	Факультет	Математики, физики и информатики
	Кафедра	Информатики и информационных технологий
	Направление подготовки	02.03.02 Фундаментальная информатика и информационные технологии
	Профиль	Открытые информационные системы
	Информационные технологии в защите персональных данных	Б1.В.ДВ.14

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тульский государственный педагогический университет им. Л.Н. Толстого»
ФГБОУ ВО «ТГПУ им. Л.Н. Толстого»

УТВЕРЖДЕНА

на заседании Ученого совета университета

протокол № 2 от 11 февраля 2016 г.

Рабочая программа дисциплины «Информационные технологии в защите персональных данных»

Трудоемкость: 3 зачетные единицы

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Рассмотрена на заседании кафедры
информатики и информационных технологий
протокол № 3 от 18 ноября 2015 г.

Заведующий кафедрой _____А.В. Якушин

Одобрена на заседании Ученого совета факультета
Математики, физики и информатики
протокол № 5 от «17» декабря 2015 г.

Декан Реброва И.Ю.

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Достижение планируемых результатов обучения, соотнесенных с общими целями и задачами ОПОП, является целью освоения дисциплины.

Планируемые результаты освоения образовательной программы (код и название компетенции)	**Планируемые результаты обучения**	**Этапы формирования компетенции в процессе освоения образовательной программы**
способностью использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4)	**Выпускник знает:** понятие персональных данных и способы их защиты; **умеет:** осуществлять защиту персональных данных с использованием средств ИКТ; **владеет:** использования основных технических и программных средств для защиты персональных данных на предприятии и в организациях.	1 этап из 1 (7 семестр)

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

Дисциплина «Информационные технологии в защите персональных данных» относится к дисциплинам по выбору вариативной части образовательной программы. Изучение данной дисциплины осуществляется в 7 семестре.

К началу изучения дисциплины студенты должны владеть:

- знаниями основных понятий информационной безопасности, защиты данных;
- умениями использовать современное программное обеспечение, правильно эксплуатировать компьютер и обеспечивать безопасность и целостность данных;
- навыками и (или) опытом деятельности безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Очная форма обучения

Вид учебной работы	**Объем зачетных единиц / часов по формам обучения**
Максимальная учебная нагрузка (всего)	108/3
Контактная работа обучающихся с преподавателем (всего)	22
в том числе:	
лекции	8
лабораторные занятия (включая защиту отчета по лабораторным работам)	
семинарские занятия	
практические занятия	12
контрольные работы	
другие виды контактной работы (КСРС)	2
Самостоятельная работа студента (всего)	86

в том числе:	
внеаудиторная самостоятельная работа по подготовке к лекционным занятиям	22
внеаудиторная самостоятельная работа по подготовке к лабораторным занятиям и защите отчета	
внеаудиторная самостоятельная работа при подготовке к семинарским и/или практическим занятиям	30
подготовка учебного проекта	
подготовка к контрольной работе	
выполнение заданий для самостоятельной работы в системе управления обучением MOODLE	30
выполнение курсового проекта (работы)	
подготовка к зачету	4
подготовка к экзамену	
другие виды самостоятельной работы студента	
Промежуточная аттестация в форме зачета	

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

Очная форма обучения

Наименование тем (разделов).	Количество академических или астрономических часов по видам учебных занятий			
	Занятия лекционного типа	З Практические занятия	Другие виды учебных занятий	Самостоятельная работа обучающихся
Тема 1. Понятие «персональные данные»	2	4		20
Тема 2. Правовые основы защиты персональных данных	2	2		20
Тема 3. Программные средства защиты персональной информации	2	4		22
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	2	2		20
Контроль самостоятельной работы студентов			2	
Индивидуальные консультации				
Подготовка к зачету				4
Групповые консультации				
ИТОГО	8	12	2	86

Тема 1. Понятие «персональные данные»

Понятие данные. Персональные данные как вид защищаемой информации. Понятие «персональные данные». Понятие и виды защищаемой информации в Российской Федерации Основные понятия служебной и конфиденциальной информации. Основные понятия коммерческой тайны. Конфиденциальная информация. Понятия «оператор Пдн», «персональные данные», «обработка ПДн». Цель и принципы обработки персональных данных.

Практическое занятие №1 Работа в программе Консультант Плюс. Изучение ФЗ № 152-ФЗ «О персональных данных»

Тема 2. Правовые основы защиты персональных данных

Нормативно-правовые документы, регламентирующие отношения в сфере работы с персональными данными. Предмет и задачи правового обеспечения защиты ПДн. Законодательство о безопасности и защите ПДн, его структура и содержание. Федеральный закон РФ №152 «О защите персональных данных». Правовые документы основных органов, регулирующие процесс обработки персональных данных. Требование к документации предприятия по защите персональных. Система обеспечения информационной безопасности Российской Федерации. Правовой механизм ограничения доступа к персональным данным. Ответственность за нарушения защиты персональных данных. Уголовная ответственность за разглашение персональных данных. Административная ответственность в сфере защиты персональных данных. Иные виды ответственности в сфере защиты персональных данных. Требование к документации юридических лиц по защите персональных данных.
Практическое занятие №2 Поиск правовых документов в программе Консультант Плюс.
Практическое занятие №3. Изучение ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Тема 3. Программные средства защиты персональной информации
Системы контроля, управления и разграничения доступа. Основные понятия о ключах, идентификаторах и блокирующих устройствах. Обзор средств криптографической защиты конфиденциальной информации. Основы электронной подписи. Понятие электронной подписи. Взаимосвязь между протоколами аутентификации и электронной подписи. Хэш - функция и ее использование в системах электронной подписи. Схемы ЭП. Подготовка рабочего места к работе с электронной подписью. Выработка и проверка электронной подписи. Установка и настройка совместной работы КриптоПро CSP, Rutoken, eToken. Требования к документации по обработке персональных данных работников. Типовые документы, регламентирующие получение, обработку, хранение и передачу персональных данных. Планирование мероприятий по защите персональных данных. Угрозы безопасности персональных данных. Классификация информационных систем ПДн.
Практическое занятие №4 Модели угроз безопасности персональных данных при их обработке в информационных системах

Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных
Классификация и характеристика технических каналов перехвата информации при ее передаче по каналам связи. Средства перехвата телефонных разговоров. Средства перехвата факсимильных передач. Основы организации и обеспечения комплексной защиты персональных данных при их обработке в ИСПДн. Порядок создания и эксплуатации ИСПДн. Формулирование актуальных угроз ПДн в образовательной организации. Перечень возможных угроз персональным данным в образовательной организации. Уровни защищенности персональных данных в ОО. Ответственность за нарушения обработки ПДн в организациях. Система защиты ПДн в организациях. Работа с реестром операторов. Перечень нормативных правовых актов, непосредственно регулирующих проведение проверок Роскомнадзора
Практическое занятие №5 Порядок работы с персональными данными работника.
Практическое занятие №6 Планирование мероприятий по защите персональных данных.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Преподавание дисциплины предполагает использование следующего учебно-методического обеспечения.

Комплекта мультимедийных презентаций для лекционных занятий.

Теоретического курса и информационных приложений, размещенных в электронной образовательной среде MOODLe.

Комплекса тестовых заданий и заданий для практических занятий, размещенных в

электронной образовательной среде MOODLe.

Виды самостоятельной работы обучающихся: выполнение заданий на практические занятия, выполнение индивидуального проектного задания, тестирование.

При подготовке к занятиям и выполнении самостоятельной работы студентам доступны следующие учебно-методические ресурсы, перечисленные в п.7 рабочей программы, а также электронный учебный ресурс размещенный в среде электронного обучения ТГПУ им. Л.Н. Толстого (http://moodle.tsput.ru)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы представлен в таблице пункта 1 рабочей программы.

Формирование компетенции “ способностью использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4)” осуществляется в течение одного этапа освоения основной образовательной программы.

Первый этап формирования компетенции осуществляется в процессе освоения дисциплин «Информационная безопасность и защита персональных данных», «Правоведение» и «Технологии визуализации данных».

6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Дескриптор компетенций	Показатели оценивания	Критерии оценивания
Знания	понятия персональных данных и способов их защиты;	Отметка «зачтено» выставляется, если студент в целом за семестр набрал от 61 до 100 баллов (с учетом баллов, набранных на промежуточной аттестации (зачете)). Отметка «незачтено» выставляется, если студент в целом за семестр набрал менее 61 балла (с учетом баллов, набранных на промежуточной аттестации (зачете)).
Умения	осуществлять защиту персональных данных с использованием средств ИКТ;	
Навыки и опыт деятельности	использования основных технических и программных средств для защиты персональных данных на предприятии и в организациях.	

Критерии оценивания компетенций формируются на основе балльно-рейтинговой системы с помощью всего комплекса методических материалов, определяющих процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих данный этап формирования компетенций.

Баллы,	Баллы за	Общая сумма	Отметка

набранные студентом в течение семестра	промежуточную аттестацию (зачет)	баллов за модуль в семестр	
21 – 60	0 – 40	61-100	Зачтено
0 – 20	0 – 40	0 – 60	Не зачтено

Оценка «*зачтено*» ставится, если студент освоил программный материал всех разделов, последователен в изложении программного материала, достаточно последовательно и логически стройно его излагает, умеет увязывать теорию с практикой, успешно прошел текущий контроль успеваемости по дисциплине, продемонстрировал индивидуальные знания, умениями и навыки практической работы.

