

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Гаранин Максим Алексеевич  
Должность: И.о. ректора  
Дата подписания: 15.04.2020 10:44:09  
Уникальный программный ключ:  
09f9c0855a13fb1cc9fc841ffccb251a28eca6f4

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ  
(СамГУПС)**

УТВЕРЖДЕНА:  
решением Учёного совета СамГУПС  
протокол № 39 от 05.03.2018 г.  
в составе основной профессиональной  
образовательной программы

АКТУАЛИЗИРОВАНА:  
решением Учёного совета СамГУПС  
протокол Учёного совета СамГУПС № 50 от 27.03.2019г.

## **Информационная безопасность и защита информации рабочая программа дисциплины (модуля)**

Кафедра	<b>Мехатроника, автоматизация и управление на транспорте</b>
Направление подготовки	<b>27.04.03 Системный анализ и управление</b>
Направленность (профиль)	<b>"Системный анализ в распределенных технических системах»</b>
Квалификация	<b>магистр</b>
Форма обучения	<b>очная</b>
Объем дисциплины	<b>4 ЗЕТ</b>

**1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

**1.1. Цели освоения дисциплины (модуля)**

Дисциплина « Информационная безопасность и защита информации» имеет цель подготовить студентов к организации и эксплуатации средств защиты компьютерной информации.

**1.2 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)**

**ОК-2: готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения**

**Знать:**

<b>Уровень 1 (базовый)</b>	основы теории выбора вариантов из заданного множества альтернатив при различных типах неопределенностей;
<b>Уровень 2 (продвинутый)</b>	методы реализации системы поддержки принятия решений;
<b>Уровень 3 (высокий)</b>	основы теории оптимизации и экспертных систем принятия решений.
<b>Уметь:</b>	
<b>Уровень 1 (базовый)</b>	использовать методы обработки информации для развития современного информационного общества;
<b>Уровень 2 (продвинутый)</b>	использовать методы обработки информации для решения задач управления в социальных системах;
<b>Уровень 3 (высокий)</b>	разрабатывать дополнительные программы по обработке и использованию информации.

**Владеть:**

<b>Уровень 1 (базовый)</b>	методами обработки информации в социальных системах;
<b>Уровень 2 (продвинутый)</b>	методами моделирования социальных систем;
<b>Уровень 3 (высокий)</b>	владеть способами разработки программного обеспечения в рамках решения задач в развитии современного общества.

**ОПК-5: способностью организовать работу коллектива исполнителей, принятие исполнительских решений в условиях спектра мнений, определить порядок выполнения работ**

**Знать:**

<b>Уровень 1 (базовый)</b>	основные понятия функционального анализа: метрического пространства, нормированного пространства, понятия оператора и их свойства;
<b>Уровень 2 (продвинутый)</b>	методы аппроксимации характеристик динамических систем на основе функционального анализа;
<b>Уровень 3 (высокий)</b>	основные численные алгоритмы решения задач аппроксимации.
<b>Уметь:</b>	
<b>Уровень 1 (базовый)</b>	разрабатывать математические модели процессов и объектов;
<b>Уровень 2 (продвинутый)</b>	применять методы функционального анализа при решении уравнений;
<b>Уровень 3 (высокий)</b>	разрабатывать простые численные методы аппроксимации модели.

**Владеть:**

<b>Уровень 1 (базовый)</b>	методами анализа динамических систем управления;
<b>Уровень 2 (продвинутый)</b>	методами оценивания параметров моделей динамических систем;
<b>Уровень 3 (высокий)</b>	методами анализа метрологических характеристик динамических моделей.

**1.3. Результаты обучения по дисциплине (модулю)**

**В результате освоения дисциплины обучающийся должен:**

**Знать:**

- принципы и методы организации угроз, атак и вторжения;
- модели безопасности и секретности;
- способы и методы обнаружения угроз, атак и вторжения,
- методы шифрования;
- программные и технические средства защиты компьютерной информации.

