

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Кислова Наталья Николаевна  
Должность: Проректор по УМР и качеству образования  
Дата подписания: 30.11.2021  
Уникальный программный ключ:  
52802513f5b14a975b7e9b13008093d5726b159bf6064f865ae65b96a966c035

**МИНОБРНАУКИ РОССИИ**

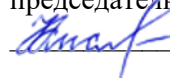
**Федеральное государственное бюджетное образовательное учреждение  
высшего образования**

**«Самарский государственный социально-педагогический университет»**

**Кафедра информатики, прикладной математики и методики их преподавания**

УТВЕРЖДАЮ

Проректор по УМР и КО,  
председатель УМС СГСПУ  
Н.Н. Кислова



# МОДУЛЬ "ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ"

## Информационная безопасность рабочая программа дисциплины (модуля)

Закреплена за кафедрой	<b>Информатики, прикладной математики и методики их преподавания</b>		
Учебный план	ФМФИ-619ПИЗ(4г6м).plx Направление подготовки 09.03.03 Прикладная информатика Направленность (профиль): «Прикладная информатика в государственном и муниципальном управлении» протокол №8 от 29.04.2020 протокол №10 от 26.06.2020		
Квалификация	<b>бакалавр</b>		
Форма обучения	<b>заочная</b>		
Общая трудоемкость	<b>6 ЗЕТ</b>		
Часов по учебному плану	216	Виды контроля в семестрах:	
в том числе:		экзамены 7	
аудиторные занятия	26		
самостоятельная работа	181		
часов на контроль	9		

### Распределение часов дисциплины по семестрам

Семестр(Курс.Номер семестра на курсе)	7(4.1)		Итого	
	УП	РПД	УП	РПД
Лекции	10	10	10	10
Лабораторные	16	16	16	16
В том числе инт.	6	6	6	6
Итого ауд.	26	26	26	26
Контактная работа	26	26	26	26
Сам. работа	181	181	181	181
Часы на контроль	9	9	9	9
Итого	216	216	216	216

Направление подготовки 09.03.03 Прикладная информатика, направленность (профиль): «Прикладная информатика в государственном и муниципальном управлении»

Рабочая программа дисциплины «Информационная безопасность»

Программу составил(и):

*Добудько Александр Валерьянович*

Рабочая программа дисциплины

**Информационная безопасность**

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата) (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана:

Направление подготовки 09.03.03 Прикладная информатика

Направленность (профиль): «Прикладная информатика в государственном и муниципальном управлении»

протокол №8 от 29.04.2020

протокол №10 от 26.06.2020

утвержденного учёным советом вуза от 31.08.2018 протокол № 1.

Рабочая программа одобрена на заседании кафедры

**Информатики, прикладной математики и методики их преподавания**

Протокол от 28.08.2018 г. № 1

Зав. кафедрой Добудько Т.В.

Начальник УОП



Н.А. Доманина

### 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

**Цель изучения дисциплины:** Формирование профессиональных компетенций учащихся с целью реализации на практике комплекса знаний по защите информации путем выполнения сложных работ, связанных с обеспечением защиты информации на основе разработанных программ и методик, а также проведения сбора и анализа материалов учреждений, организаций и предприятий отрасли с целью выработки и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля, обнаружения возможных каналов сетевых атак и утечки сведений, представляющих служебную или коммерческую тайну.

**Задачи изучения дисциплины:** формирование готовности решения стандартных задач профессиональной деятельности с учетом требований информационной безопасности; использования нормативных документов в области защиты информации и информационной безопасности; информационное обеспечение прикладных процессов.

**Область профессиональной деятельности:**

06 Связь, информационные и коммуникационные технологии

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

Цикл (раздел) ОП: Б1.О.04

#### 2.1 Требования к предварительной подготовке обучающегося:

Содержание дисциплины базируется на материале:

Теоретические основы информатики

Вычислительные системы, сети и телекоммуникации

Информационные системы и технологии

#### 2.2 Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Выполнение и защита выпускной квалификационной работы

### 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. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**

Знает: основные требования, предъявляемые к информационным системам в области защиты информации

**ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**

Умеет: использовать нормативные документы в области защиты информации и информационной безопасности; формировать теоретическую модель угроз информационной безопасности

**ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности**

Способен объективно оценить необходимый уровень информационной безопасности при подготовке публикаций обзорного характера о деятельности органов государственного и муниципального управления

**ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью**

**ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы**

Знает: законодательную базу защиты информации в РФ, модели разграничения доступа, аутентификацию субъектов доступа

**ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы**

Умеет: использовать нормативные документы в области защиты информации и информационной безопасности

**ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы**

Способен проводить экспертизу технической документации на информационные системы на соответствие требованиям информационной безопасности

### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Интеракт.
	<b>Раздел 1. Основы информационной безопасности</b>			
1.1	Информация как объект защиты /Лек/	7	1	1
1.2	Информация как объект защиты /Лаб/	7	2	2
1.3	Информация как объект защиты /Ср/	7	21	

1.4	Информационная безопасность /Лек/	7	1	1
1.5	Информационная безопасность /Лаб/	7	2	2
1.6	Информационная безопасность /Ср/	7	20	
1.7	Критерии оценки безопасности компьютерных систем /Лек/	7	1	
1.8	Критерии оценки безопасности компьютерных систем /Лаб/	7	2	
1.9	Критерии оценки безопасности компьютерных систем /Ср/	7	20	
1.10	Криптографические средства защиты информации /Лек/	7	1	
1.11	Криптографические средства защиты информации /Лаб/	7	2	
1.12	Криптографические средства защиты информации /Ср/	7	20	
1.13	Электронная цифровая подпись /Лек/	7	1	
1.14	Электронная цифровая подпись /Лаб/	7	2	
1.15	Электронная цифровая подпись /Ср/	7	20	
1.16	Защита от копирования /Лек/	7	1	
1.17	Защита от копирования /Лаб/	7	2	
1.18	Защита от копирования /Ср/	7	20	
1.19	Программы с потенциально опасными последствиями /Лек/	7	2	
1.20	Программы с потенциально опасными последствиями /Лаб/	7	2	
1.21	Программы с потенциально опасными последствиями /Ср/	7	20	
1.22	Защита в интернет /Лек/	7	2	
1.23	Защита в интернет /Лаб/	7	2	
1.24	Защита в интернет /Ср/	7	40	

## 5. Оценочные и методические материалы по дисциплине (модулю)

### 5.1. Содержание аудиторной работы по дисциплине (модулю)

#### Лекция №1

Информация как объект защиты

Вопросы

Введение в защиту информации и информационную безопасность

#### Лекция №2

Информационная безопасность

Вопросы

Информационная безопасность. Основные угрозы информационной безопасности. Обеспечение информационной безопасности. Аппаратно-программные средства защиты информации

#### Лекция №3

Критерии оценки безопасности компьютерных систем Вопросы

Критерии оценки безопасности компьютерных систем. Оранжевая книга. Основные элементы политики безопасности. Классы безопасности.

#### Лекция №4

Криптографические средства защиты информации Вопросы

Простые криптосистемы. Шифрование методом замены (подстановки). Шифрование методом перестановки. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Организационные проблемы криптозащиты.

#### Лекция №5

Электронная цифровая подпись

Вопросы

Проблема аутентификации данных и электронная цифровая подпись. Однонаправленные хэш-функции. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Алгоритм безопасного хэширования SHA. Отечественный стандарт хэш-функции. Алгоритмы электронной цифровой подписи. Алгоритм цифровой подписи Эль Гамала (EGSA). Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи.

#### Лекция №6

Защита от копирования

Вопросы

Защита от копирования. Защита CD от копирования. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя. Протоколы идентификации с нулевой передачей знаний.

**Лекция №7**

Программы с потенциально опасными последствиями Вопросы

Программы с потенциально опасными последствиями. Вирус. Люк. Троянский конь. Логическая бомба. Программные закладки. Атака салями.

**Лекция №8**

Защита в интернет Вопросы

Межсетевые экраны. Компьютерные атаки и технологии их обнаружения. Безопасность электронной коммерции.

Безопасность электронных платежных систем. Идеальная служба информационной безопасности. План проведения лабораторных работ

**Лабораторная работа №1**

Средства защиты компьютера от вирусов Вопросы

1. Продемонстрировать знание теоретического материала, его применение для решения практических задач;
2. Составить отчет в формате MS Word.

**Лабораторная работа №2**

Построение кода постоянной длины Вопросы

1. Продемонстрировать знание теоретического материала, его применение для решения практических задач;
2. Составить отчет в формате MS Word.

**Лабораторная работа №3**

Построение кода переменной длины Вопросы

1. Продемонстрировать знание теоретического материала, его применение для решения практических задач; 2. Составить отчет в формате MS Word

**Лабораторная работа №4**

Методы защиты информации. Шифр простой перестановки Вопросы

1. Продемонстрировать знание теоретического материала, его применение для решения практических задач;
2. Составить отчет в формате MS Word.