Оценка «*не зачтено*» ставится, если студент не знает значительной части программного материала, допускает существенные ошибки, непоследователен в его изложении, не прошел текущий контроль успеваемости, не в полной мере владеет необходимыми знаниями, умениями и навыками при выполнении практических заданий, то есть студент не может продолжить обучение без дополнительной подготовки по соответствующей дисциплине.

6.3. 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

Образцы заданий к практическим занятиям:

Задание 1. Найдите в Интернете и сохраните в свою папку Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию". В Законе сформулировано понятие «информационная безопасность детей», а также виды информации, распространение которой среди детей определенных возрастных категорий ограничено. Данный материал необходимо оформить в виде отчета.

Задание 2. Найдите в Интернете в законодательных актах понятие авторского права. Приведите примеры ответственности за нарушение авторских прав.

Задание 3. Что такое Институт онлайновой безопасности семьи (Family Online Safety Institute) и какие рекомендации он дает.

Задание 4. Найдите в Интернете понятие «сетевая культура». Укажите источники найденной информации

Задание 5. Перечислите к какой ответственности (уголовной и административной) за нарушения в информационной сфере могут привлечь гражданина Российской Федерации.

Задание 6. Найдите и сохраните в свою папку «Национальную стратегию действий в интересах детей на 2012 - 2017 годы». Ознакомьтесь с мерами, направленными на обеспечение информационной безопасности детства, представьте их в отчете.

Вопросы к зачету:

1. Правовое и нормативное обеспечение защиты ПДн.
2. Назначение и средства антивирусной защиты.
3. Категории ПДн.
4. Назначение и средства идентификации и аутентификации субъектов.
5. Контролирующие органы в области ПДн, их функции.
6. Назначение и способы ограничения программной среды.
7. Мероприятия по обеспечению защиты ПДн при их обработке в информационных системах ПДн.
8. Согласие субъекта на обработку ПДн.
9. Назначение и способы физической защиты технических средств компьютерной системы.
10. Документы, предусмотренные постановлением Правительства 211, вид и краткое содержание.

11. Назначение и способы обеспечения доступности персональных данных.

12. Назначение выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них.

13. Условия обработки персональных данных.

14. Назначение средств обнаружения (предотвращения) вторжений.

15. Модель угроз ИСПДн. Методика разработки.

16. Назначение и способы управление доступом субъектов доступа к объектам доступа.

17. Классификация информационных систем.

18. Назначение и способы обеспечение целостности информационной системы и персональных данных.

19. Определение уровня защищенности ПДн.

20. Назначение средств контроля (анализа) защищенности персональных данных.

21. Аттестация ОИ, имеющего в своем составе ИСПДн.

22. Назначение и средства регистрация событий безопасности (аудит).

23. Контроль и надзор за выполнением требований по обеспечению безопасности ПДн.

Индивидуальное проектное задание удовлетворяющее системе требований:

План, по которому следует действовать при создании мультимедийного продукта с помощью программных средств.

I этап - выбор темы и описание проблемы;

II этап - анализ объекта;

III этап - разработка сценария и синтез модели;

IV этап - форма представления информации и выбор программных продуктов;

V этап - синтез компьютерной модели объекта

Процесс создания мультимедийного продукта

Процесс создания мультимедиа-информационных систем может рассматриваться как состоящий из двух основных фаз:

- **фазы проектирования**
- **фазы реализации**

Фаза проектирования

1. Проектирование концептуальной модели сценария для мультимедиа-информационной системы.
2. Проектирование медиа-зависимых представлений информации.
3. Проектирование информационных структур.

Фаза реализации

Реализация должна сопровождаться инструментами и методами создания.

1. Первичная интеграция
   a) Создание фрагментов
   b) Создание структуры

Полная интеграция мультимедиа-продукта монтаж, т.е. соединение всех элементов в единый продукт, в соответствии с определенной структурой и заданными средствами навигации. Производство мультимедиа-продукта (определяется носителем)

Рекомендации по оценке проектов

Вопросы	Да	Нет
Содержание учебного материала точно (вся фактическая информация и иллюстративный материал не содержат ошибок) Замечания _____		

Учебный материал полон (исчерпывающе покрывает изучаемую область) Замечания _____		
Содержание учебного материала современно (нет элементов, которые не отвечают современным требованиям) Замечания _____		
Деятельность обучаемых улучшится, если они освоят предложенный материал Замечания _____		

Требования к проекту

Количественная оценка проекта							
Выполненные работы							
Оцениваемые составляющие проекта	Электронный текст	Электронные таблицы	Презентация, Буклет	Сетевые технологии	Содержание	Дизайн проекта	Итого
Баллы	1	2	3	4	5	5	20
Название проекта							
Автор							

Требования к электронному тексту:

1. Текст состоит из трех частей, объеденных одной темой (10-20 страниц): текст, набранный с клавиатуры; текст, найденный в Интернете; сканированный текст.
2. Параметры страницы: Верхнее поле – 2, Нижнее поле – 2, Левое – 3, Правое – 1.
3. Параметры абзаца: Первая строка – 1,25, Интервал – 1,5; Выравнивание по ширине.
4. Параметры шрифта: Обычный, Times New Roman; размер 14
5. Текст должен содержать заголовки
6. Текст содержит: 5-7 рисунков с различным расположением в тексте; формулы; таблицу; список
7. Автоматически создано оглавление, расставлены номера страниц вверху по центру, оформлен титульный лист.
8. Создан список используемой литературы, оформленный по правилам с указанием адресов сайтов; на каждый источник в тексте должна иметься ссылка, оформленная в виде числа в квадратных скобках, соответствующему номеру в списке.
9. Текст может содержать сноски и колонтитулы.

Требования к презентациям:

1. Презентация содержит 8-15 слайдов.
2. Использованы различные виды разметки слайдов
3. Текст на слайдах должен содержать не больше 250 символов, размер шрифта не менее 26 пунктов, сплошной текст выровнен по ширине. Текст на слайдах не должен содержать орфографических и синтаксических ошибок.
4. Слайды содержат рисунки, подходящие по смыслу теме презентации и тексту слайда
5. На слайдах расположены управляющие кнопки.

6. К объектам на слайдах применены эффекты анимации
7. На отдельном слайде создан список используемой литературы, оформленный по правилам с указанием адресов сайтов.

Темы индивидуальных проектов

1. Биометрические системы аутентификации. Статические и динамические методы. Дактилоскопия по фотографиям рук; распознавание по сетчатке глаза и (или) по 13 радужной оболочке по фотографиям глаз; распознавание по геометрии лица по фотографиям лиц.
2. Хранение и обработка персональных медицинских данных. Особенности защиты персональных данных в медицинской отрасли. Защита врачебной тайны.
3. Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.
4. Стандарт OpenId. Аутентификация и авторизация через открытый протокол OAuth. Безопасность при аутентификации и авторизации на сайтах по OpenID.
5. Государственные информационные системы (ГИС). Проблемы классификации ГИС. Аспекты классификации государственных информационных систем с точки зрения Федеральных законов №149 и №242.
6. Трансграничная передача ПДн. Ответственность за нарушение правил трансграничной передачи. "Адекватная" защита прав субъектов персональных данных.
7. Законность видеосъемки, фотосъемки и звукозаписи в общественных местах. Охрана изображения гражданина. Нарушение неприкосновенности частной жизни. Статья 137 УК РФ, статьи 151, 152, 152.1 Гражданского Кодекса РФ.
8. Уничтожение электронных данных. Уровни уничтожения электронных данных (очистка, очищение, разрушение). Стандартизация уничтожения электронных данных.
9. Хранение ПДн в «облаке». Необходимые свойства «облака» для построения «облачной» ИСПДн. Требования регулирующих органов по защите ИСПДн в «облаке».
10. Защита персональных данных в мобильных устройствах. Проблемы приватности данных, хранящихся на мобильных устройствах. Защитные механизмы мобильных операционных систем и приложений

Примеры тестовых заданий

Примерный тест: «Безопасный интернет для детей и подростков»

1. Возможностью анализа изображений Интернета обладает модуль, входящий в состав следующего антивируса:
   - BitDefender Internet Security
   - McAfree Internet Security
   - F-Secure Internet Security
   - Dr. Web Security Space
2. Функцией ограничения доступа к жестким дискам и папкам на компьютере **не** обладает программа родительского контроля:
   - Kaspersky Internet Security
   - F-Secure Internet Security
   - Dr. Web Security Space
   - BitDefender Internet Security

3. Возможностью анализа изображений Интернета обладает модуль, входящий в состав следующего антивируса:
   - Подзарядка
   - StaffCop Home Edition
   - KidsControl
   - Time Boss
4. Расположите Интернет-угрозы для детей и подростков, начиная с наименьшей:
   - Неконтролируемые покупки
   - Доступ к «нежелательному контенту»
   - Контакты с незнакомцами с помощью интернет-сервисов
   - Сайты знакомств
5. Программы родительского контроля могут быть реализованы в виде:
   - Самостоятельных программ
   - В составе операционных систем
   - Средствами поисковых систем
   - Входящих в состав антивирусов модулей
6. Возможностью устанавливать системные ограничения обладает программа родительского контроля
   - КиберМама
   - KidsControl
   - Time Boss
   - Подзарядка
7. Выделяют следующие направления воспитательной работы по формированию информационной культуры учащихся:
   - Работа с городской администрацией
   - Работа с педагогическим коллективом
   - Работа с учащимися
   - Работа с родителями
8. Подсистема информационной обучающей системы для своевременного формирования и выдачи достоверной информации это…
   - Математическое обеспечение
   - Программное обеспечение
   - Информационное обеспечение
   - Организационное обеспечение
9. Возможностью блокировки рекламных баннеров на сайтах обладает программа родительского контроля:
   - КиберМама
   - KidsControl
   - Winadmin
   - Ворчун
10. В каких ОС семейства Windows реализована встроенная система контроля доступа (родительский контроль UAC)?
    - Windows NT 4

- Windows Vista
- Windows 2000
- Windows 7

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

Процедура промежуточной аттестации проходит в соответствии с Положением о текущем контроле и промежуточной аттестации студентов ТГПУ им. Л.Н. Толстого.

