

Документ подписан простой электронной подписью

Информация о владельце: **МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**

ФИО: Гаранин Максим Александрович **ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Должность: Ректор

Федеральное государственное бюджетное образовательное учреждение высшего образования

Дата подписания: 05.09.2023 16:06:25

Уникальный программный ключ:

7708e3a47e66a8ee02711b298d7c78bd1e40bf88

САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

Безопасность и защита информации в САПР рабочая программа дисциплины (модуля)

Направление подготовки 09.04.01 Информатика и вычислительная техника
Направленность (профиль) АСОИУ на транспорте

Квалификация **Магистр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Виды контроля в семестрах:
экзамены 2

Распределение часов дисциплины по семестрам

Семестр (<Курс>. <Семестр на курсе>)	2 (1.2)		Итого	
	Неделя		Итого	
Вид занятий	уп	рп	уп	рп
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Конт. ч. на аттест. в период ЭС	2,35	2,35	2,35	2,35
Итого ауд.	48	48	48	48
Контактная работа	50,35	50,35	50,35	50,35
Сам. работа	69	69	69	69
Часы на контроль	24,65	24,65	24,65	24,65
Итого	144	144	144	144

Программу составил(и):

к.т.н., доцент, Припутников А.П.

Рабочая программа дисциплины

Безопасность и защита информации в САПР

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

составлена на основании учебного плана: 09.04.01-23-2-ИВТм.plm.plx

Направление подготовки 09.04.01 Информатика и вычислительная техника Направленность (профиль) АСОИУ на транспорте

Рабочая программа одобрена на заседании кафедры

Цифровые технологии

Зав. кафедрой

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Целью освоения дисциплины является формирование общепрофессиональной компетенции, заключающееся в способности анализировать правила управления безопасностью вычислительных систем и компьютерных сетей, проводить комплексный подход к обеспечению безопасности, анализировать и структурировать угрозы безопасности, оформлять и представлять аналитические обзоры рисков безопасности, изучать методы и средства обеспечения безопасности вычислительных систем и компьютерных сетей с обоснованными выводами и рекомендациями.
-----	--

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ОП:	Б1.О.08
-------------------	---------

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

ОПК-3 Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями;

ОПК-3.1 Анализирует профессиональную информацию, направленную на безопасность и защиту информации, и представляет её в виде аналитических обзоров

ОПК-3.2 Оформляет и представляет научно-техническую информацию в соответствии со сложившимся академическим этикетом

В результате освоения дисциплины (модуля) обучающийся должен

3.1	Знать:
3.1.1	основные положения законодательства в области современного авторского права и защиты информации;
3.1.2	основные методы и средства защиты конфиденциальной информации;
3.1.3	состав и организацию систем информационной безопасности, методы криптографических преобразований;
3.1.4	основные стандарты и протоколы шифрования и электронной подписи;
3.1.5	методы и средства обеспечения информационной безопасности компьютерных систем;
3.1.6	современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования;
3.1.7	современные подходы к построению систем защиты информации.
3.2	Уметь:
3.2.1	определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий;
3.2.2	использовать современные программные средства для защиты информации;
3.2.3	принимать адекватные решения при выборе средств защиты информации на основе анализа угроз;
3.2.4	разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности;
3.2.5	обоснованно выбирать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты.
3.3	Владеть:
3.3.1	навыками разработки защищенных приложений;
3.3.2	навыками создания защищенной среды с помощью аппаратно-программных средств защиты;
3.3.3	навыками самостоятельного проектирования систем защиты информации;
3.3.4	методами оценки эффективности систем защиты информации в компьютерных системах.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Примечание
	Раздел 1. Основы защиты информации			
1.1	Средства и методы защиты дисков от несанкционированного доступа и копирования. Способы создания ключевых носителей информации. Привязка программных средств к конкретному компьютеру. Критерии выбора системы защиты. Технические устройства защиты информации и программного обеспечения. Принципы действия электронных ключей. /Лек/	2	2	

1.2	Взлом моноалфавитного подстановочного шифра методом частотной атаки /Лаб/	2	4	
1.3	Классификация средств защиты информации и программного обеспечения от несанкционированного доступа и копирования: средства собственной защиты, средства защиты в составе вычислительной системы, средства защиты с запросом информации. Активные и пассивные методы защиты программного обеспечения. /Лек/	2	2	
1.4	Одноразовые блокноты /Лаб/	2	4	
1.5	Запись и чтение информации для пластиковых карт с магнитной полосой /Лаб/	2	4	
1.6	Изучение и практическая реализация современных методик защиты компьютерной информации. Исследование методики защиты информации /Ср/	2	6	
	Раздел 2. Криптографические средства защиты информации			
2.1	Основы криптографии. Критерий надежности шифрования. Основные криптографические приемы. Блочное шифрование. Схема поточного шифрования. Использование генераторов псевдослучайных чисел для шифрования. /Лек/	2	4	
2.2	Скрытая передача информации в JPEG изображениях /Лаб/	2	4	
2.3	Основы симметричного шифрования данных /Ср/	2	6	
2.4	Блочное и поточное шифрование данных Асимметричное шифрование данных /Ср/	2	6	
	Раздел 3. Защита информационных и операционных систем			
3.1	Шифрование с открытым ключом. Идентификация электронной подписи. Хеширование данных. Стандарты шифрования данных. /Лек/	2	2	
3.2	Метод шифрования с открытым ключом RSA /Лаб/	2	4	
3.3	Шифрование с открытым ключом и электронная цифровая подпись на GPG /Лаб/	2	4	
3.4	Организация систем защиты информации от несанкционированного доступа. Идентификация и установление подлинности. Установление подлинности пользователя, файла, вычислительной системы. Выбор пароля. Установление полномочий. Матрица установления полномочий. Иерархические системы установления полномочий. Системы регистрации пользователей, событий, используемых ресурсов. Компьютерное пиратство. /Лек/	2	2	
3.5	Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому /Лаб/	2	4	

3.6	Компьютерные вирусы. Вирусы, заражающие загрузочные сектора. Файловые вирусы. Загрузочно-файловые вирусы. Полиморфные вирусы. Организационные и программные способы борьбы с вирусным заражением программного обеспечения. /Лек/	2	2	
3.7	Защита информации в компьютерных сетях. Классификация удаленных атак. Методы защиты от них. Технологии VPN. Шифрование данных на сетевом уровне. Применение технологий шифрования данных совместно с межсетевыми экранами. Защищенные протоколы прикладных /Лек/	2	2	
3.8	Сеть Фейштеля /Лаб/	2	4	
3.9	Модель безопасности современной операционной системы /Ср/	2	6	
3.10	Основы защиты данных в компьютерных сетях /Ср/	2	5	
Раздел 4. Самостоятельная работа				
4.1	Подготовка к лабораторным занятиям /Ср/	2	32	
4.2	Подготовка лекционным занятиям /Ср/	2	8	
Раздел 5. Контактная часы на аттестацию				
5.1	Экзамен /КЭ/	2	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 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	Алешкин А. С., Лесько С. А., Жуков Д. О.	Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности): Учебное пособие	Москва: МИРЭА, 2020	https://e.lanbook.com/bo

6.1.2. Дополнительная литература

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

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Бурова М. А., Овсянников А. С.	Информационная безопасность и криптографическая защита информации: конспект лекций	Самара: СамГУП С, 2009	https://e.lanbook.com/bc
Л2.2	Яковлева Е.М.	Автоматизированное проектирование средств и систем управления: учебное пособие	Томск: Томский политехнический университет, 2016	https://e.lanbook.com/bc

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	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