МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Учебный план ФМФИ-622ПИо(4г)
Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль): «Корпоративные информационные системы»

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
аудиторные занятия 84
самостоятельная работа 132

Виды контроля в семестрах:
экзамены 5

Распределение часов дисциплины по семестрам

Семестр(Курс.Номер семестра на курсе)	**5(3.1)**		Итого	
Вид занятий	УП	РПД	УП	РПД
Лекции	32	32	32	32
Лабораторные	52	52	52	52
В том числе инт.	16	16	16	16
Итого ауд.	84	84	84	84
Контактная работа	84	84	84	84
Сам. работа	132	132	132	132
Итого	216	216	216	216

Программу составил(и):

Добудько Александр Валерьянович

При наличии обучающихся из числа лиц с ограниченными возможностями здоровья, которым необходим особый порядок освоения дисциплины (модуля), по их желанию разрабатывается адаптированная к ограничениям их здоровья рабочая программа дисциплины (модуля).

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): «Корпоративные информационные системы»

утвержден учёным советом СГСПУ от 24.09.2021 протокол № 2.

Рабочая программа одобрена на заседании кафедры

Информатики, прикладной математики и методики их преподавания

Протокол от 27.08.2021 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 обучающихся 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 учреждений и предприятий

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.
	Раздел 1. Основы информационной безопасности			
1.1	Информация как объект защиты /Лек/	5	4	2
1.2	Информация как объект защиты /Лаб/	5	6	2
1.3	Информация как объект защиты /Ср/	5	16	0

1.4	Информационная безопасность /Лек/	5	4	2
1.5	Информационная безопасность /Лаб/	5	6	2
1.6	Информационная безопасность /Ср/	5	16	0
1.7	Критерии оценки безопасности компьютерных систем /Лек/	5	4	2
1.8	Критерии оценки безопасности компьютерных систем /Лаб/	5	6	2
1.9	Критерии оценки безопасности компьютерных систем /Ср/	5	16	0
1.10	Криптографические средства защиты информации /Лек/	5	4	0
1.11	Криптографические средства защиты информации /Лаб/	5	6	2
1.12	Криптографические средства защиты информации /Ср/	5	16	0
1.13	Электронная цифровая подпись /Лек/	5	4	0
1.14	Электронная цифровая подпись /Лаб/	5	6	2
1.15	Электронная цифровая подпись /Ср/	5	16	0
1.16	Защита от копирования /Лек/	5	4	0
1.17	Защита от копирования /Лаб/	5	6	0
1.18	Защита от копирования /Ср/	5	16	0
1.19	Программы с потенциально опасными последствиями /Лек/	5	4	0
1.20	Программы с потенциально опасными последствиями /Лаб/	5	8	0
1.21	Программы с потенциально опасными последствиями /Ср/	5	18	0
1.22	Защита в интернет /Лек/	5	4	0
1.23	Защита в интернет /Лаб/	5	8	0
1.24	Защита в интернет /Ср/	5	18	0

5. Оценочные и методические материалы по дисциплине (модулю)

5.1. Содержание аудиторной работы по дисциплине (модулю)

5 семестр, 16 лекций, 26 лабораторных занятий

Раздел 1. Основы информационной безопасности

Лекция №1-2 (4 часа)

Информация как объект защиты

Вопросы:

1. Определение понятий защита информации и информационная безопасность.
2. Составные части защиты информации и информационной безопасности.
3. Информация и задача её защиты.
4. Нормативно-правовые основы информационной безопасности в РФ

Лекция №3-4 (4 часа)

Информационная безопасность

Вопросы:

1. Стандарты информационной безопасности.
2. Угрозы информационной безопасности: классификация и анализ угроз.
3. Модель построения системы информационной безопасности предприятия.
4. Аппаратно-программные средства защиты информации

Лекция №5-6 (4 часа)

Критерии оценки безопасности компьютерных систем

Вопросы:

1. Основные определения и положения защиты информации в компьютерных системах.
2. Понятие и классификация методов несанкционированного доступа.
3. Классификация способов защиты в компьютерных системах от случайных и преднамеренных угроз.
4. Критерии оценки безопасности компьютерных систем.
5. Основные элементы политики безопасности.
6. Классы безопасности.

