МИНПРОСВЕЩЕНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования "Тульский государственный педагогический университет им. Л.Н. Толстого"

(ФГБОУ ВО "ТГПУ им. Л.Н. Толстого")

Защита персональных данных в здравоохранении

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **институт передовых информационных технологий**

ОПОП **Направление 09.03.03 Прикладная информатика**
направленность (профиль) Прикладная информатика в здравоохранении

Квалификация **Бакалавр**

Год начала подготовки **2022**

Форма обучения **очная**

Общая трудоемкость **3 з.е.**

Виды контроля по семестрам:
зачет 8

Семестр(Курс.Номер семестра на курсе)	**8(4.2)**		Итого	
	УП	РПД	УП	РПД
Лекции	22	22	22	22
Лабораторные	24	24	24	24
Итого ауд.	46	46	46	46
КСР	2	2	2	2
Контактная работа	48	48	48	48
Сам. работа	60	60	60	60
Часы на контроль	0	0	0	0
Практическая подготовка	0	0	0	0
Семинары	0	0	0	0
Консультации	0	0	0	0
Итого трудоемкость в часах	108	108	108	108

Программу составил(и):

д.п.н., профессор, Богатырева Юлия Игоревна

Рабочая программа дисциплины

Защита персональных данных в здравоохранении

разработана в соответствии с ФГОС:

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

составлена на основании учебного плана:

Направление 09.03.03 Прикладная информатика
направленность (профиль) Прикладная информатика в здравоохранении
утвержденного Учёным советом вуза от 28.02.2022 протокол № 3.

РПД утверждена Учёным советом университета
протокол от 28.2.2022 г. № 3

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина дает базовую основу для понимания, анализа и оценки основных проблем, связанных с защитой персональных данных в здравоохранении

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Цикл (раздел) ООП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
1.	Информационная безопасность
2.	эксплуатационная практика
3.	Системы здравоохранения
4.	Тестирование программного обеспечения
5.	Язык Python для анализа данных
6.	технологическая (проектно-технологическая) практика
7.	Алгоритмы и структуры данных
8.	практика по получению первичных навыков научно-исследовательской работы
9.	Информатика и информационные технологии
10.	ознакомительная практика
11.	Деловая коммуникация и основы деловой этики
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
1.	Выпускная квалификационная работа

3. СООТНЕСЕНИЕ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) С ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ

3.1 Компетенции обучающегося и индикаторы их достижения:

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
ОПК-3.1	Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	понятие персональных данных и способы их защиты
ОПК-3.2	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	применять программные и технические средства для защиты персональных данных
ОПК-3.3	Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
	использования основных технических и программных средств для организации ИТ-инфраструктуры и управления информационной безопасностью.
ПК-2: Способен проводить тестирование компонентов программного обеспечения ИС	
ПК-2.1	Знает современные технологии тестирования программного обеспечения ИС
	основные требования информационной безопасности
ПК-2.2	Умеет использовать подобные технологии при проведении тестовых испытаний
	использовать основы правовых знаний для защиты персональных данных
ПК-2.3	Имеет практический навык проведения тестирования компонентов программного обеспечения ИС
	использования основных технических и программных средств для защиты персональных данных на предприятии и в организациях.
УК-10: Способен формировать нетерпимое отношение к коррупционному поведению	
УК-10.1	Понимает сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями
	правовые основы для управления информационной безопасностью
УК-10.2	Анализирует и правильно применяет правовые нормы о противодействии коррупционному поведению
	осуществлять защиту персональных данных с использованием классификации информационных систем;

3.2 Результаты обучения по дисциплине:
В результате освоения дисциплины обучающийся должен:

	Знать:
З.1	понятие персональных данных и способы их защиты
З.2	основные требования информационной безопасности
З.3	правовые основы для управления информационной безопасностью
	Уметь:
У.1	осуществлять защиту персональных данных с использованием классификации информационных систем;
У.2	применять программные и технические средства для защиты персональных данных
У.3	использовать основы правовых знаний для защиты персональных данных
	Владеть:
В.1	безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов;
В.2	использования основных технических и программных средств для защиты персональных данных на предприятии и в организациях.
В.3	использования основных технических и программных средств для организации ИТ-инфраструктуры и управления информационной безопасностью.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература	Содержание
	Основные понятия информационной безопасности				
1.1	Определение и эволюция понятия «персональные данные» /Лек/	8	4	Л1.1Л2.2	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
1.2	Работа в программе Консультант Плюс. Изучение ФЗ № 152-ФЗ «О персональных данных» /Лаб/	8	2	Л1.1Л2.2 Л2.3	Безопасный поиск. Настройка браузеров. Конфиденциальность и безопасность в Интернете.
1.3	Информационная безопасность как компонент национальной безопасности государства /Ср/	8	10	Л1.1Л2.2	Сформулируйте ваши предложения по вопросу повышения уровня информационной безопасности в системе образования, здравоохранения или ИТ-отрасли.
1.4	Понятие персональных данных в нормативных документах /Лаб/	8	2	Л1.1Л2.2 Л2.3	Изучение ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
1.5	Тестирование по теоретическому материалу /КСР/	8	2		тестирование по дисциплине
	Правовые основы информационной безопасности и защита интеллектуальной собственности				

2.1	Нормативно-правовое обеспечение информационной безопасности и защиты персональных данных /Лек/	8	4	Л1.1 Л1.2Л2.1 Л2.2	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
2.2	Классификация информационных систем персональных данных и требования к их защищенности /Лаб/	8	2	Л1.1 Л1.2Л2.1 Л2.2	Категории обрабатываемых в информационной системе персональных данных. Постановление Правительства РФ “Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”. Объем обрабатываемых персональных данных. Определение типа угроз безопасности персональных данных, актуальных для информационной системы. Определение уровня защищенности персональных данных. Выполнение требований для обеспечения защищенности персональных данных при их обработке в информационной системе.
2.3	Требования к обеспечению информационной безопасности персональных данных /Ср/	8	10	Л1.1 Л1.2Л2.1 Л2.2	Опишите требования к обеспечению безопасности ИС ПДн. Сформулируйте и представьте в отчете выводы: какие из этих требований предусмотрены в информационной системе и какие следует ввести для организации защиты ПДн
2.4	Основные понятия в области защиты авторских прав /Лек/	8	2	Л1.1Л2.2	История создания правового института по охране авторского права. Субъекты авторского права. Права обладателей авторских прав. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность. Всемирная конвенция об авторском праве. Основные институты и понятия международного авторского права. Произведения, пользующиеся охраной.
2.5	Ответственность за нарушения защиты персональных данных /Лаб/	8	2	Л2.2 Л1.1 Л1.2	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.
	Программные средства защиты персональной информации				

3.1	Угрозы информационной безопасности и защите персональных данных /Лек/	8	4	Л1.1 Л1.2Л2.2	Факторы, риски угроз информационным ресурсам. Виды угроз и типы атак. Информационные войны. Информационное оружие. Анализ и оценивание угроз информационной безопасности личности в современном информационном обществе Классификация компьютерных преступлений. Группы компьютерных преступлений. Хакерство в мире и в России. Закрытие информации как средство ее защиты от несанкционированного доступа.
3.2	Виды защищаемой информации /Лек/	8	2	Л1.1 Л1.2Л2.2	Понятие о защищаемой информации. Виды защищаемой информации. Свойства информации как предмета защиты. Классификация информации по категории доступа. Виды информации. Понятие ценности информации. Перечень сведений, доступ к которым не может быть ограничен. Понятие конфиденциальной информации, ее виды.
3.3	Программное обеспечение для защиты персональных данных /Лаб/	8	2	Л1.1Л2.1 Л2.2 Л2.3	Работа с сетевыми экранами, программами: анти-спам, анти-шпион. Сетевые экраны: назначение и особенности применения. Фильтрация контента. Системы контентной фильтрации. Интернет-фильтры для персональной фильтрации интернет контента. Спам и защита от него. Модели угроз безопасности персональных данных при их обработке в информационных системах
3.4	Способы защиты от вирусов. Антивирусные программы /Ср/	8	2	Л1.1Л2.2	Основные понятия. Виды вирусов. Антивирусные программы: классификация, назначение и особенности применения.
3.5	Аппаратные и программные средства для защиты данных /Ср/	8	8	Л1.1Л2.1 Л2.2	Выполнение индивидуального проекта
3.6	Организация парольной защиты /Лаб/	8	2	Л1.1Л2.2	Понятие пароля. Методы вскрытия и шифрования паролей. Атака полным перебором. Комбинированная атака по словарю. Формирование пароля с помощью программы ViPNet. Программы для хранения паролей. Методы шифрования паролей
3.7	Программные средства защиты персональных данных /Лек/	8	2	Л2.1 Л1.1 Л1.2 Л2.3	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.
	Технические средства защиты и комплексное обеспечение безопасности персональных данных				
4.1	Технические средства защиты персональных данных в здравоохранении /Лек/	8	4	Л1.1 Л1.2Л2.1 Л2.2	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

