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) Управление цифровой инфраструктурой организации

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Виды контроля в семестрах:

экзамены 7
курсовые работы 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16,7			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	48	48	48	48
Конт. ч. на аттест.	1,5	1,5	1,5	1,5
Конт. ч. на аттест. в период ЭС	2,35	2,35	2,35	2,35
Итого ауд.	64	64	64	64
Контактная работа	67,85	67,85	67,85	67,85
Сам. работа	123,5	123,5	123,5	123,5
Часы на контроль	24,65	24,65	24,65	24,65
Итого	216	216	216	216

Программу составил(и):
к.п.н., доцент, Додонов М.В.

Рабочая программа дисциплины
Информационная безопасность

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана: 09.03.03-24-1-ПИб.plm.plx
Направление подготовки 09.03.03 Прикладная информатика Направленность (профиль) Управление цифровой инфраструктурой организации

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.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-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 Оформлеет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам

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/	7	1	
1.2	Понятия экономической и информационной безопасности. Ключевые вопросы ИБ. Экономическая и информационная безопасность. Составляющие информационной безопасности. /Лек/	7	1	
1.3	Предмет и объект защиты. Угрозы безопасности информации в компьютерных системах. /Лек/	7	1	
1.4	Виды угроз информационной безопасности и классификация источников угроз. Основные виды защищаемой информации. /Лек/	7	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. /Лаб/	7	2	
1.6	Основы законодательства в области обеспечения информационной безопасности /Лаб/	7	2	
	Раздел 2. Направления обеспечения информационной безопасности.			

2.1	Правовая защита. Организационная защита. Инженерно-техническая защита. /Лек/	7	2	
2.2	Программные средства защиты. Криптографические средства защиты. /Лаб/	7	2	
2.3	Хакерские утилиты и прочие вредоносные программы. Классические компьютерные вирусы. Скрипт-вирусы. Троянские программы. Сетевые черви. /Лаб/	7	2	
2.4	Обеспечение антивирусной защиты операционных систем на основе продуктов компании «Лаборатория Касперского». /Лаб/	7	4	
2.5	От чего надо защищаться в первую очередь? Как надо защищаться? Антивирусная защита. Современные средства биометрической идентификации. /Лаб/	7	4	
2.6	Идентификация и аутентификация. Парольная зашита. /Лаб/	7	4	
2.7	Классические методы шифрования. /Лаб/	7	2	
2.8	Изучение криптографического стандарта DES /Лаб/	7	4	
2.9	Изучение криптографического стандарта ГОСТ 28147-89 /Лаб/	7	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/	7	2	
3.2	Мероприятия по защите информации. Политика информационной безопасности. /Лаб/	7	2	
3.3	Анализ и управление рисками при реализации информационной безопасности. Соотношение эффективности и рентабельности систем информационной безопасности. /Лаб/	7	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/	7	2	
4.2	Методология анализа защищенности информационной системы. Концепция защищенных виртуальных частных сетей. /Лаб/	7	2	
	Раздел 5. Защита информации от утечки по техническим каналам			
5.1	Способы защиты информации. Характеристика защитных действий. /Лаб/	7	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. /Лаб/	7	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/	7	2	
6.2	Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра. /Лек/	7	2	
6.3	Защита от копирования. /Лаб/	7	2	
6.4	Передача зашифрованных сообщений по электронной почте /Лаб/	7	4	
	Раздел 7. Защита информации в электронных платежных системах			
7.1	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. /Лек/	7	2	
7.2	Персональный идентификационный номер. Универсальная электронная платежная система UEPS. Обеспечение безопасности электронных платежей через сеть Internet. /Лаб/	7	2	

	Раздел 8. Самостоятельная работа			
8.1	Подходы и методология оценки рисков информационной безопасности /Ср/	7	15,5	
8.2	Обеспечение безопасности электронных платежей через сеть Internet. /Ср/	7	8	
8.3	Особенности DoS и DDoS, характеристика атак. /Ср/	7	8	
8.4	Анализ уязвимостей в сетевой инфраструктуре предприятия /Ср/	7	4	
8.5	Разработка политики защиты информации в организации /Ср/	7	8	
8.6	Исследование методов обнаружения и предотвращения кибератак /Ср/	7	8	
8.7	Оценка эффективности механизмов шифрования данных /Ср/	7	8	
8.8	Аудит безопасности информационных систем и разработка рекомендаций по улучшению /Ср/	7	8	
8.9	Сравнительный анализ методов аутентификации и их применение в современных системах безопасности /Ср/	7	8	
8.10	Анализ угроз и уязвимостей в облачных вычислениях и разработка мер по защите данных /Ср/	7	8	
8.11	Тестирование системы мониторинга безопасности сетевого трафика /Ср/	7	8	
8.12	Подготовка к лекциям /Ср/	7	8	
8.13	Подготовка к лабораторным занятиям /Ср/	7	24	
	Раздел 9. Контактные часы на аттестацию			
9.1	Экзамен /КЭ/	7	2,35	
9.2	Курсовая работа /КА/	7	1,5	

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	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: чебник для вузов	Москва: Юрайт, 2021	https://urait.ru/bcode/469866

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес

	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	Операционная система Microsoft® Windows Professional 8 Russian Upgrade OLP NL Academic Edition Договор на поставку № 0342100004813000011 от года.
6.2.1.2	Microsoft Office 2013 Professional Договор № 0342100004814000045

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