**Лабораторная работа №5**

Методы защиты информации. Шифр Цезаря Вопросы

1. Продемонстрировать знание теоретического материала, его применение для решения практических задач;
2. Составить отчет в формате MS Word.

**Лабораторная работа №6**

Модифицированный шифр Цезаря со сдвигом по кодовому слову Вопросы

1. Продемонстрировать знание теоретического материала, его применение для решения практических задач;
2. Составить отчет в формате MS Word.

**Лабораторная работа №7**

Архивация информации. Сравнение методов сжатия данных Вопросы

1. Продемонстрировать знание теоретического материала, его применение для решения практических задач; Составить отчет в формате MS Word.

**5.2. Содержание самостоятельной работы по дисциплине (модулю)**

**Содержание обязательной самостоятельной работы по дисциплине**

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1	Информация как объект защиты	Работа с материалами системы управления электронным обучением по теме «Информация как объект защиты».	Отчет в системе управления обучением
2	Информационная безопасность	Работа с материалами системы управления электронным обучением по теме «Информационная безопасность».	Отчет в системе управления обучением
3	Критерии оценки безопасности компьютерных систем	Работа с материалами системы управления электронным обучением по теме «Критерии оценки безопасности компьютерных систем».	Отчет в системе управления обучением
4	Криптографические средства защиты информации	Работа с материалами системы управления электронным обучением по теме «Криптографические средства защиты информации».	Отчет в системе управления обучением
5	Электронная цифровая подпись	Работа с материалами системы управления электронным обучением по теме «Электронная цифровая подпись».	Отчет в системе управления обучением

6	Защита от копирования	Работа с материалами системы управления электронным обучением по теме «Защита от копирования».	Отчет в системе управления обучением
7	Программы с потенциально опасными последствиями	Работа с материалами системы управления электронным обучением по теме «Программы с потенциально опасными последствиями».	Отчет в системе управления обучением
8	Защита в интернет	Работа с материалами системы управления электронным обучением по теме «Защита в интернет».	Отчет в системе управления обучением

**Содержание самостоятельной работы по дисциплине на выбор студента**

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1	Информация как объект защиты	Создание презентации по теме «Информация как объект защиты».	Подготовленная и размещенная в информационно-образовательной среде презентация
2	Информационная безопасность	Создание презентации по теме «Информационная безопасность».	Подготовленная и размещенная в информационно-образовательной среде презентация
3	Критерии оценки безопасности компьютерных систем	Создание презентации по теме «Критерии оценки безопасности компьютерных систем».	Подготовленная и размещенная в информационно-образовательной среде презентация
4	Криптографические средства защиты информации	Создание презентации по теме «Криптографические средства защиты информации».	Подготовленная и размещенная в информационно-образовательной среде презентация
5	Электронная цифровая подпись	Создание презентации по теме «Электронная цифровая подпись».	Подготовленная и размещенная в информационно-образовательной среде презентация
6	Защита от копирования	Создание презентации по теме «Защита от копирования».	Подготовленная и размещенная в информационно-образовательной среде презентация
7	Программы с потенциально опасными последствиями	Создание презентации по теме «Программы с потенциально опасными последствиями».	Подготовленная и размещенная в информационно-образовательной среде презентация
8	Защита в интернет	Создание презентации по теме «Защита в интернет».	Подготовленная и размещенная в информационно-образовательной среде презентация

**5.3. Образовательные технологии**

При организации изучения дисциплины будут использованы следующие образовательные технологии: информационно-коммуникационные технологии, технология организации самостоятельной работы, технология рефлексивного обучения, технология модульного обучения, технология игрового обучения, технологии групповой дискуссии, интерактивные технологии, технология проблемного обучения, технология организации учебно-исследовательской деятельности, технология проектного обучения, технология развития критического мышления.

**5.4. Текущий контроль, промежуточный контроль и промежуточная аттестация**

Балльно-рейтинговая карта дисциплины оформлена как приложение к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине оформлен отдельным документом.