Лекция №7-8 (4 часа)

Криптографические средства защиты информации

Вопросы:

1. Простые криптосистемы.
2. Шифрование методом замены (подстановки).
3. Шифрование методом перестановки.
4. Шифрование методом гаммирования.
5. Шифрование с помощью аналитических преобразований.
6. Комбинированные методы шифрования.
7. Организационные проблемы криптозащиты.

Лекция №9-10 (4 часа)

Электронная цифровая подпись

Вопросы:
1. Проблема аутентификации данных и электронная цифровая подпись.
2. Однонаправленные хэш-функции.
3. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
4. Алгоритм безопасного хэширования RSA.
5. Отечественный стандарт хэш-функции.
6. Алгоритмы электронной цифровой подписи.
7. Алгоритм цифровой подписи Эль Гамаля (EGSA).
8. Алгоритм цифровой подписи DSA.
9. Отечественный стандарт цифровой подписи.

Лекция №11-12 (4 часа)

Защита от копирования

Вопросы:
1. Защита от копирования.
2. Защита CD от копирования.
3. Защиты от несанкционированного доступа.
4. Идентификация и аутентификация пользователя.
5. Протоколы идентификации с нулевой передачей знаний.

Лекция №13-14 (4 часа)

Программы с потенциально опасными последствиями

Вопросы
1. Программы с потенциально опасными последствиями.
2. Вирус. Люк. Троянский конь. Логическая бомба.
3. Программные закладки.
4. Атака салями.

Лекция №15-16 (4 часа)

Защита в интернет

Вопросы
1. Межсетевые экраны.
2. Компьютерные атаки и технологии их обнаружения.
3. Безопасность электронной коммерции.
4. Безопасность электронных платежных систем.
5. Идеальная служба информационной безопасности.

Лабораторное занятие №1. (6 часов)

«Информация как объект защиты»

Задания:
1. Составить перечень основных нормативных документов, регламентирующих деятельность в области информационной безопасности и защиты информации в РФ.
2. Составить глоссарий понятий в области защиты информации и информационной безопасности.

Лабораторное занятие №2. (6 часов)

«Информационная безопасность»

Задания:
1. С помощью средств информационных технологий создайте модель построения системы информационной безопасности предприятия.

Лабораторное занятие №3. (6 часов)

«Критерии оценки безопасности компьютерных систем»

Задания:
1. Используя существующие стандарты и методики оценки рисков информационной безопасности, провести анализ защищенности объекта защиты информации

Лабораторная работа №4. «Криптографические средства защиты информации»

1. Построение кода постоянной длины. Изучить метод построения кода постоянной длины и оценить эффективность полученного кода.
2. Построение кода переменной длины. Изучить метод построения кода переменной длины, оценить эффективность полученного кода и сравнить ее с эффективностью кода постоянной длины.
3. Методы защиты информации. Шифр простой перестановки. Выполнить шифрование заданного сообщения простейшим шифром перестановок и выполнить проверку правильности шифрования.
4. Методы защиты информации. Шифр Цезаря. Освоить технологию шифрования и дешифрования информации с использованием шифра Цезаря. Модифицированный шифр Цезаря со сдвигом по кодовому слову. Освоить технологию шифрования и дешифрования информации с использованием модифицированного шифра Цезаря.

Лабораторное занятие №5. (6 часов)

«Электронная цифровая подпись»

Задания:
Создайте сертификат цифровой подписи. Установите созданный вами сертификат. Подпишите созданный вами документ цифровой подписью.

Лабораторное занятие №6. (6 часов)

«Защита от копирования»

Задания:
1. Выполните защиту текстового документа различными способами (ограничение доступа к файлу, настройка копирования при запрете редактирования, запрет копирования и редактирования, запрет копирования, редактирования и печати).
2. Организуйте защиту от несанкционированного просмотра файла, созданного в электронной таблице (защита файла от открытия, защита листа от просмотра, защита элементов листа от просмотра); от несанкционированного изменения (защита файла, защита листа, защита отдельных ячеек листа, защита книги).
3. Опишите способы защиты от несанкционированного доступа в СУБД.
4. Настройте брандмауэр операционной системы. Определите список программ, которым разрешено обрабатывать данные, поступающие в компьютер из внешнего окружения. Не нужно ли сократить этот список?
5. Запустите оснастку Службы. Просмотрите список установленных и работающих служб. Все ли они необходимы для вашей повседневной работы. Остановите ненужные службы.
6. В целях конфиденциальности вашей информации проведите очистку четырех частей данных браузера: списка вводившихся адресов, журнала с историей посещения веб-сайтов, списка временных файлов Интернета и списка cokie-файлов.

