

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гаранин Максим Александрович
Должность: Ректор
Дата подписания: 15.05.2024 14:02:48
Уникальный программный ключ:
7708e3a47e66a8ee02711b298d7c78bd1e40bf88

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

Безопасность информационных технологий и систем рабочая программа дисциплины (модуля)

Направление подготовки 09.03.02 Информационные системы и технологии
Направленность (профиль) Информационные системы и технологии на транспорте

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:
экзамены 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		Итого	
	Неделя		16 1/6	
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Практические	16	16	16	16
Конт. ч. на аттест. в период ЭС	2,35	2,35	2,35	2,35
Итого ауд.	64	64	64	64
Контактная работа	66,35	66,35	66,35	66,35
Сам. работа	53	53	53	53
Часы на контроль	24,65	24,65	24,65	24,65
Итого	144	144	144	144

Программу составил(и):

PhD, Ефимова Т.Б.

Рабочая программа дисциплины

Безопасность информационных технологий и систем

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)

составлена на основании учебного плана: 09.03.02-24-1-ИСТб.plm.plx

Направление подготовки 09.03.02 Информационные системы и технологии Направленность (профиль) Информационные системы и технологии на транспорте

Рабочая программа одобрена на заседании кафедры

Цифровые технологии

Зав. кафедрой Ефимова Т.Б,

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Целью изучения дисциплины "Безопасность информационных технологий и систем" является формирование у обучаемых знаний, умений и навыков (уровня сформированности соответствующих компетенций) в результате последовательного изучения содержательно связанных между собой разделов (тем) учебных занятий, а также подготовить студентов к организации и эксплуатации средств защиты компьютерной информации.
-----	---

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:	Б1.О.21
-------------------	---------

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-3.2 Решает задачи связанные с профессиональной деятельностью с учетом основных требований информационной безопасности компьютерных сетей

ПК-5 Способен организовывать мониторинг и контроль функционирования инфокоммуникационных систем и сервисов

ПК-5.2 Оценивает наличие и степень нарушения требований обеспечения информационной и функциональной безопасности инфокоммуникационных систем и соответствующих сервисов

06.040. Профессиональный стандарт "СПЕЦИАЛИСТ ПО КОНТРОЛЮ КАЧЕСТВА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ И СЕРВИСОВ", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 29 сентября 2020 г. N 676н (зарегистрирован Министерством юстиции Российской Федерации 3 ноября 2020 г., регистрационный N 60722)

ПК-5. В. Анализ результатов контроля качества функционирования инфокоммуникационных систем и предоставляемых на их основе сервисов

В/01.6 Организация мониторинга и контроля функционирования инфокоммуникационных систем и сервисов

В результате освоения дисциплины (модуля) обучающийся должен

3.1	Знать:
3.1.1	принципы и методы организации угроз, компьютерных атак и несанкционированного вторжения;
3.1.2	способы и средства защиты информации от утечки по техническим каналам;
3.1.3	
3.2	Уметь:
3.2.1	прогнозировать угрозы, обнаруживать атаки и вторжения, шифровать данные
3.2.2	оценивать коррупционные риски в части защиты информации на объектах информатизации
3.3	Владеть:
3.3.1	организационными, нормативно-правовыми, программными и техническими средствами защиты компьютерной информации
3.3.2	методами и средствами технической защиты информации на объектах информатизации
3.3.3	методами выявления проблем в организации технической защиты информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Примечание
	Раздел 1. Основные понятия и положения защиты информации в компьютерных системах			
1.1	Введение. Доктрина информационной безопасности России. Основные понятия и определения информационной безопасности. /Лек/	6	1	
1.2	Понятия экономической и информационной безопасности. Ключевые вопросы ИБ. Экономическая и информационная безопасность. Составляющие информационной безопасности. /Лек/	6	1	
1.3	Предмет и объект защиты. Угрозы безопасности информации в компьютерных системах. /Лек/	6	1	
1.4	Виды угроз информационной безопасности и классификация источников угроз. Основные виды защищаемой информации. /Лек/	6	1	
1.5	Краткий обзор зарубежного законодательства в области информационной безопасности. Российское законодательство в области информационной безопасности. Закон «Об информации, информационных технологиях и защите информации». Другие законы и нормативные акты. /Лек/	6	2	
1.6	Основы законодательства в области обеспечения информационной безопасности /Пр/	6	2	