Описание балльно-рейтинговой системы по дисциплине.

Составляющие итоговой оценки за дисциплину:

1) Текущий контроль (общий вес 80 баллов):

до 4 баллов - посещение лекций;

до 26 баллов – выполнение заданий в LMS Moodle;

до 50 баллов - выполнение практических работ, индивидуальных заданий, самостоятельная работа)

2) Итоговый контроль заключается в проведении зачета (общий вес - 20 баллов): тестирования, защиты проектов. Зачет по желанию студентов может быть проведен в форме публичной защиты проектов по темам курса. К созданию проектов допускаются студенты, успешно прошедшие аттестацию.

Перевод процентов в академические оценки производится после суммирования процентов текущего и итогового контроля. При этом, для получения положительной итоговой оценки на зачете необходимо получить не менее 50% по каждой составляющей и выполнить все лабораторные работы. Шкала перевода баллов в оценку: до 40 - «не зачтено»; 41 - 100 - «зачтено».

Итоговая рейтинговая оценка по дисциплине складывается из следующих составляющих:

1) За каждый укрупненный блок тем студент может максимально получить количество баллов, указанное в следующей таблице:

	Max балл
Учебная работа	
Тема 1. Понятие «персональные данные»	10
Тема 2. Правовые основы защиты персональных данных	10
Тема 3. Программные средства защиты персональной информации	20
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	20
Контроль самостоятельной работы и выполнение заданий в LMS Moodle в форме тестировани	20
Зачет	20
Итого	100

2) Обязательной формой текущей аттестации знаний является тестирование. Максимальная оценка на тестировании может составить 10 баллов.

3) На зачете ответ студента может быть максимально оценен в 30 баллов. Из них 10 баллов могут быть получены на тестировании и 10 баллов за защиту индивидуального проекта.

1. Оценочная таблица

Место контроля в структуре дисциплины	**Форма контроля**	**Используемый критерий оценивания**		**Максимальный балл** *(исходя из весового коэффициента)*
Тема 1. Понятие «персональные данные»	Опрос индивидуальное задание	Критерий оценивания 1 Критерий оценивания 4	5 5	10
Тема 2. Правовые основы защиты персональных данных	индивидуальное задание	Критерий оценивания 4	10	10
Тема 3. Программные средства защиты персональной информации	Опрос индивидуальное задание	Критерий оценивания 2 Критерий оценивания 3	5 5	20
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	Опрос индивидуальное задание	Критерий оценивания 3 Критерий оценивания 4	10 10	20
Контроль самостоятельной работы студентов	Контрольная работа Выполнение заданий в LMS Moodle	Критерий оценивания 3 Критерий оценивания 4	10 10	20
Промежуточная аттестация	Зачет	Критерий оценивания 1 Критерий оценивания 2 Критерий оценивания 3 Критерий оценивания 4	5 5 10 10	20
Итого:				100

3. Сводная таблица учета результатов обучения по каждому студенту в процессе освоения дисциплины

4. Уровень сформированности компетенций определяется с помощью оценочной карты сформированности компетенций по дисциплине, представленной в приложении 1.

	Max балл	Иванов И. И.
Учебная работа		
Тема 1. Понятие «персональные данные»	10	3
Тема 2. Правовые основы защиты персональных данных	10	6
Тема 3. Программные средства защиты персональной информации	10	7
Тема 4. Технические средства защиты и комплексное	20	5

обеспечение безопасности персональных данных		
Контроль самостоятельной работы студентов	20	7
Зачет	30	23
Итого	100	70

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

7.1. Основная литература

основная литература:

1. Богатырева Ю.И. Информационная безопасность. Учебно–методическое пособие для студентов, обучающихся по направлению 050100 «Педагогическое образование» /Ю.И. Богатырева. – Тула: ТГПУ им. Л.Н. Толстого, 2014. – Электрон. изд. – 1 электрон. оптич. диск (CD–ROM). – № гос. регистрации 0321400675 – № рег. свид. ФГУП НТЦ «Информрегистр» 35205 от 12.03.2014.

2. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - 5-е изд., стер. - М : Академия, 2011. - 336 с. - ISBN 9785769577383

б) дополнительная литература:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-Ф.3 // Собрание законодательства РФ. 2006. №31. Ст. 3448.
2. Доктрина информационной безопасности РФ. Совм. Изд. Ред. «Российская газета» Международной академии информатизации. –М.: Информациология, 2000.
3. Закон РФ «О безопасности» от 05.03.1992 №2446-1 (ред.02.03.2007) // Ведомости Верховного Совета РФ. 1992. №15. Ст. 769.
4. Мельников, В.П. Информационная безопасность и защита информации: Учеб. пособ.для студ.вузов /В.П.Мельников, С.А.Клейменов, А.М.Петраков.-5-е изд., стер .- М: Академия, 2011. - 336 с.
5. Куприянов, А.И. Основы защиты информации: учебное пособие для студентов вузов / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов .-3-е изд. М.: Академия, 2008. – 256 с.
6. Анин, Б. Защита компьютерной информации. – С.-Петербург: Изд-во БХВ, 2009. – 354 с.
7. Барсуков В.С., Водолазский В.В. Современные технологии безопасности. Интегральный подход. - М.: Изд-во «НОЛИДЖ», 2010 – 244 с.
8. Мамаев, М., Петренко, С. Технологии защиты информации в Интернете [текст]: / М. Мамаев, С. Петренко.- Санкт-Петрбург, Изд-во «ПИТЕР». Москва-Харьков-Минск. 2009 – 272с.
9. Расторгуев, С.П. Основы информационной безопасности: учеб.пособ. для студ.вузов / С.П. Расторгуев. - М: Академия, 2007. - 192с.
10. Соколов, А.В., Степанюк, О.М., Методы информационной защиты объектов и компьютерных сетей [текст]: / А.В. Соколов, О.М. Степанюк.-М.: ООО “Фирма “Издательство АСТ” – 300с.

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. **http://www.google.ru/, http://www.yandex.ru/ , http://www.rambler.ru/ - поисковые системы**
2. http://www.edu.ru – портал Министерства образования и науки РФ

3. http://www.ict.edu.ru – система федеральных образовательных порталов «ИКТ в образовании»
4. http://www.openet.ru - Российский портал открытого образования
5. http://www.tspu.tula.ru – сайт ГОУ ВПО ТГПУ им. Л.Н. Толстого
6. http://www.mon.gov.ru - Министерство образования и науки Российской Федерации
7. http://www.fasi.gov.ru - Федеральное агентство по науке и инновациям
8. http://www.informika.ru - Государственный научно-исследовательский институт информационных технологий и телекоммуникаций (ГНИЙ ИТТ "Информика")
9. http://ege.edu.ru - Портал информационной поддержки Единого государственного экзамена
10. http://periodika.websib.ru - Педагогическая периодика: каталог статей российской образовательной прессы
11. http://www.wikibooks.org/wiki/Информационные_технологии – Викиучебник «Информационные технологии»
12. http://www.alleng.ru – Образовательные ресурсы Интернета школьникам и студентам
13. http://www.knigafund.ru – Электронная библиотечная система «Книгафонд»
14. http://www.planeta-it.ru – Образовательный проект по созданию анимационных и графических работ

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с учебной программой, учебной, научной и методической литературой, имеющейся в библиотеке университета, встретиться с преподавателем, ведущим дисциплину, получить в библиотеке рекомендованные учебники и учебно-методические пособия, осуществить запись на соответствующий курс в среде электронного обучения университета.

Глубина усвоения дисциплины зависит от активной и систематической работы студента на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

На лекциях важно сосредоточить внимание на ее содержании. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине. Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы. Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности студентов.

Прочное усвоение и долговременное закрепление учебного материала невозможно без продуманной самостоятельной работы. Такая работа требует от студента значительных усилий, творчества и высокой организованности. В ходе самостоятельной работы студенты выполняют следующие задачи: дорабатывают лекции, изучают рекомендованную литературу, готовятся к практическим занятиям, к коллоквиуму, контрольным работам по отдельным темам дисциплины. При этом эффективность учебной деятельности студента во многом зависит от того, как он распорядился выделенным для самостоятельной работы бюджетом времени.

Результатом самостоятельной работы является прочное усвоение материалов по предмету согласно программы дисциплины. В итоге этой работы формируются профессиональные умения

и компетенции, развивается творческий подход к решению возникших в ходе учебной деятельности проблемных задач, появляется самостоятельности мышления.