4.2	Порядок работы с персональными данными работника. /Лаб/	8	2	Л1.1 Л1.2Л2.1 Л2.2	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.
4.3	Планирование мероприятий по защите персональных данных. /Лаб/	8	4	Л1.2Л2.2	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
4.4	Технические средства защиты персональных данных /Лаб/	8	4	Л1.1Л2.2 Л2.3	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

4.5	Комплексное обеспечение информационной безопасности и защиты персональных данных в здравоохранении /Лаб/	8	2	Л1.1Л2.1 Л2.2 Л2.3	Концепция информационной безопасности. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в информационных система и сервисах. Правовые нормы и стандарты по лицензированию и сертификации. Служба информационной безопасности предприятия. Состав, цели и задачи службы информационной безопасности предприятия.
4.6	Политика информационной безопасности /Ср/	8	8	Л1.1 Л1.2Л2.2 Л2.3	Методические документы ФСТЭК России в области обеспечения безопасности персональных данных, при их обработке в ИСПД. Содержание базовой модели угроз безопасности персональных данных. Задачи, решаемые с помощью «Базовой модели угроз … ». Типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных. Понятие "Политика ИБ". Цели политики ИБ. Составляющие политики ИБ.
4.7	Подготовка к зачету /Ср/	8	22	Л1.1 Л1.2Л2.1 Л2.2 Л2.3	Вопросы к зачету

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Типовые задания для проведения текущего контроля

Индивидуальное задание по теме «Проектирование и создание системы защиты персональных данных»

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

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

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.

Примерные тестовые вопросы

1. Термин «информация» определен как «сведения (сообщения, данные) независимо от формы их представления»:

Федеральным законом РФ N 149-ФЗ «Об информации, информационных технологиях и защите информации»
Федеральным законом РФ N 85-ФЗ «Об участии в международном информационном обмене»
Доктриной информационной безопасности
Законом РФ «О безопасности»

2. Что такое целостность информации?

свойство информационных ресурсов, заключающееся в возможности их изменения любым субъектом
свойство информационных ресурсов, заключающееся в их неизменности в процессе передачи или хранения

свойство информационных ресурсов, заключающееся в возможности их изменения только единственным пользователем
свойство информационных ресурсов, заключающееся в их существовании в виде единого набора файлов
3. Принцип системы обеспечения информационной безопасности «своевременности» предполагает, что:
все меры, направленные на обеспечение информационной безопасности, должны вводиться в самом начале построения системы, а уже затем улучшаться
все меры, направленные на обеспечение информационной безопасности, должны планироваться с ранних стадий системы безопасности и вводиться своевременно
разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы, но внедряться системы защиты должна только после окончания работ по построению системы
разработка мер систем защиты должна осуществляться после окончания работ по построению системы
4. К коммерческой тайне не могут быть отнесены:
сведения о загрязнении окружающей среды
сведения о противопожарной безопасности
сведения, относящиеся к ноу-хау предприятия
сведения о численности работников
сведения о наличии свободных мест
сведения о заработной плате работников
5. К объектам служебной тайны относятся:
врачебная тайна
судебная тайна
тайна следствия
адвокатская тайна
военная тайна
6. К какой категории относятся персональные данные, позволяющие идентифицировать субъекта персональных данных?
1 категория
2 категория
3 категория
4 категория
7. Какой класс присваивается информационным системам, если нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных?
К4
К3
К2
К1
8. Какие процедуры включает в себя система ЭЦП?
процедуру формирования и проверки цифровой подписи
процедуру формирования цифровой подписи
процедуру проверки цифровой подписи
процедуру шифрования и формирования цифровой подписи
9. Какие угрозы безопасности информации являются непреднамеренными?
стихийные бедствия
поджог
забастовка
ошибки пользователей
неумышленное повреждение каналов связи
действия случайных помех
сбои в работе аппаратуры и оборудования
хищение носителей информации
10. К косвенным каналам утечки информации относятся:
кража или утеря носителей информации
копирование защищаемой информации из информационной системы
инсайдерские действия
исследование не уничтоженного мусора
перехват электромагнитных излучений
11. Kerberos – это:
сетевой протокол аутентификации
прикладной протокол аутентификации
криптографический алгоритм
сетевой протокол идентификации
12. Какие задачи информационной безопасности решаются на организационном уровне?
внедрение системы безопасности
ограничение доступа на объект
внедрение системы контроля и управления доступом
разработка документации
обучение персонала
сертификация средств защиты информации