**Уметь:**

создавать модели безопасности и секретности

**Владеть:**

программными и техническими средствами защиты компьютерной информации

## 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код дисциплины	Наименование дисциплины	Коды формируемых компетенций
<b>2.1 Осваиваемая дисциплина</b>		
<b>Б1.Б.5</b>	<b>Информационная безопасность и защита информации</b>	<b>ОК-2; ОПК-5</b>
<b>2.2 Предшествующие дисциплины</b>		
Б1 В.ОД.1	Программные средства компьютерного моделирования	ПК-3, 4
<b>2.3 Осваиваемые параллельно дисциплины</b>		
Б1.Б.9	Проектирование распределенных систем управления	ОПК-4, 5; ПК-1, 8
Б1.Б.7	Современные компьютерные технологии в науке	ОПК-3; ПК-4, 7
<b>2.4 Последующие дисциплины</b>		
Б2.П.4	Преддипломная практика	ПК-1, 2, 3, 5
Б3	Государственная итоговая аттестация	ОК-1; ОПК-3, 4; ПК-1, 3, 4, 5, 6

## 3. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

<b>3.1 Объем дисциплины (модуля)</b>	<b>4 ЗЕТ</b>
--------------------------------------	--------------

### 3.2 Распределение академических часов по семестрам (для офо)/курсам( для зфо) и видам учебных занятий

Вид занятий	№ семестра (для офо) / курса ( для зфо)																				Итого		
	1		2		3		4		5		6		7		8		9		10				
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РП	УП	РПД	УП	РПД	УП	РП	УП	РПД	УП	РПД	
<b>Контактная работа:</b>					42	42																42	42
<i>Лекции</i>																							
<i>Лабораторные</i>					42	42																42	42
<i>Практические</i>																							
<i>Консультации</i>																							
<i>Инд. работа</i>																							
<b>Контроль</b>					36	36																36	36
<b>Сам. работа</b>					66	66																66	66
<b>ИТОГО</b>					144	144																144	144

### 3.3. Формы контроля и виды самостоятельной работы обучающегося

Форма контроля	Семестр (офо)/ курс(зфо)	Нормы времени на самостоятельную работу обучающегося	
		Вид работы	Нормы времени, час
<b>Экзамен</b>	3	Подготовка к лекциям	0,5 часа на 1 час аудиторных занятий
		Подготовка к практическим/ лабораторным занятиям	1 час на 1 час аудиторных занятий
<b>Зачет</b>		Подготовка к зачету	9 часов (офо)
<b>Курсовой проект</b>		Выполнение курсового проекта	72 часа
<b>Курсовая работа</b>		Выполнение курсовой работы	36 часов
<b>Контрольная работа</b>		Выполнение контрольной работы	9 часов
<b>РГР</b>		Выполнение РГР	18 часов
<b>Реферат/эссе</b>		Выполнение реферата/эссе	9 часов

## 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем	Вид занятия	Семестр / курс	К-во ак. часов	Компетенции	Литература	Часы в интерактивной форме	
							К-во ак. часов	Форма занятия
	Раздел 1. Криптографические методы обеспечения информационной безопасности.							

1.1	Шифрование DES.	Лаб	3	6	ОК-2 ОПК-5	Л1.1 Л2.1 Э1 Э2 М1	4	Выполнение заданий по образцу
1.2	Шифрование RC6	Лаб	3	10	ОК-2 ОПК-5	Л1.1 Л2.1 Э1 Э2 М1	4	Выполнение заданий по образцу
1.3	Шифрование AES.	Лаб	3	10	ОК-2 ОПК-5	Л1.1 Л2.1 Э1 Э2 М1	4	Выполнение заданий по образцу
1.4	Шифрование методом Хаффмана.	Лаб	3	16	ОК-2 ОПК-5	Л1.1 Л2.1 Э1 Э2 М1	4	Выполнение заданий по образцу
<b>Раздел 2 Самостоятельная работа</b>								
2.1	Изучение приемов и методов шифрования информации.	Ср	3	8	ОК-2 ОПК-5	Л1.1 Л2.1 Э1 Э2 М1		
2.2	Изучение методов и средств защиты информации в Windows.	Ср	3	8	ОК-2 ОПК-5	Л1.1 Л2.1 Э1 Э2 М1		
2.3	Изучение сети Фейштеля.	Ср	3	8	ОК-2 ОПК-5	Л1.1 Л2.1 Э1 Э2 М1		
2.4	Подготовка к лабораторным работам	Ср	3	42	ОК-2 ОПК-5	Л1.1 Л2.1 Э1 Э2 М1		

## 5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

### 5.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Основными этапами формирования компетенций в рамках дисциплин выступает последовательное изучение содержательно связанных между собой разделов (тем учебных занятий), которые отражены в разделе 4.

