовка к экзамену /Ср/	7	20	
6.5	Подготовка к лекциям /Ср/	7	16	
6.6	Подготовка к лабораторным работам /Ср/	7	48	
6.7	Выполнение курсовой работы /Ср/	7	40	
6.8	Контроль	7	24.7	
Раздел 7 . Контактная часы на аттестацию				
7.1	КЭ	7	2,3	
7.2	КА	7	1	

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	https://urait.ru/bcode/450868

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Артиюшенко 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)			