Целью практических занятий по данной дисциплине является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации: изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т. д.; при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа студента под управлением преподавателя. На них пополняются теоретические знания студентов, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение студентов к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы. После подведения итогов занятия студент обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

Преподавание дисциплины должно включать в себя следующие образовательные технологии:

1) Проведение лекций с использованием презентаций на основе мультимедийных технологий;
2) Обеспечение студентов сопутствующими материалами, размещенными среде Moodle;

Примерная тематика практических занятий по дисциплине.

Полные варианты практических занятий размещены в в системе управления обучением MOODLE.

№	Наименование практических занятий	Объем в часах
1	Правовые аспекты ИБ	2
2	Безопасность и конфиденциальность в Интернете	2
3	ПО для защиты информации	4
4	Основные принципы стенографии, кодирования и шифрования.	4
	Итого	12

Типовые задания для самостоятельной работы по дисциплине

Задание 1. Установите на ваш компьютер один сетевой экран и опишите его по следующей схеме:

1. Название брандмауэра
2. Производитель
3. Системные требования для установки
4. Основное назначение
5. Скриншоты установленной программы и ее основных функций
6. Дополнительные возможности

Задание 2. Опишите не менее 5 программ для фильтрации контента, информацию оформите в виде таблицы:

№ п/п	**Название программы**	**Адрес для скачивания**	**Основное назначение**	**Методы фильтрации**

Задание 3. Перечислите известные вам программы анти-шпионы, представьте подробное описание одной из них.

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

Материально-техническое обеспечение дисциплины:

1. Специально оборудованные аудитории и компьютерные классы: персональные компьютеры (модели: Intel Pentium4, AMD Athlon, AMD Duron), мультимедийные проекторы, аудиовизуальные устройства;
2. Программное обеспечение в соответствии с программой курса;
3. Методические пособия и литература в библиотеке университета и на кафедре.
4. Студентам обеспечен доступ к сети Internet.

Перечень лицензионного программного обеспечения, используемого при освоении дисциплины:

1. Подписка Microsoft DreamSpark Premium - Сублицензионный договор № S-2042626/M18 от 04.06.2013:
   - 1.1. Средства для разработки и проектирования Visual Studio 2008, 2010, 2012 и 2013 Professional Editions;
   - 1.2. Операционная система Windows 7 Professional;
   - 1.3. Операционная система Windows 8 Pro;
   - 1.4. Операционная система Windows 8.1 Pro;
   - 1.5. Отдельные программы из Office 2007, Office 2010, Office 2013 (в том числе Access, Visio, Project и др.);
2. Свободное программное обеспечение по лицензии GNU
   - 2.1. Debian Linux Weezy
   - 2.2. Apache Web Server
   - 2.3. MySQL
   - 2.4. PHP 5.0
   - 2.5. Domain Technologie Control Контрольная панель локального хостинга

У обучающихся имеется доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин и подлежит ежегодному обновлению:

1. Компьютерная информационно-правовая система «Гарант» - регистрационный номер клиента 71-70685-000033.
2. Официальный интернет-портал правовой информации http://pravo.gov.ru.
3. Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.
4. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц. URL: http://www.mathnet.ru
5. ИКТ [Электронный ресурс] : федеральный образовательный портал / ФГАУ ГНИИ ИТТ "Информика". - М. : [б. и.], 2003. - Загл. с титул. экрана. - Б. ц. URL: http://www.ict.edu.ru
6. Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: www.biblioclub.ru

7. Универсальные базы данных East View [Электронный ресурс] : информационный ресурс / East View Information Services. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц. URL: www.ebiblioteka.ru
8. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : информационный портал / ООО "РУНЭБ" ; Санкт-Петербургский государственный университет. - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. ц. URL: www.eLibrary.ru

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1. Учебные аудитории для проведения занятий лекционного типа, оборудованные мультимедийными средствами обучения.
2. Учебные аудитории для проведения практических занятий.
3. Компьютерные классы с доступом в интернет для работы с информационно-правовыми системами, в том числе «Гарант» и с доступом к электронно-библиотечной системе.
4. Аудитории для самостоятельной работы студентов, оснащенные компьютерной техникой, имеющей доступ к информационно-телекоммуникационной сети «Интернет», электронной информационно-образовательной среде ТГПУ им. Л.Н. Толстого, внутривузовскому сетевому окружению.

12. АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ.

1.Планируемые результаты обучения при освоении дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины у студента должна быть сформирована следующая компетенция: способностью использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4).

В результате освоения дисциплины студент должен приобрести:

знания понятия персональных данных и способов их защиты;

умения осуществлять защиту персональных данных с использованием средств ИКТ;

навыки использования основных технических и программных средств для защиты персональных данных на предприятии и в организациях.

2.Место дисциплины в структуре ОПОП.

Дисциплина «Информационные технологии в защите персональных данных» относится к дисциплинам по выбору вариативной части образовательной программы. Изучение данной дисциплины осуществляется в 7 семестре.

3.Объем дисциплины: 3 зачетные единицы.

4.Образовательный процесс осуществляется на русском языке.

5.Разработчик: Богатырева Ю.И., д.п.н., профессор кафедры ИиИТ.

13. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1) Внесены изменения в п.7 «Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины».

2) Обновлен п.10 «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем» на основании действующих лицензионных соглашений

Заведующий кафедрой ИиИТ _____А.В. Якушин

«26» августа 2016 г..

Программа составлена в соответствии с требованиями ФГОС ВО.

Разработчик (и):

Фамилия, имя, отчество	**Учёная степень**	**Учёное звание**	**Должность**	**Дата разработки**	**Подпись**
Богатырева Юлия Игоревна	д.п.н	доцент	профессор кафедры И и ИТ		

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Информационные технологии в защите персональных данных»

Состав:

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Планируемые результаты освоения образовательной программы (код и название компетенции)	**Планируемые результаты обучения**	**Этапы формирования компетенции в процессе освоения образовательной программы**
способностью использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4)	**Выпускник знает:** понятие персональных данных и способы их защиты; **умеет:** осуществлять защиту персональных данных с использованием средств ИКТ; **владеет:** использования основных технических и программных средств для защиты персональных данных на предприятии и в организациях.	1 этап из 1 (7 семестр)

Формирование компетенции “ способностью использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4)” осуществляется в течение одного этапа освоения основной образовательной программы.

Первый этап формирования компетенции осуществляется в процессе освоения дисциплин «Информационная безопасность и защита персональных данных», «Правоведение» и «Технологии визуализации данных».

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Дескриптор компетенций	**Показатели оценивания**	**Критерии оценивания**
Знания	понятия персональных данных и способов их защиты;	Отметка «зачтено» выставляется, если студент в целом за семестр набрал от 61 до 100 баллов (с учетом баллов, набранных на промежуточной аттестации (зачете)). Отметка «незачтено» выставляется, если студент в целом за семестр набрал менее 61 балла (с учетом баллов, набранных на промежуточной аттестации (зачете)).
Умения	осуществлять защиту персональных данных с использованием средств ИКТ;	
Навыки и опыт деятельности	использования основных технических и программных средств для защиты персональных данных на предприятии и в организациях.	

Критерии оценивания компетенций формируются на основе балльно-рейтинговой системы с помощью всего комплекса методических материалов, определяющих процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих данный этап формирования компетенций.

Баллы, набранные студентом в течение семестра	Баллы за промежуточную аттестацию (зачет)	Общая сумма баллов за модуль в семестр	Отметка
21 – 60	0 – 40	61-100	Зачтено
0 – 20	0 – 40	0 – 60	Не зачтено

3. КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

.

3.1. Вопросы к зачету

Вопросы к зачету

Правовое и нормативное обеспечение защиты ПДн.

2. Назначение и средства антивирусной защиты.

3. Категории ПДн.

4. Назначение и средства идентификации и аутентификации субъектов.

5. Контролирующие органы в области ПДн, их функции.

6. Назначение и способы ограничения программной среды.

7. Мероприятия по обеспечению защиты ПДн при их обработке в информационных системах ПДн.

8. Согласие субъекта на обработку ПДн.

9. Назначение и способы физической защиты технических средств компьютерной системы.

10. Документы, предусмотренные постановлением Правительства 211, вид и краткое содержание.

11. Назначение и способы обеспечения доступности персональных данных.

12. Назначение выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них.

13. Условия обработки персональных данных.

14. Назначение средств обнаружения (предотвращения) вторжений.

15. Модель угроз ИСПДн. Методика разработки.

16. Назначение и способы управление доступом субъектов доступа к объектам доступа.

17. Классификация информационных систем.

18. Назначение и способы обеспечение целостности информационной системы и персональных данных.

19. Определение уровня защищенности ПДн.

20. Назначение средств контроля (анализа) защищенности персональных данных.

21. Аттестация ОИ, имеющего в своем составе ИСПДн.

22. Назначение и средства регистрация событий безопасности (аудит).

23. Контроль и надзор за выполнением требований по обеспечению безопасности ПДн.

Критерии оценки зачета по дисциплине

Оценка «*зачтено*» ставится, если студент освоил программный материал всех разделов, последователен в изложении программного материала, достаточно последовательно и логически стройно его излагает, умеет увязывать теорию с практикой, успешно прошел текущий контроль

успеваемости по дисциплине, продемонстрировал индивидуальные знания, умениями и навыки практической работы.