13. Укажите все верные утверждения о шифровании данных.
длина шифрованного текста должна быть равной длине исходного текста
между всеми используемыми в алгоритме ключами должна существовать четкая зависимость
современные алгоритмы шифрования ГОСТ 28147-89 (Россия) и AES (США) являются асимметричными
основной недостаток симметричных алгоритмов шифрования – трудность в обмене ключами
основной недостаток асимметричных алгоритмов шифрования – медленная работа по сравнению с симметричными алгоритмами

14. 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

15. 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

16. Возможностью анализа изображений Интернета обладает модуль, входящий в состав следующего антивируса:
- Подзарядка
- StaffCop Home Edition
- KidsControl
- Time Boss

Примерные задания для самостоятельного выполнения:
1. Определить дату выпуска антивирусных баз, при необходимости обновить их. Рассмотреть различные способы обновления антивирусных баз.
2. Изучить интерфейс представленного антивирусного программного обеспечения Kaspersky Internet Security
3. Проанализировать назначение каждого компонента, входящего в состав KIS, произвести настройку каждого компонента на оптимальный уровень защиты.
4. Провести полную проверку компьютера на наличие вредоносного программного обеспечения. В случае обнаружения вредоносных программ, оформить отчет, в котором описать вредоносную программу, предложить методы защиты.
5. Составить подробное описание основных классов вирусов.
6. Существуют ли службы, аналогичные службам в IE InPrivate, в браузерах Google и Firefox?
7. Сформулируйте основные принципы защиты от фальшивых сайтов.
8. Сформулируйте правила безопасного скачивания файлов из интернета.
9. Сформулируйте какие виды атак на пароль Вы знаете.
10. Сформулируйте правила выбора паролей.
11. Как можно противостоять атаке полным перебором?
12. Как длина пароля влияет на вероятность раскрытия пароля?
13. Сформулируйте рекомендации по составлению и хранению паролей.

5.2. Типовые задания для проведения промежуточной аттестации

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.

5.3. Перечень видов оценочных средств

1. Индивидуальное проектное задание.
2. Тестирование.
3. Выполнение заданий к лабораторно-практическим занятиям.
3. Вопросы к зачету.

5.4. Процедура применения оценочных материалов

Промежуточная аттестация может проводиться с применением электронного обучения и (или) дистанционных образовательных технологий в соответствии с "Порядком проведения промежуточной аттестации с применением электронного обучения и /или дистанционных образовательных технологий".

Оценочные материалы представлены в Приложении файл "ОМД ИБиЗПД_Богатырева.pdf"

Описание балльно-рейтинговой системы по дисциплине.
Составляющие итоговой оценки за дисциплину:
1) Текущий контроль (общий вес 60 баллов):
до 20 баллов – посещение лекций, работа на практических занятиях;
до 40 баллов - выполнение индивидуальных проектных заданий, тестирование.
2) Промежуточная аттестация заключается в проведении экзамена (общий вес - 40 баллов): тестирование, ответы на дополнительные вопросы.
При этом, для получения положительной итоговой оценки на зачете необходимо получить не менее 50% по каждой составляющей и выполнить все практические задания. Шкала перевода баллов в оценку: до 40 - «неудовлетворительно»; 41 -60 – «удовлетворительно»; 61-80 – «хорошо»; 81 и выше - "отлично".