#### Матрица оценки результатов обучения по дисциплине

Код компетенции	Планируемые результаты обучения (показатели оценивания компетенций)	Оценочные средства/формы контроля		
		Отчет по лабораторным работам	Тестовые задания	Экзамен
ОК-2	знает	+	+	+
	умеет	+	+	+
	владеет		+	+
ОПК-5	знает	+	+	+
	умеет		+	+
	владеет	+	+	+

### 5.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

#### Критерии формирования оценок по выполнению лабораторных работ

«Зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов в соответствии с заданием, выданным для выполнения лабораторной работы. Обучающийся полностью владеет информацией о нормативных документах, регулирующих хозяйственные процессы в организации; на основании данных о финансовой деятельности может решить все поставленные в задании задачи.

«Не зачтено» - ставится за работу, если обучающийся правильно выполнил менее 2/3 всей работы, использовал при выполнении работы устаревшую нормативную базу, в качестве исходных данных выступили данные учебника, а не реальной организации.

#### Критерии формирования оценок по выполнению тестовых заданий

«Отлично» (5 баллов) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 100 – 90% от общего объема заданных тестовых вопросов.

«Хорошо» (4 балла) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 89 – 70% от общего объема заданных тестовых вопросов.

«Удовлетворительно» (3 балла) – получают обучающиеся с правильным количеством ответов на тестовые вопросы – 69 – 60% от общего объема заданных тестовых вопросов.

«Неудовлетворительно» (0 баллов) - получают обучающиеся с правильным количеством ответов на тестовые вопросы – 59% и менее от общего объема заданных тестовых вопросов. .

### Критерии формирования оценок по экзамену

«Отлично» (5 баллов) – обучающийся демонстрирует знание всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; умение излагать программный материал с демонстрацией конкретных примеров. Свободное владение материалом должно характеризоваться логической ясностью и четким видением путей применения полученных знаний в практической деятельности, умением связать материал с другими отраслями знания.

«Хорошо» (4 балла) – обучающийся демонстрирует знания всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности. Таким образом данная оценка выставляется за правильный, но недостаточно полный.

«Удовлетворительно» (3 балла) – обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. Однако знание основных проблем курса не подкрепляется конкретными практическими примерами, не полностью раскрыта сущность вопросов, ответ недостаточно логичен и не всегда последователен, допущены ошибки и неточности.

### 5.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к экзамену:

1. Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации
2. Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства
3. Информация, для которой установлен специальный режим сбора, хранения, обработки, распространения и использования
4. Перечислить виды информации с ограниченным доступом
5. Перечислить сведения, составляющие государственную тайну и имеющие гриф секретности
6. Дать определение конфиденциальной информации
7. Какие виды защиты имеются от утечки
8. Как определяется степень соответствия результатов защиты информации поставленной цели защиты информации
9. Определить длину ключевого элемента в алгоритме шифрования DES
10. Чем определяется количество циклов шифрования в алгоритме DES
  11. Определить объем ключа в алгоритме DES
  12. Определить длина ключевого элемента в ГОСТ блочного шифрования
  13. Определить количество циклов шифрования в ГОСТ блочного шифрования
  14. Определить объем ключа в ГОСТ блочного шифрования
15. Какие преобразования лежат в основе композиционных блочных шифров
16. В каких криптосистемах открытый ключ и криптограмма могут передаваться по незащищенным каналам
17. Чему должны принадлежать в криптосистемах RSA открытый ключ, секретный ключ, сообщение и криптограмма
18. Как вычисляется секретный ключ в криптосистеме RSA
19. Какой алгоритм применяется для вычисления секретного ключа в криптосистеме RSA
20. Как определяется проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности
21. Определить функцию, осуществляющую отображение элементов некоторого множества в индекс линейного множества
22. Что включает в себя система электронной цифровой подписи
23. Что используется в качестве подписываемого документа
24. Что используется для сжатия подписываемого документа до нескольких десятков или сотен бит
25. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

#### Тестовые задания

Тестирование по дисциплине проводится с использованием ресурсов электронной образовательной среды «Moodle» (режим доступа: <http://do.samgups.ru/moodle/>)

### 5.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

**Описание процедуры оценивания «Тестирование».** Тестирование по дисциплине проводится с использованием ресурсов электронной образовательной среды «Moodle» (режим доступа: <http://do.samgups.ru/moodle/>). Количество тестовых заданий и время задается системой. Во время проведения тестирования обучающиеся могут пользоваться программой дисциплины, справочной литературой, калькулятором. Результат каждого обучающегося оценивается в соответствии с универсальной шкалой, приведенной в пункте 5.2.