Оценка «*не зачтено*» ставится, если студент не знает значительной части программного материала, допускает существенные ошибки, непоследователен в его изложении, не прошел текущий контроль успеваемости, не в полной мере владеет необходимыми знаниями, умениями и навыками при выполнении практических заданий, то есть студент не может продолжить обучение без дополнительной подготовки по соответствующей дисциплине.

3.2. Тестовые задания

3.2.1. Банк вопросов

1. Основные угрозы доступности информации:

•непреднамеренные ошибки пользователей

•злонамеренное изменение данных

•хакерская атака

•отказ программного и аппаратно обеспечения

•перехват данных

2. Основные угрозы доступности информации:

•непреднамеренные ошибки пользователей

•злонамеренное изменение данных

•хакерская атака

•отказ программного и аппаратно обеспечения

•перехват данных

3. При магнитостатическом экранировании заземление экрана не влияет на эффективность магнитостатического экранирования.

•Нет, эффективность уменьшается

•Да

4. Сигнал с равномерной спектральной плотностью на всех частотах и дисперсией, равной бесконечности можно охарактеризовать как:

•белый шум

•розовый шум

•черный шум

•зеленый шум

•синий шум

5. SYN-атака – это пример …

•DoS-атаки

•Переполнения буфера (buffer overflow)

•Подмены или спуфинга (spoofing)

•Перехвата соединения (hijacking)

•Повторной передачи (replay)

6. Антивирусные базы можно обновить на компьютере, не подключенном к Интернет.

• да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы

•да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором

•нет

7. Антивирусные базы можно обновить на компьютере, не подключенном к Интернет.

• да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы

•да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором

•нет

8. Антиспамовая программа, установленная на домашнем компьютере, служит для …

•корректной установки и удаления прикладных программ

•обеспечения регулярной доставки антивирусной программе новых антивирусных баз

•защиты компьютера от хакерских атак

•защиты компьютера от нежелательной и/или не запрошенной корреспонденции

9. Антиспамовая программа, установленная на домашнем компьютере, служит для …

•корректной установки и удаления прикладных программ

•обеспечения регулярной доставки антивирусной программе новых антивирусных баз

•защиты компьютера от хакерских атак

•защиты компьютера от нежелательной и/или не запрошенной корреспонденции

10. Брандмауэр (firewall) – это программа, …

• которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил

•которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл подробную статистику сетевой активности

•на основе которой строится система кэширования загружаемых веб-страниц

•реализующая простейший антивирус для скриптов, использующихся в Интернет активных элементах

11. Брандмауэр (firewall) – это программа, …

• которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил

•которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл

подробную статистику сетевой активности

•на основе которой строится система кэширования загружаемых веб-страниц

•реализующая простейший антивирус для скриптов, использующихся в Интернет активных элементах

12. В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата техническими средствами разведки технические каналы утечки информации для телекоммуникационной информации можно разделить на:

•электромагнитные

•электростатические

•электрические

•магнитные

•параметрические

13. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …

• обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

• реализацию права на доступ к информации

• соблюдение норм международного права в сфере информационной безопасности

• выявление нарушителей и привлечение их к ответственности

• соблюдение конфиденциальности информации ограниченного доступа

• разработку методов и усовершенствование средств информационной безопасности

14. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …

• обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

• реализацию права на доступ к информации

• соблюдение норм международного права в сфере информационной безопасности

• выявление нарушителей и привлечение их к ответственности

• соблюдение конфиденциальности информации ограниченного доступа

• разработку методов и усовершенствование средств информационной безопасности

15. Виброизлучатели бывают:

•пьезоэлектрические

•магнитодинамические

•оптические

•телефонные

16. Вид действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – …

•активная угроза

• пассивная угроза

•кража

•модификация

•искажение

17. Вид действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – …

•активная угроза

• пассивная угроза

•кража

•модификация

•искажение

18. Вирус – это программа, способная…

• создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты, при этом дубликаты сохраняют способность к дальнейшему распространению

•нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети

•нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети: прямо или посредством других программ и/или приложения

•уничтожить диск компьютера

19. Вирус – это программа, способная…

• создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты, при этом дубликаты сохраняют способность к дальнейшему распространению

•нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети

•нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети: прямо или посредством других программ и/или приложения

•уничтожить диск компьютера

20. Выполнение вредоносной программой, относящейся к классическим утилитам дозвона, вызывает …

• явные проявления

•косвенные проявления

•материальные проявления

•скрытые проявления

21. Выполнение вредоносной программой, относящейся к классическим утилитам дозвона, вызывает …

• явные проявления

•косвенные проявления

•материальные проявления

•скрытые проявления

22. Главное преимущество встроенного в Microsoft Windows XP (с установленным Service Pack 2) брандмауэра по сравнению с устанавливаемыми отдельно персональными брандмауэрами

•более ясный и интуитивно понятный интерфейс

• отсутствие необходимости отдельно покупать его и устанавливать

•наличие более полного функционала

•возможность более точно задавать исключения

23. Главное преимущество встроенного в Microsoft Windows XP (с установленным Service Pack 2) брандмауэра по сравнению с устанавливаемыми отдельно персональными брандмауэрами

•более ясный и интуитивно понятный интерфейс

• отсутствие необходимости отдельно покупать его и устанавливать

•наличие более полного функционала

•возможность более точно задавать исключения

24. Деятельность клавиатурных шпионов

•находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают

•переписывает пароли туда, откуда их может без особого труда извлечь злоумышленник.

•находясь в оперативной памяти следят за вводимой информацией и как только пользователь введет кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором

•находясь в оперативной памяти следят за вводимой пользователем информацией и по команде злоумышленника производят нужную ему замену одних символов (или групп символов) другими

•передают злоумышленнику марку и тип используемой пользователем клавиатуры

25. Деятельность клавиатурных шпионов

•находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают

•переписывает пароли туда, откуда их может без особого труда извлечь злоумышленник.

•находясь в оперативной памяти следят за вводимой информацией и как только пользователь введет кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором

•находясь в оперативной памяти следят за вводимой пользователем информацией и по команде злоумышленника производят нужную ему замену одних символов (или групп символов) другими

•передают злоумышленнику марку и тип используемой пользователем клавиатуры

26. Дискретизация речи с последующим шифрованием для защиты речевых сообщений в телефонных каналах связи обеспечивает:

•неузнаваемость

•нечитабельность

•невоспроизводимость

•неразборчивость

27. Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется .... (1) зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС – .....(2) зашумление. Что пропущено?

•линейное, пространственное

•пространственное, линейное

28. Для перехвата информативного сигнала по виброакустическому каналу утечки используют:

•электронные стетоскопы

•устройства типа "электронное ухо"

•направленные микрофоны

•радиостетоскопы

•акустические сетевые закладные устройства

•портативные диктофоны

•акустические радиозакладные устройства

29. Задача, выполняющая модуль планирования, входящий в антивирусный комплекс

• настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.)

•определения параметров взаимодействия различных компонентов антивирусного комплекса

•определения областей работы различных задач поиска вирусов

•настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса

30. Задача, выполняющая модуль планирования, входящий в антивирусный комплекс

• настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.)

•определения параметров взаимодействия различных компонентов антивирусного комплекса

•определения областей работы различных задач поиска вирусов

•настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса

31. Защита информации обеспечивается применением антивирусных средств

• да

•нет

•не всегда

32. Защита информации обеспечивается применением антивирусных средств

• да

•нет

•не всегда

33. Злонамеренный код обладает следующими отличительными чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Назовите тип этого злонамеренного кода.

•Макровирус

•Троянский конь

•Червь

•Файловый вирус

34. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

• с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

•с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации

•способна противостоять только информационным угрозам, как внешним так и внутренним

•способна противостоять только внешним информационным угрозам

35. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

• с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

•с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации

•способна противостоять только информационным угрозам, как внешним так и внутренним

•способна противостоять только внешним информационным угрозам

36. Информация, составляющая государственную тайну не может иметь гриф…

• «для служебного пользования»

•«секретно»

•«совершенно секретно»

•«особой важности»

37. Информация, составляющая государственную тайну не может иметь гриф…

• «для служебного пользования»

•«секретно»

•«совершенно секретно»

•«особой важности»

38. Использование брандмауэров относят к …

•методам антивирусной защиты.

•теоретическим

•практическим

•организационным

• техническим

39. Использование брандмауэров относят к …

•методам антивирусной защиты.