Лабораторное занятие №7. (8 часов)

«Программы с потенциально опасными последствиями»

Задания:
Ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методами борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Получить навыки работы с антивирусным пакетом.

Лабораторное занятие №8. (8 часов)

«Защита в интернет»

Задания
1. Запустите виртуальную машину Ubuntu. Определить настройки протокола TCP/IP Вашего компьютера с помощью команды ifconfig. Сделайте экранный снимок сетевых настроек.
2. Для использования утилиты iptables требуются привилегии суперпользователя (root). В консоли введите команду su root и далее пароль суперпользователя.
3. Установите политику по умолчанию ACCEPT для цепочек INPUT, FORWARD и OUTPUT. В отчет вставьте введенные правила.
4. Закройте порт 80 цепочки INPUT для всех IP адресов. Остальные порты цепочки INPUT должны быть открыты. В отчет вставьте введенные правила. Перейдите в браузере по адресу http://localhost/. Проанализируйте в Wireshark какие изменения произошли в сетевом трафике после закрытия 80 порта цепочки INPUT.
8. Откройте возможность работы с локальным Web-сервером только Вашему компьютеру. Все остальные IP адреса не должны иметь доступ к Web-серверу компьютера. В отчет вставьте введенные правила.
9. Заблокируйте с помощью межсетевого экрана выбранные Вами Web-сайты. В отчет вставьте введенные правила.

5.2. Содержание самостоятельной работы по дисциплине (модулю)

Содержание обязательной самостоятельной работы по дисциплине

№ п/п	Темы дисциплины	Содержание самостоятельной работы	Продукты деятельности
1	Информация как объект защиты	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
2	Информационная безопасность	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
3	Критерии оценки безопасности компьютерных систем	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
4	Криптографические средства защиты информации	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
5	Электронная цифровая подпись	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
6	Защита от копирования	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
7	Программы с потенциально опасными последствиями	Оформление отчета по лабораторной работе	Отчет по лабораторной работе
8	Защита в интернет	Оформление отчета по лабораторной работе	Отчет по лабораторной работе

Содержание самостоятельной работы по дисциплине на выбор

№ п/п	Темы дисциплины	Содержание самостоятельной работы	Продукты деятельности
1	Информация как объект защиты	Подготовка доклада на конференцию	Доклад

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, 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	Гультяева, Т. А.	Основы информационной безопасности: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=574729	Новосибирск: Новосибирский государственный технический университет, 2018
Л1.2	Вострецова, Е. В	Основы информационной безопасности: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=697636	Екатеринбург: Издательство Уральского университета, 2019

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
Л2.1	Прохорова, О. В.	Информационная безопасность и защита информации: учебник URL: https://biblioclub.ru/index.php?page=book&id=438331	Самара: Самарский государственный архитектурно-строительный университет, 2014
Л2.2	Аверченков, В. И.	Аудит информационной безопасности: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=93245	Москва: ФЛИНТА, 2021
Л2.3	Ковалев, Д. В.	Информационная безопасность: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=493175	Ростов-на-Дону: Южный федеральный университет, 2016

6.2 Перечень программного обеспечения

- Acrobat Reader DC
- Dr.Web Desktop Security Suite, Dr.Web Server Security Suite
- GIMP
- Microsoft Office 365 Pro Plus - subscription license (12 month) (Пакет программ Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher, Teams, OneDrive, Yammer, Stream, SharePoint Online).
- Microsoft Windows 10 Education
- XnView
- Архиватор 7-Zip

6.3 Перечень информационных справочных систем, профессиональных баз данных

- ЭБС «Университетская библиотека онлайн»
- Базы данных Springer eBooks

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Наименование специального помещения: учебная аудитория для проведения занятий лекционного типа, лабораторных 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 зал. Оснащенность: ПК-4шт. с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СГСПУ, Письменный стол-4 шт., Парта-2 шт.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Работа над теоретическим материалом происходит кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать 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 удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю.
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.
Также в процессе изучения дисциплины методические рекомендации могут быть изданы отдельным документом.