**Описание процедуры оценивания «Защита отчета по лабораторным работам».** Защита отчета по лабораторной работе представляет собой устный публичный отчет обучающегося о результатах выполнения, ответы на вопросы преподавателя. Ответ обучающегося оценивается преподавателем в соответствии с критериями, описанными в пункте 5.2

**Описание процедуры оценивания «Экзамен».** Экзамен принимается ведущим преподавателем по данной учебной дисциплине. Проведение экзамена в устной форме, обучающемуся предоставляется 30 минут на подготовку. Опрос обучающегося по билету на устном экзамене не должен превышать 0,35 часа. Ответ обучающегося оценивается в соответствии с критериями, описанными в пункте 5.2.

## 6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

<b>6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)</b>				
<b>6.1.1. Основная литература</b>				
	<b>Авторы, составители</b>	<b>Заглавие</b>	<b>Издательство, год</b>	<b>Кол-во</b>
<b>Л1.1</b>	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте. В 2 ч. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте: учебник для вузов	Москва: УМЦ по образованию на железнодорожном транспорте, 2014	40
<b>6.1.2 Дополнительная литература</b>				
	<b>Авторы, составители</b>	<b>Заглавие</b>	<b>Издательство, год</b>	<b>Кол-во</b>
<b>Л2.1</b>	Корт, С. С.	Теоретические основы защиты информации [Текст] : учеб. пособие для студ. вузов	М. : Гелиос АРВ, 2004,240с.	10
<b>6.2 Методические разработки</b>				
	<b>Авторы, составители</b>	<b>Заглавие</b>	<b>Издательство, год</b>	<b>Кол-во</b>
<b>М 1</b>	Тюмиков Д. К.	Криптографические методы обеспечения информационной безопасности и защиты информации: метод. указ. к вып. лаб. работ для магистров по напр. подгот. САУ	Самара: СамГУПС, 2014	2
<b>6.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"</b>				
	<b>Наименование ресурса</b>		<b>Эл.адрес</b>	
<b>Э1</b>	Викизнание		<a href="http://www.wikiznanie.ru">http://www.wikiznanie.ru</a>	
<b>Э2</b>	Дистанционные образовательные ресурсы СамГУПС		<a href="http://do.samgups.ru/moodle/">http://do.samgups.ru/moodle/</a>	
<b>7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)</b>				
<p>Для освоения дисциплины обучающемуся необходимо: систематически посещать и выполнять лабораторные работы; успешно пройти все формы текущего контроля; успешно пройти промежуточную аттестацию.</p> <p>Данная работа предполагает самостоятельное изучение обучающимся отдельных тем (см. п.4), дополнительную подготовку к каждому лекционному и практическому занятию.</p> <p>Самостоятельная работа обучающихся является важной формой образовательного процесса. Она реализуется вне рамок расписания, а также в библиотеке, дома.</p> <p>Цель самостоятельной работы - научить обучающегося осмысленно и самостоятельно работать сначала с учебным материалом, затем с научной информацией, заложить основы самоорганизации и самовоспитания с тем, чтобы повысить уровень освоения компетенций, а также привить умение в дальнейшем непрерывно повышать свою квалификацию.</p>				
<b>8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)</b>				
Размещение учебных материалов в разделе «Информационная безопасность и защита информации» системы обучения Moodle: <a href="http://do.samgups.ru/moodle/">http://do.samgups.ru/moodle/</a>				
<b>8.1 Перечень программного обеспечения и информационных справочных систем</b>				
<b>8.1.1</b>	Операционная система Windows			
<b>9. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)</b>				
<p>Лекционная и аудитория для проведения лабораторных занятий оборудованные учебной мебелью; неограниченный доступ к электронно-библиотечным системам (через ресурсы библиотеки СамГУПС), к электронной информационно-образовательной среде moodle и к информационно-телекоммуникационной сети «Интернет» в рамках самостоятельной работы обучающегося.</p> <p>Для проведения лабораторных работ по дисциплине «Информационная безопасность и защита информации» необходимо: мультимедийное оборудование (проектор, экран, ноутбук или компьютер).</p>				