•теоретическим

•практическим

•организационным

• техническим

40. К активным поисковым устройствам закладных устройств относятся:

•нелинейный локатор

•металлоискатель

•тепловизор

•ренгинометр

•детектор магнитного поля

•акустокорелятор

41. К какому типу Использование инструкций по работе за компьютером, введенные в отдельно взятом компьютерном классе, можно отнести к …

•методам антивирусной защиты

•теоретическим

•практическим

• организационным

•техническим

42. К какому типу Использование инструкций по работе за компьютером, введенные в отдельно взятом компьютерном классе, можно отнести к …

•методам антивирусной защиты

•теоретическим

•практическим

• организационным

•техническим

43. К классу условно опасных относятся программы …

• о которых нельзя однозначно сказать, что они вредоносны

•последствия выполнения которых нельзя предугадать

•которые можно выполнять только при наличии установленного антивирусного программного обеспечения

•характеризующиеся способностью при срабатывании заложенных в них условий выполнять какое-либо действие, например, удаление файлов, в остальное время они безвредны

44. К классу условно опасных относятся программы …

• о которых нельзя однозначно сказать, что они вредоносны

•последствия выполнения которых нельзя предугадать

•которые можно выполнять только при наличии установленного антивирусного программного обеспечения

•характеризующиеся способностью при срабатывании заложенных в них условий выполнять какое-либо действие, например, удаление файлов, в остальное время они безвредны

45. К среде распространения акустического сигнала по виброакустическому каналу утечки относятся:

•стены

•воздух

•трубы водоснабжения

•системы электропитания

•пол

46. К формам защиты информации не относится…

• аналитическая

• правовая

• организационная

• инженерно-техническая

• страховая

47. К формам защиты информации не относится…

• аналитическая

• правовая

• организационная

• инженерно-техническая

• страховая

48. Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?

•Организационное

•Организационно-техническое

•Техническо-организационное

•Техническое

49. Какие есть способы экранирования?

•Магнитостатическое

•Электростатическое

•Электрическое

•Статическое

•Магнитное

•Электромагнитное

50. Какие мероприятия с использованием пассивных технических средств позволяют закрывать каналы утечки информации (укажите все подходящие мероприятия)?

•Локализация излучений

•Пространственное зашумление

•Развязывание информационных сигналов

•Линейное зашумление

•Уничтожение закладных устройств

51. Какие пункты относятся к активным методам защиты речевой информации?

•создание маскирующих акустических и вибрационных помех

•выявление факта несанкционированного подключения к линии

•создание прицельных электромагнитных помех акустическим закладным устройствам

•выявление излучений акустических закладных устройств

•уничтожение средств несанкционированного подключения к телефонной линии

52. Какие пункты относятся к пространственному зашумлению?

•созданные помехи не должны иметь регулярной структуры

•уровень помехи должен превышать уровень всех остальных шумов

•помеха должна быть создана по горизонтальной и вертикальной составляющей

•ничего из названого

53. Какими бывают случайные антенны?

•Сосредоточенными

•Распределенными

•Видов не имеют

54. Какое свойство имеет случайная антенна?

•Способна принимать побочные электромагнитные излучения

•Способна отражать побочные электромагнитные излучения

•Способна создавать побочные электромагнитные излучения

55. Концепция системы защиты от информационного оружия не должна включать…

• средства нанесения контратаки с помощью информационного оружия

•механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры

•признаки, сигнализирующие о возможном нападении

•процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

56. Концепция системы защиты от информационного оружия не должна включать…

• средства нанесения контратаки с помощью информационного оружия

•механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры

•признаки, сигнализирующие о возможном нападении

•процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

57. Криптосистема обладает следующими чертами: предусматривает использование одного и того же закрытого ключа для шифрования и дешифрования данных, характеризуется высокой скоростью работы, но сложностью безопасной передачи самого этого закрытого ключа. Назовите тип криптосистемы.

•Асимметричная криптосистема

•Симметричная криптосистема

•Криптосистема, использующая инфраструктуру открытых ключей (PKI)

•Избыточная криптосистема

58. Логические бомбы относятся к классу …

•файловых вирусов

•макровирусов

•сетевых червей

• троянов

•условно опасных программ

59. Логические бомбы относятся к классу …

•файловых вирусов

•макровирусов

•сетевых червей

• троянов

•условно опасных программ

60. Методы повышения достоверности входных данных

• Замена процесса ввода значения процессом выбора значения из предлагаемого множества

• Отказ от использования данных

• Проведение комплекса регламентных работ

• Использование вместо ввода значения его считывание с машиночитаемого носителя

• Введение избыточности в документ первоисточник

• Многократный ввод данных и сличение введенных значений

61. Методы повышения достоверности входных данных

• Замена процесса ввода значения процессом выбора значения из предлагаемого множества

• Отказ от использования данных

• Проведение комплекса регламентных работ

• Использование вместо ввода значения его считывание с машиночитаемого носителя

• Введение избыточности в документ первоисточник

• Многократный ввод данных и сличение введенных значений

62. Можно ли использовать оптоволоконный кабель в качестве способа защиты линий связи от контактного несанкционированного доступа?

•Да

•Нет

63. На высоких частотах при больших размерах заземляемых устройств и значительных расстояниях между ними используется многоточечная система заземления

•Нет, одноточечная

•Да

•Нет, гибридная

64. Назовите стандарт, применяемый в проводных и беспроводных сетях, который обеспечивает безопасность на уровне порта, то есть обеспечивает доступ к порту коммутатора или беспроводной точки доступа только после предварительной аутентификации клиента.

•802.1x

•802.3u

•802.11g

•EAP-TLS

•WPA

65. Наиболее эффективное средство для защиты от сетевых атак

• использование сетевых экранов или «firewall»

•использование антивирусных программ

•посещение только «надёжных» Интернет-узлов

•использование только сертифицированных программ-броузеров при доступе к сети Интернет

66. Наиболее эффективное средство для защиты от сетевых атак

• использование сетевых экранов или «firewall»

•использование антивирусных программ

•посещение только «надёжных» Интернет-узлов

•использование только сертифицированных программ-броузеров при доступе к сети Интернет

67. Необходимость модуля обновления для любого современного антивирусного средства – для …

•доставки сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу

•взаимодействия антивирусной программы с сайтом компании-производителя

• подключения антивирусных баз к антивирусной программе

•обеспечения взаимодействия операционной системы с антивирусным комплексом

68. Необходимость модуля обновления для любого современного антивирусного средства – для …

•доставки сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу

•взаимодействия антивирусной программы с сайтом компании-производителя

• подключения антивирусных баз к антивирусной программе

•обеспечения взаимодействия операционной системы с антивирусным комплексом

69. Обязательные свойства любого современного антивирусного комплекса

• не мешать выполнению основных функций компьютера

• не занимать много системных ресурсов

• не занимать канал Интернет

• надежно защищать от вирусов

• быть кроссплатформенным (работать под управлением любой операционной системы)

• интегрироваться в браузер

70. Обязательные свойства любого современного антивирусного комплекса

• не мешать выполнению основных функций компьютера

• не занимать много системных ресурсов

• не занимать канал Интернет

• надежно защищать от вирусов

• быть кроссплатформенным (работать под управлением любой операционной системы)

• интегрироваться в браузер

71. Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет

• трудности с регулярным автоматическим получением новых антивирусных баз

•невозможность использовать антиспамовую программу в режиме реального времени

•ложные срабатывания в работе персонального брандмауэра

•невозможность запуска антивирусной проверки в режиме реального времени

72. Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет

• трудности с регулярным автоматическим получением новых антивирусных баз

•невозможность использовать антиспамовую программу в режиме реального времени

•ложные срабатывания в работе персонального брандмауэра

•невозможность запуска антивирусной проверки в режиме реального времени

73. Основная задача, которую решает антивирусная проверка в режиме реального времени

• обеспечение непрерывности антивирусной проверки

•обеспечение невмешательства в процесс деятельности других программ

•обеспечение взаимодействия между пользователем и антивирусной программой

•предоставление возможности глубокой проверки заданных объектов

74. Основная задача, которую решает антивирусная проверка в режиме реального времени

• обеспечение непрерывности антивирусной проверки

•обеспечение невмешательства в процесс деятельности других программ

•обеспечение взаимодействия между пользователем и антивирусной программой

•предоставление возможности глубокой проверки заданных объектов

75. Основной задачей экранирования электрических полей (при электростатическом экранировании) является снижение емкости связи между экранируемыми элементами конструкции.

•Да

•Нет, не снижение емкости связи, а увеличение

76. Основные угрозы конфиденциальности информации:

• карнавал

• переадресовка

• перехват данных

• блокирование

• злоупотребления полномочиями

77. Основные угрозы конфиденциальности информации:

• карнавал

• переадресовка

• перехват данных

• блокирование

• злоупотребления полномочиями

78. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

• несанкционированного управления удаленным компьютером

•внедрения агрессивного программного кода в рамках активных объектов Web-страниц

•перехвата или подмены данных на путях транспортировки

•вмешательства в личную жизнь

•поставки неприемлемого содержания

79. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

• несанкционированного управления удаленным компьютером

•внедрения агрессивного программного кода в рамках активных объектов Web-страниц

•перехвата или подмены данных на путях транспортировки

•вмешательства в личную жизнь

•поставки неприемлемого содержания

80. Подозрительная сетевая активность может быть вызвана …

• сетевым червем

• P2P-червем

• трояном

• логической бомбой

81. Подозрительная сетевая активность может быть вызвана …

• сетевым червем

• P2P-червем

• трояном

• логической бомбой

82. Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности:

• уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer

•уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer

•возможность установить отличную от www.msn.com стартовую страницу

•возможность одновременно работать в нескольких окнах

83. Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности:

• уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer

•уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer

•возможность установить отличную от www.msn.com стартовую страницу

•возможность одновременно работать в нескольких окнах

84. Преднамеренная угроза безопасности информации

• кража

•наводнение

•повреждение кабеля, по которому идет передача, в связи с погодными условиями

•ошибка разработчика

85. Преднамеренная угроза безопасности информации

• кража

•наводнение

•повреждение кабеля, по которому идет передача, в связи с погодными условиями

•ошибка разработчика

86. Преимущества сигнатурного метода антивирусной проверки над эвристическим

• более надежный

•существенно менее требователен к ресурсам

•не требует регулярного обновления антивирусных баз

•позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

87. Преимущества сигнатурного метода антивирусной проверки над эвристическим

• более надежный

•существенно менее требователен к ресурсам

•не требует регулярного обновления антивирусных баз

•позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

88. Преимущества эвристического метода антивирусной проверки над сигнатурным

• более надежный

• существенно менее требователен к ресурсам

• не требует регулярного обновления антивирусных баз

• позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

89. Преимущества эвристического метода антивирусной проверки над сигнатурным

• более надежный

• существенно менее требователен к ресурсам

• не требует регулярного обновления антивирусных баз

• позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

90. При магнитостатическом экранировании на низких частотах используют

•Коаксиальные кабели с двойной оплеткой (триаксиальные кабели)

•Коаксиальные кабели

•Витая пара, защищенная экранирующей оболочкой

91. При электростатическом экранировании в металлическом экране узкие щели и отверстия, размеры которых малы по сравнению с ..... (с чем ?), практически не ухудшают экранирование электрического поля.