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год (кол-во экземпляров для печатных изданий)	Ссылка на электронное издание
Л1.1	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Издательство Южного федерального университета, 2016	http://biblioclub.ru/index.php?page=book&id=493175
Л1.2	Скрипник Д. А.	Обеспечение безопасности персональных данных: курс	Москва: Интернет-Университет Информационных Технологий, 2011	http://biblioclub.ru/index.php?page=book&id=234794

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год (кол-во экземпляров для печатных изданий)	Ссылка на электронное издание
Л2.1	Петренко В. И.	Защита персональных данных в информационных системах: учебное пособие	Ставрополь: СКФУ, 2016	http://biblioclub.ru/index.php?page=book&id=459205
Л2.2	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	http://biblioclub.ru/index.php?page=book&id=438331
Л2.3	Шилов А. К.	Управление информационной безопасностью: учебное пособие	Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2018	http://biblioclub.ru/index.php?page=book&id=500065

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Официальный сайт ФГБОУ ВО «Тульский государственный педагогический университет им. Л.Н. Толстого»
Э2	Среда электронного обучения LMS Moodle

6.3.Информационные технологии

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения

1.	Операционная система Microsoft Windows XP Professional Russian. Лицензия № 16698685 от 08.08.2003 г.
2.	Операционная система Microsoft Windows Professional 7 Russian. Лицензия №48497058 от 13.05.2011 г., договор № Пр/16/6 от 05 апреля 2016 г.
3.	Операционная система Microsoft Windows 10 Professional Russian. Контракт № ПР/ФЕН/15/18 от 23.10.2015 г., договор № Пр/16/6 от 05 апреля 2016 г.
4.	Файловый архиватор 7z. Свободно распространяемое ПО
5.	Браузеры Google Chrome, Mozilla, Opera. Свободно распространяемое ПО
6.	Редактор диаграмм, схем, блок-схем, UML-схем Dia 0.97.2. Свободно распространяемое ПО
7.	Система облачного хранилища Dropbox. Свободно распространяемое ПО
6.3.2 Перечень информационных справочных систем и профессиональных баз данных	
1.	Компьютерная информационно-правовая система «Гарант»
2.	Официальный интернет-портал базы данных правовой информации (http://pravo.gov.ru)
3.	Портал Федеральных государственных образовательных стандартов высшего образования (http://fgosvo.ru)
4.	Портал «Информационно-коммуникационные технологии в образовании» (http://www.ict.edu.ru)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Ауд.	Назначение	Оборудование и технические средства обучения	Вид
2-16	Компьютерный класс	интерактивная доска, компьютеры, маркерная доска, принтер, сканер, стол преподавателя, столы учебные	Лаб
4-305	Компьютерный класс	аудиоколонки для проектора и интерактивной доски, аудиоколонки учебные, интерактивная доска, компьютеры, кондиционер, маркерная доска, проектор, столы компьютерные, столы учебные	Ср
4-306	Компьютерный класс	аудиоколонки для проектора и интерактивной доски, интерактивная доска, компьютеры, кондиционер, маркерная доска, проектор, столы компьютерные, столы учебные	Экзамен
4-307	Компьютерный класс	аудиоколонки, компьютеры, кондиционер, маркерная доска, столы компьютерные, столы учебные, телевизор	КСР
4-318	Компьютерный класс	компьютеры, маркерная доска, серверная стойка лаборатории МТС, стол преподавателя, столы компьютерные, столы учебный большой	Лек
4-304	Лекционная с мультимедийным комплексом	доска учебная, проектор, стол преподавателя, столы учебные, стул преподавателя, экран	Лек

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

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:
7) Проведение лекций с использованием презентаций на основе мультимедийных технологий;
8) Обеспечение студентов сопутствующими материалами, размещенными среде Moodle;
Примерная тематика практических занятий по дисциплине.
Полные варианты практических занятий размещены в в системе управления обучением MOODLE.