**6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ**

**6.1. Рекомендуемая литература**

**6.1.1. Основная литература**

	Авторы, составители	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
Л1.1	Гулятьева Т.А.	Основы информационной безопасности: учебное пособие <a href="http://biblioclub.ru/index.php?page=book&amp;id=574729">http://biblioclub.ru/index.php?page=book&amp;id=574729</a>	Новосибирск: Новосибирский государственный технический университет, 2018
Л1.2	Ковалев Д.В., Богданова Е.А.	Информационная безопасность: учебное пособие <a href="http://biblioclub.ru/index.php?page=book&amp;id=493175">http://biblioclub.ru/index.php?page=book&amp;id=493175</a>	Ростов-на-Дону: Южный федеральный университет, 2016

**6.1.2. Дополнительная литература**

	Авторы, составители	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
--	---------------------	--	-------------------

Рабочая программа дисциплины «Информационная безопасность»

Л2.1	Прохорова О.В.	Информационная безопасность и защита информации: учебник <a href="http://biblioclub.ru/index.php?page=book&amp;id=438331">http://biblioclub.ru/index.php?page=book&amp;id=438331</a>	Самара: Самарский государственный архитектурно-строительный университет, 2014
Л2.2	Аверченков В.И.	Аудит информационной безопасности: учебное пособие для вузов <a href="http://biblioclub.ru/index.php?page=book&amp;id=93245">http://biblioclub.ru/index.php?page=book&amp;id=93245</a>	Москва: Флинта, 2016

**6.2 Перечень программного обеспечения**

- ABBYY Lingvo x6 Многоязычная Академическая версия (30 раб. мест)
- Acrobat Reader DC
- Dr.Web Desktop Security Suite, Dr.Web Server Security Suite
- GIMP
- Microsoft Office 2016 Professional Plus (Пакет программ Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher)
- Microsoft Office 365 Pro Plus - subscription license (12 month) (Пакет программ Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher, Skype for Business, OneDrive, SharePoint Online)
- Microsoft Windows 10 Education
- Microsoft Windows 7/8.1 Professional
- RINEL Lingvo v7.0
- XnView
- Архиватор 7-Zip
- НордМастер 5.0, НордКлиент (16 рабочих мест)
- Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»

**6.3 Перечень информационных справочных систем**

- Elsevier (база данных «Freedom Collection» и коллекции электронных книг «Freedom Collection eBook collection», национальная подписка на полнотекстовые ресурсы)
- SCOPUS издательства Elsevier
- SpringerNature (национальная подписка на полнотекстовые ресурсы)
- База данных международных индексов научного цитирования Web of Science
- БД «Polpred.com. Обзор СМИ»
- УИС РОССИЯ
- ЭБС «E-LIBRARY.RU»
- ЭБС «ЛАНЬ»
- ЭБС «РУКОНТ» (Контекстум)
- ЭБС «Университетская библиотека онлайн»
- ЭБС «ЮРАЙТ» (Коллекция Легендарные книги)

**7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

7.1	Наименование специального помещения: учебная аудитория для проведения занятий лекционного типа, практических занятий, групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации, Учебная аудитория. Оснащенность: Меловая доска-1шт., Комплект учебной мебели
7.2	Наименование специального помещения: помещение для самостоятельной работы, Читальный. Оснащенность: ПК -4шт., Письменный стол-4 шт., Парта-2 шт.

**8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

<p>Работа над теоретическим материалом происходит кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю.</p> <p>Проработка рабочей программы дисциплины, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с информационными источниками в разных форматах.</p> <p>Также в процессе изучения дисциплины методические рекомендации могут быть изданы отдельным документом.</p>
--

Вид контроля		Минимальное количество баллов	Максимальное количество баллов
<b>Наименование раздела «Информационная безопасность»</b>			
Текущий контроль по разделу:			
1	Аудиторная работа	13	26
2	Самостоятельная работа (специальные обязательные формы)	5	10
3	Самостоятельная работа (специальные формы на выбор студента)	2	4
Контрольное мероприятие по разделу		-	-
Промежуточный контроль		20	40
Промежуточная аттестация		36	60
Итого:		<b>56</b>	<b>100</b>