•С размерами экрана

•С длиной волны

•С размерами экранируемого прибора

92. Разделы современной криптографии:

• Симметричные криптосистемы

• Криптосистемы с открытым ключом

• Криптосистемы с дублированием защиты

• Системы электронной подписи

• Управление паролями

• Управление передачей данных

• Управление ключами

93. Разделы современной криптографии:

• Симметричные криптосистемы

• Криптосистемы с открытым ключом

• Криптосистемы с дублированием защиты

• Системы электронной подписи

• Управление паролями

• Управление передачей данных

• Управление ключами

94. Свойство вируса, позволяющее называться ему загрузочным – способность …

• заражать загрузочные сектора жестких дисков

•заражать загрузочные дискеты и компакт-диски

•вызывать перезагрузку компьютера-жертвы

•подсвечивать кнопку Пуск на системном блоке

95. Свойство вируса, позволяющее называться ему загрузочным – способность …

• заражать загрузочные сектора жестких дисков

•заражать загрузочные дискеты и компакт-диски

•вызывать перезагрузку компьютера-жертвы

•подсвечивать кнопку Пуск на системном блоке

96. Сервисы безопасности:

• идентификация и аутентификация

• шифрование

• инверсия паролей

• контроль целостности

• регулирование конфликтов

• экранирование

• обеспечение безопасного восстановления

• кэширование записей

97. Сервисы безопасности:

• идентификация и аутентификация

• шифрование

• инверсия паролей

• контроль целостности

• регулирование конфликтов

• экранирование

• обеспечение безопасного восстановления

• кэширование записей

98. Скрытые проявлениям вирусного заражения:

• наличие на рабочем столе подозрительных ярлыков

• наличие в оперативной памяти подозрительных процессов

• наличие на компьютере подозрительных файлов

• подозрительная сетевая активность

• неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт

• неожиданное уведомление антивирусной программы об обнаружении вируса

99. Скрытые проявлениям вирусного заражения:

• наличие на рабочем столе подозрительных ярлыков

• наличие в оперативной памяти подозрительных процессов

• наличие на компьютере подозрительных файлов

• подозрительная сетевая активность

• неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт

• неожиданное уведомление антивирусной программы об обнаружении вируса

100. Средства защиты объектов файловой системы основаны на…

• определении прав пользователя на операции с файлами и каталогами

•задании атрибутов файлов и каталогов, независящих от прав пользователей

•определении допустимых операций с файлами и каталогами

•ограничении прав пользователя

101. Средства защиты объектов файловой системы основаны на…

• определении прав пользователя на операции с файлами и каталогами

•задании атрибутов файлов и каталогов, независящих от прав пользователей

•определении допустимых операций с файлами и каталогами

•ограничении прав пользователя

102. Стадии жизненного цикла классического трояна:

• проникновение на чужой компьютер

• активация

• поиск объектов для заражения

• подготовка копий

• внедрение копий

• выполнение вредоносных действий

103. Стадии жизненного цикла классического трояна:

• проникновение на чужой компьютер

• активация

• поиск объектов для заражения

• подготовка копий

• внедрение копий

• выполнение вредоносных действий

104. Суть компрометации информации

•внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

•несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

• внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

105. Суть компрометации информации

•внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

•несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

• внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

106. Типы методов антивирусной защиты

• теоретические

• практические

• организационные

• технические

• программные

107. Типы методов антивирусной защиты

• теоретические

• практические

• организационные

• технические

• программные

108. Типы троянов:

• клавиатурные шпионы

• похитители паролей

• дефрагментаторы дисков

• утилиты скрытого удаленного управления

• логические бомбы

• шутки

• вирусные мистификации

109. Типы троянов:

• клавиатурные шпионы

• похитители паролей

• дефрагментаторы дисков

• утилиты скрытого удаленного управления

• логические бомбы

• шутки

• вирусные мистификации

110. Трояны классифицируются по …

•методу размножения

•методу распространения

•методу маскировки

• типу вредоносной нагрузки

111. Трояны классифицируются по …

•методу размножения

•методу распространения

•методу маскировки

• типу вредоносной нагрузки

112. Увеличение толщины стенок экрана улучшает эффект экранирования. К какому типу экранирования это относится?

•электростатическому

•Магнитостатическому

•статическому

•всем видам экранирования

113. Устройство обеспечивает разрыв первичной и вторичной цепи по сигналам наводок. Что это за устройство?

•полосовой фильтр

•маскиратор

•фильтр-синтезатор

•разделяющий трансформатор

114. Утечка информации – это …

• это бесконтрольный выход конфиденциальной информации за пределы организации или

•круга лиц, которым она была доверена

•процесс раскрытия секретной информации

•процесс уничтожения информации

•непреднамеренная утрата носителя информации

115. Утечка информации – это …

• это бесконтрольный выход конфиденциальной информации за пределы организации или

•круга лиц, которым она была доверена

•процесс раскрытия секретной информации

•процесс уничтожения информации

•непреднамеренная утрата носителя информации

116. Чем отличается статический режим работы скремблера от динамического?

•статический предполагает работу с одним шифром, а динамический - нет

•в статичестом режиме скремблер функционирует строго отведенный промежуток времени, а при динамическом - имеет плавающий промежуток работы

•в статическом режиме не меняется ключ шифрования в течении сеанса связи

•в статическом режиме скремблер работает на одном канале связи, а в динамическом меняет каналы в соответствии с алгоритмом

117. Что должна включать в себя система заземления?

•Общий заземлитель

•Заземляющий кабель

•Шины и провода, соединяющие заземлитель с объектом

•Все вышеперечисленное

118. Что из перечисленного не относится к техническим мероприятиям с использованием активных средств?

•Пространственное зашумление

•Линейное зашумление

•Развязывание информационных сигналов

119. Что можно сказать о черном шуме?

•это тишина

•является практически невозможным

•спектр шума имеет нулевую энергию (возможны пики)

•ничего из вышеперечисленного

120. Что такое (опасная) зона 2?

•Зона, в которой возможны перехват (с помощью разведывательного приемника) побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации

•Зона, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков

•Зона, в пределах которой отношение “информационный сигнал/помеха” превышает допустимое нормированное значение

•Зона, в пределах которой отношение “информационный сигнал/помеха” не превышает допустимое нормированное значение

121. Что такое контролируемая зона?

•Зона, в которой возможно появление лиц и транспортных средств, не имеющих постоянных или временных пропусков

•Зона, в которой исключено появление только транспортных средств, не имеющих

постоянных или временных пропусков

•Зона, в которой исключено появление лиц и транспортных средств, имеющих только временные пропуска

•Зона, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков

122. Что такое местный эффект?

•прослушивание в телефонном аппарате звуков собственной речи

•прослушивание в телефонном аппарате шумов, идущих от распределительной коробки или АТС

•прослушивание в телефонном аппарате чужого разговора при поднятой трубке

•искажения речевого сигнала при изменении среды передачи

123. Что такое организационное мероприятие?

•Мероприятие по защите информации, проведение которого не требует применения специально разработанных технических средств

•Мероприятие по защите информации, которое проводит сама организация без привлечения сторонних лиц

•Мероприятие по защите информации, при проведении которого исследуется организация

124. Элементы знака охраны авторского права:

• буквы С в окружности или круглых скобках

• буквы Р в окружности или круглых скобках

• наименования (имени) правообладателя

• наименование охраняемого объекта

• года первого выпуска программы

125. Элементы знака охраны авторского права:

• буквы С в окружности или круглых скобках

• буквы Р в окружности или круглых скобках

• наименования (имени) правообладателя

• наименование охраняемого объекта

• года первого выпуска программы

3.2.2.Критерии оценки тестовых заданий

При тестировании число всех верных ответов берется за 100%.

Для оценки тестов применяется следующая методика баллов за данный вид работы:

Процент выполненных тестов умножается на максимальное количество баллов, определяемое бально-рейтинговой системой по дисциплине.

3.3. Индивидуальные проектные задания

Темы индивидуальных проектов

11. Биометрические системы аутентификации. Статические и динамические методы.