	Раздел 2. Направления обеспечения информационной безопасности.			
2.1	Правовая защита. Организационная защита. Инженерно-техническая защита. /Лек/	6	2	
2.2	Программные средства защиты. Криптографические средства защиты. /Лек/	6	2	
2.3	Хакерские утилиты и прочие вредоносные программы. Классические компьютерные вирусы. Скрипт-вирусы. Троянские программы. Сетевые черви. /Пр/	6	2	
2.4	Обеспечение антивирусной защиты операционных систем на основе продуктов компании «Лаборатория Касперского». /Пр/	6	4	
2.5	От чего надо защищаться в первую очередь? Как надо защищаться? Антивирусная защита. Современные средства биометрической идентификации. /Пр/	6	4	
2.6	Идентификация и аутентификация. Парольная защита. /Пр/	6	4	
2.7	Классические методы шифрования. /Лаб/	6	2	
2.8	Изучение криптографического стандарта DES /Лаб/	6	4	
2.9	Изучение криптографического стандарта ГОСТ 28147-89 /Лаб/	6	4	
	Раздел 3. Построения системы информационной безопасности			
3.1	Основные аспекты построения системы информационной безопасности. Программа информационной безопасности. Модели ИБ, требования и основные этапы реализации информационной безопасности. /Лек/	6	2	
3.2	Мероприятия по защите информации. Политика информационной безопасности. /Лек/	6	2	
3.3	Анализ и управление рисками при реализации информационной безопасности. Соотношение эффективности и рентабельности систем информационной безопасности. /Лек/	6	2	
	Раздел 4. Защита информации в информационных системах и компьютерных сетях			
4.1	Определение защищенной информационной системы. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. /Лек/	6	2	
4.2	Методология анализа защищенности информационной системы. Концепция защищенных виртуальных частных сетей. /Лек/	6	2	
	Раздел 5. Защита информации от утечки по техническим каналам			
5.1	Способы защиты информации. Характеристика защитных действий. /Лек/	6	2	
5.2	Защита информации от утечки по визуально-оптическим каналам. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным. Защита информации от утечки по материально-вещественным каналам. /Лек/	6	2	
	Раздел 6. Противодействие несанкционированному доступу к источникам конфиденциальной информации			
6.1	Способы несанкционированного доступа. Технические средства несанкционированного доступа к информации. Защита от наблюдения и фотографирования. Защита от подслушивания. /Лек/	6	2	
6.2	Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра. /Лек/	6	2	
6.3	Защита от копирования. /Лаб/	6	2	
6.4	Передача зашифрованных сообщений по электронной почте /Лаб/	6	4	
6.5	Особенности DoS и DDoS, характеристика атак. /Ср/ /Ср/	6	2	
6.6	Подходы и методология оценки рисков информационной безопасности /Ср/	6	2	
	Раздел 7. Защита информации в электронных платежных системах			

7.1	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. /Лек/	6	2	
7.2	Персональный идентификационный номер. Универсальная электронная платежная система UEPS. Обеспечение безопасности электронных платежей через сеть Internet. /Лек/	6	2	
7.3	Обеспечение безопасности электронных платежей через сеть Internet. /Ср/	6	1	
Раздел 8. Самостоятельная работа				
8.1	Подготовка к лекциям /Ср/	6	16	
8.2	Подготовка к практическим занятиям /Ср/	6	16	
8.3	Подготовка к лабораторным занятиям /Ср/	6	16	
Раздел 9. Контактные часы на аттестацию				
9.1	Экзамен /КЭ/	6	2,35	

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 фиксации 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	https://urait.ru/bcode/469866

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

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 Windows10 Pro Договор №034210000481700004
6.2.1.2	Microsoft office 2013 (Лицензия № 61887848) Договор на поставку № 0342100004813000011
6.2.1.3	7-zip (http://www.7-zip.org/) (GNU LGPL license)

6.2.2 Перечень профессиональных баз данных и информационных справочных систем

6.2.2.1	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- https://github.com/
6.2.2.2	База книг и публикаций Электронной библиотеки "Наука и Техника" - http://www.n-t.ru

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	База данных «Отраслевой портал специалистов» http://www.connect-wit.ru/
6.2.2.6	Гарант.ру https://www.garant.ru/
6.2.2.7	КонсультантПлюс http://www.consultant.ru/
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	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