Виды контроля	Перечень или примеры заданий, критерии оценки и количество баллов	Темы для изучения и образовательные результаты
<b>Текущий контроль по разделу «Информационная безопасность»</b>		
1	<p>Аудиторная работа</p> <p>Выступление с презентацией по темам модуля (x4)</p> <ul style="list-style-type: none"> <li>• Доклад раскрывает ключевые аспекты выбранной темы.</li> <li>• Прослеживается связь между понятиями и логика изложения материала.</li> <li>• Выбраны достоверные источники информации, их список оформлен по ГОСТ.</li> <li>• Выдержана структура презентации, стиль соответствует теме изложения.</li> <li>• Студент ответил на все заданные вопросы.</li> </ul> <p>Каждый критерий оценивается в 1 балл, итого 5x4=20 баллов</p> <p>Решен кейс по заданию преподавателя (x2)</p> <ul style="list-style-type: none"> <li>• Представлено несколько (2 и более) возможных решения, среди которых выбрано оптимальное</li> <li>• Оптимальное решение оформлено в соответствии со стандартами отрасли (таблицы, диаграммы)</li> <li>• Студент свободно отвечает на вопросы аудитории и преподавателя</li> </ul> <p>Каждый критерий оценивается в 1 балл, итого 3x2=6 баллов</p> <p>Итого – 26 баллов</p>	<p>Темы:</p> <ol style="list-style-type: none"> <li>1. Информация как объект защиты</li> <li>2. Информационная безопасность</li> <li>3. Критерии оценки безопасности компьютерных систем</li> <li>4. Криптографические средства защиты информации</li> <li>5. Электронная цифровая подпись</li> <li>6. Защита от копирования</li> <li>7. Программы с потенциально опасными последствиями</li> <li>8. Защита в интернет.</li> </ol> <p>Образовательные результаты:</p> <p>Знает: основные требования, предъявляемые к информационным системам в области защиты информации;</p> <p>Умеет: использовать нормативные документы в области защиты информации и информационной безопасности; формировать теоретическую модель угроз информационной безопасности.</p> <p>Способен объективно оценить необходимый уровень информационной безопасности при подготовке публикаций обзорного характера о</p>



			<p>деятельности органов государственного и муниципального управления.                  Знает: законодательную базу защиты информации в РФ, модели разграничения доступа, аутентификацию субъектов доступа                  Умеет: использовать нормативные документы в области защиты информации и информационной безопасности;                  Имеет опыт подготовки технической документации для этапов проектирования, внедрения и эксплуатации информационной системы</p>
2	<p>Самостоятельная работа (обязательные формы)</p>	<p>Подготовлены текстовые отчеты по заданиям лабораторных работ.                  Отчеты содержат результаты выполнения всех заданий лабораторных работ.                  В документе приведены снимки экрана ключевых моментов работ.                  Отчеты содержат оформленный по ГОСТ библиографический список.                  Текст работы и иллюстрации оформлены согласно требованиям ГОСТ.                  Отчет отправлен преподавателю в установленные сроки/загружен на проверку в систему управления обучением.                  Каждый критерий оценивается в 0-2 балла.</p>	<p>Темы:                  1. Информация как объект защиты                  2. Информационная безопасность                  3. Критерии оценки безопасности компьютерных систем                  4. Криптографические средства защиты информации                  5. Электронная цифровая подпись                  6. Защита от копирования                  7. Программы с потенциально опасными последствиями                  8. Защита в интернет                  Образовательные результаты:                  Знает: основные требования, предъявляемые к информационным системам в области защиты информации;                  Умеет: использовать нормативные документы в области защиты информации и информационной безопасности; формировать теоретическую модель угроз информационной безопасности.                  Способен объективно оценить необходимый уровень информационной безопасности при подготовке публикаций обзорного характера о деятельности органов государственного и муниципального управления.                  Знает: законодательную базу защиты информации в РФ, модели разграничения доступа, аутентификацию субъектов доступа                  Умеет: использовать нормативные документы в области защиты информации и информационной безопасности;</p>

			Имеет опыт подготовки технической документации для этапов проектирования, внедрения и эксплуатации информационной системы
3	Самостоятельная работа (на выбор студента)	<p>Подготовлены материалы в формате HTML по заданной теме.</p> <ul style="list-style-type: none"> <li>• Студент подготовил материал в формате MS Word.</li> <li>• Подготовлено графическое оформление материала</li> <li>• Сформированы электронные таблицы к материалу</li> <li>• Материал конвертирован в формат HTML и размещен в ЭИОС вуза Каждый критерий оценивается в 1 балл.</li> </ul> <p>Итого – 4x1=4 балла</p>	<p>Темы: Информация как объект защиты Информационная безопасность Критерии оценки безопасности компьютерных систем Криптографические средства защиты информации Электронная цифровая подпись Защита от копирования Программы с потенциально опасными последствиями Защита в интернет Образовательные результаты: Знает: основные требования, предъявляемые к информационным системам в области защиты информации; Умеет: использовать нормативные документы в области защиты информации и информационной безопасности; формировать теоретическую модель угроз информационной безопасности. Способен объективно оценить необходимый уровень информационной безопасности при подготовке публикаций обзорного характера о деятельности органов государственного и муниципального управления.</p>
Промежуточный контроль (кол-во баллов)		Минимальное количество баллов – 20, максимальное – 40	
Промежуточная аттестация		Представлены в фонде оценочных средств для промежуточной аттестации по дисциплине	