Дактилоскопия по фотографиям рук; распознавание по сетчатке глаза и (или) по 13 радужной оболочке по фотографиям глаз; распознавание по геометрии лица по фотографиям лиц.

12. Хранение и обработка персональных медицинских данных. Особенности защиты персональных данных в медицинской отрасли. Защита врачебной тайны.
13. Многофакторная аутентификация. Примеры многофакторной аутентификации. Протоколы аутентификации.
14. Стандарт OpenId. Аутентификация и авторизация через открытый протокол OAuth. Безопасность при аутентификации и авторизации на сайтах по OpenID.
15. Государственные информационные системы (ГИС). Проблемы классификации ГИС. Аспекты классификации государственных информационных систем с точки зрения Федеральных законов №149 и №242.
16. Трансграничная передача ПДн. Ответственность за нарушение правил трансграничной передачи. "Адекватная" защита прав субъектов персональных данных.
17. Законность видеосъемки, фотосъемки и звукозаписи в общественных местах. Охрана изображения гражданина. Нарушение неприкосновенности частной жизни. Статья 137 УК РФ, статьи 151, 152, 152.1 Гражданского Кодекса РФ.
18. Уничтожение электронных данных. Уровни уничтожения электронных данных (очистка, очищение, разрушение). Стандартизация уничтожения электронных данных.
19. Хранение ПДн в «облаке». Необходимые свойства «облака» для построения «облачной» ИСПДн. Требования регулирующих органов по защите ИСПДн в «облаке».
20. Защита персональных данных в мобильных устройствах. Проблемы приватности данных, хранящихся на мобильных устройствах. Защитные механизмы мобильных операционных систем и приложений

Требования к проекту

Количественная оценка проекта							
Выполненные работы							
Оцениваемые составляющие проекта	Электронный текст	Электронные таблицы	Презентация, Буклет	Сетевые технологии	Содержание	Дизайн проекта	Итого
Баллы	1	2	3	4	5	5	20
Название проекта							
Автор							

Требования к электронному тексту:

10. Текст состоит из трех частей, объеденных одной темой (10-20 страниц): текст, набранный с клавиатуры; текст, найденный в Интернете; сканированный текст.
11. Параметры страницы: Верхнее поле – 2, Нижнее поле – 2, Левое – 3, Правое – 1.
12. Параметры абзаца: Первая строка – 1,25, Интервал – 1,5; Выравнивание по ширине.
13. Параметры шрифта: Обычный, Times New Roman; размер 14
14. Текст должен содержать заголовки
15. Текст содержит: 5-7 рисунков с различным расположением в тексте; формулы; таблицу; список

16. Автоматически создано оглавление, расставлены номера страниц вверху по центру, оформлен титульный лист.
17. Создан список используемой литературы, оформленный по правилам с указанием адресов сайтов; на каждый источник в тексте должна иметься ссылка, оформленная в виде числа в квадратных скобках, соответствующему номеру в списке.
18. Текст может содержать сноски и колонтитулы.

Требования к презентациям:

8. Презентация содержит 8-15 слайдов.
9. Использованы различные виды разметки слайдов
10. Текст на слайдах должен содержать не больше 250 символов, размер шрифта не менее 26 пунктов, сплошной текст выровнен по ширине. Текст на слайдах не должен содержать орфографических и синтаксических ошибок.
11. Слайды содержат рисунки, подходящие по смыслу теме презентации и тексту слайда
12. На слайдах расположены управляющие кнопки.
13. К объектам на слайдах применены эффекты анимации
14. На отдельном слайде создан список используемой литературы, оформленный по правилам с указанием адресов сайтов.

Критерии оценки проектных заданий

Индивидуальное проектное задание удовлетворяющее системе требований:

План, по которому следует действовать при создании мультимедийного продукта с помощью программных средств.

I этап - выбор темы и описание проблемы;

II этап - анализ объекта;

III этап - разработка сценария и синтез модели;

IV этап - форма представления информации и выбор программных продуктов;

V этап - синтез компьютерной модели объекта

Процесс создания мультимедийного продукта

Процесс создания мультимедиа-информационных систем может рассматриваться как состоящий из двух основных фаз:

- **фазы проектирования**
- **фазы реализации**

Фаза проектирования

1. Проектирование концептуальной модели сценария для мультимедиа-информационной системы.
2. Проектирование медиа-зависимых представлений информации.
3. Проектирование информационных структур.

Фаза реализации

Реализация должна сопровождаться инструментами и методами создания.

2. Первичная интеграция
   a) Создание фрагментов
   b) Создание структуры

Полная интеграция мультимедиа-продукта монтаж, т.е. соединение всех элементов в единый продукт, в соответствии с определенной структурой и заданными средствами навигации. Производство мультимедиа-продукта (определяется носителем)

Рекомендации по оценке проектов

Вопросы	Да	Нет
Содержание учебного материала точно (вся фактическая информация и		

иллюстративный материал не содержат ошибок) Замечания _____		
Учебный материал полон (исчерпывающе покрывает изучаемую область) Замечания _____		
Содержание учебного материала современно (нет элементов, которые не отвечают современным требованиям) Замечания _____		
Деятельность обучаемых улучшится, если они освоят предложенный материал Замечания _____		

3.4. Содержание и типовые задания к практическим занятиям

Полные варианты практических занятий размещены в в системе управления обучением MOODLE.

№	Наименование практических занятий	Объем в часах
1	Правовые аспекты ИБ	2
2	Безопасность и конфиденциальность в Интернете	2
3	ПО для защиты информации	4
4	Основные принципы стенографии, кодирования и шифрования.	4
	Итого	12

Образцы заданий к практическим занятиям:

Задание 1. Найдите в Интернете и сохраните в свою папку Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию". В Законе сформулировано понятие «информационная безопасность детей», а также виды информации, распространение которой среди детей определенных возрастных категорий ограничено. Данный материал необходимо оформить в виде отчета.

Задание 2. Найдите в Интернете в законодательных актах понятие авторского права. Приведите примеры ответственности за нарушение авторских прав.

Задание 3. Что такое Институт онлайновой безопасности семьи (Family Online Safety Institute) и какие рекомендации он дает.

Задание 4. Найдите в Интернете понятие «сетевая культура». Укажите источники найденной информации

Задание 5. Перечислите к какой ответственности (уголовной и административной) за нарушения в информационной сфере могут привлечь гражданина Российской Федерации.

Задание 6. Найдите и сохраните в свою папку «Национальную стратегию действий в интересах детей на 2012 - 2017 годы». Ознакомьтесь с мерами, направленными на обеспечение информационной безопасности детства, представьте их в отчете.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

.

Описание балльно-рейтинговой системы по дисциплине.

Составляющие итоговой оценки за дисциплину:

1) Текущий контроль (общий вес 80 баллов):

до 4 баллов - посещение лекций;

до 26 баллов – выполнение заданий в LMS Moodle;

до 50 баллов - выполнение практических работ, индивидуальных заданий, самостоятельная работа)

2) Итоговый контроль заключается в проведении зачета (общий вес - 20 баллов): тестирования, защиты проектов. Зачет по желанию студентов может быть проведен в форме публичной защиты проектов по темам курса. К созданию проектов допускаются студенты, успешно прошедшие аттестацию.

Перевод процентов в академические оценки производится после суммирования процентов текущего и итогового контроля. При этом, для получения положительной итоговой оценки на зачете необходимо получить не менее 50% по каждой составляющей и выполнить все лабораторные работы. Шкала перевода баллов в оценку: до 40 - «не зачтено»; 41 - 100 - «зачтено».

Итоговая рейтинговая оценка по дисциплине складывается из следующих составляющих:

1) За каждый укрупненный блок тем студент может максимально получить количество баллов, указанное в следующей таблице:

	Max балл
Учебная работа	
Тема 1. Понятие «персональные данные»	10
Тема 2. Правовые основы защиты персональных данных	10
Тема 3. Программные средства защиты персональной информации	20
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	20
Контроль самостоятельной работы и выполнение заданий в LMS Moodle в форме тестировани	20
Зачет	20
Итого	100

2) Обязательной формой текущей аттестации знаний является тестирование. Максимальная оценка на тестировании может составить 10 баллов.

3) На зачете ответ студента может быть максимально оценен в 30 баллов. Из них 10 баллов могут быть получены на тестировании и 10 баллов за защиту индивидуального проекта.

2. Оценочная таблица

Место контроля в структуре дисциплины	**Форма контроля**	**Используемый критерий оценивания**	**Максимальный балл** *(исходя из*

				весового коэффициента)
Тема 1. Понятие «персональные данные»	Опрос индивидуальное задание	Критерий оценивания 1 Критерий оценивания 4	5 5	10
Тема 2. Правовые основы защиты персональных данных	индивидуальное задание	Критерий оценивания 4	10	10
Тема 3. Программные средства защиты персональной информации	Опрос индивидуальное задание	Критерий оценивания 2 Критерий оценивания 3	5 5	20
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	Опрос индивидуальное задание	Критерий оценивания 3 Критерий оценивания 4	10 10	20
Контроль самостоятельной работы студентов	Контрольная работа Выполнение заданий в LMS Moodle	Критерий оценивания 3 Критерий оценивания 4	10 10	20
Промежуточная аттестация	Зачет	Критерий оценивания 1 Критерий оценивания 2 Критерий оценивания 3 Критерий оценивания 4	5 5 10 10	20
Итого:				100