Приложение

Балльно-рейтинговая карта дисциплины «Информационная безопасность»

Курс 3 Семестр 5

Вид контроля		Минимальное количество баллов	Максимальное количество баллов
Наименование раздела «Основы информационной безопасности»			
Текущий контроль по разделу:			
1	Аудиторная работа	8	16
2	Самостоятельная работа (специальные обязательные формы)	8	16
3	Самостоятельная работа (специальные формы на выбор)	4	8
Контрольное мероприятие по разделу		-	-
Промежуточный контроль		20	40
Промежуточная аттестация		36	60
	Итого:	**56**	**100**

Виды контроля		Перечень или примеры заданий, критерии оценки и количество баллов	Темы для изучения и образовательные результаты
Текущий контроль по разделу «Основы информационной безопасности»			
1	Аудиторная работа	Лабораторная работа 1. Информация как объект защиты Лабораторная работа 2. Информационная безопасность Лабораторная работа 3. Критерии оценки безопасности компьютерных систем Лабораторная работа 4. Криптографические средства защиты информации Лабораторная работа 5. Электронная цифровая подпись Лабораторная работа 6. Защита от копирования Лабораторная работа 7. Программы с потенциально опасными последствиями Лабораторная работа 8. Защита в интернет. Критерий оценивания: 1 балл – выполнена базовая часть лабораторной работы, 2 балла – выполнена базовая и дополнительная(индивидуальная) часть лабораторной работы. Итого – 8х2=16 баллов	Тема: Информация как объект защиты Тема: Информационная безопасность Тема: Критерии оценки безопасности компьютерных систем Тема: Криптографические средства защиты информации Тема: Электронная цифровая подпись Тема: Защита от копирования Тема: Программы с потенциально опасными последствиями Тема: Защита в интернет.

			Результаты обучения: 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 учреждений и предприятий Знает: законодательную базу защиты информации в РФ, модели разграничения доступа, аутентификацию субъектов доступа Умеет: использовать нормативные документы в области защиты информации и информационной безопасности Способен проводить экспертизу технической документации на информационные системы на соответствие требованиям информационной безопасности
2	Самостоятельная работа (обязательные формы)	Лабораторная работа 1. Информация как объект защиты Лабораторная работа 2. Информационная безопасность Лабораторная работа 3. Критерии оценки безопасности компьютерных систем Лабораторная работа 4. Криптографические средства защиты информации Лабораторная работа 5. Электронная цифровая подпись Лабораторная работа 6. Защита от копирования Лабораторная работа 7. Программы с потенциально опасными последствиями Лабораторная работа 8. Защита в интернет. Критерий оценивания 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. Каждый критерий оценивается в 0-0,5 балла. Итого – 8х2=16 баллов	Тема: Информация как объект защиты Тема: Информационная безопасность Тема: Критерии оценки безопасности компьютерных систем Тема: Криптографические средства защиты информации Тема: Электронная цифровая подпись Тема: Защита от копирования Тема: Программы с потенциально опасными последствиями Тема: Защита в интернет. Результаты обучения: 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 учреждений и предприятий Знает: законодательную базу защиты информации в РФ, модели разграничения доступа, аутентификацию субъектов доступа Умеет: использовать нормативные документы в области защиты информации и информационной безопасности Способен проводить экспертизу технической документации на информационные системы на соответствие требованиям информационной безопасности
3	Самостоятельная работа (на выбор)	Подготовка доклада Критерий оценивания Представленные в докладе материалы соответствуют проблеме исследования Прослеживается связь между понятиями и логика изложения материала Сформулирована ключевая идея Сделаны выводы по теме Выдержана структура презентации Стиль презентации соответствует теме исследования Текст отражает авторскую позицию Выбраны достоверные источники информации Каждый критерий оценивается в 0-1 балл.	Тема: Информация как объект защиты Результаты обучения: 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 учреждений и предприятий.
Промежуточный контроль (кол-во баллов)		Минимальное количество баллов – 20, максимальное – 40	
Промежуточная аттестация		Представлены в фонде оценочных средств для промежуточной аттестации по дисциплине	