



Факультет	Математики, физики и информатики	
Кафедра	Информатики и информационных технологий	
Направление	09.03.03 Прикладная информатика	
Направленность(профиль)	Прикладная информатика в здравоохранении	
Информационные технологии в защите персональных данных		Б1.В.ДВ.14.01

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 № 8 от «31» августа 2017 г.


**Рабочая программа дисциплины
«Информационные технологии в защите
персональных данных»**

Трудоемкость: 3 зачетные единицы

Квалификация выпускника: Бакалавр

Форма обучения: очная

Год начала подготовки: 2014

И. о. заведующего кафедрой  Ю.И. Богатырева

Декан факультета  И.Ю. Реброва

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.....	3
2. Место дисциплины в структуре ОПОП бакалавриата	3
3. Объем дисциплины и виды учебной работы	3
4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий	4
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	5
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	5
6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы	5
6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.....	5
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	6
Темы индивидуальных проектов	8
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	10
7.1. Основная литература	10
8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	11
9. Методические указания для обучающихся по освоению дисциплины	11
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем	12
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	13
12. Аннотация рабочей программы дисциплины	14
13. Лист регистрации изменений к рабочей программе дисциплины.....	15

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
Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-18)	<p>Выпускник знает: правовые основы для управления информационной безопасностью;</p> <p>Умеет: применять программные и технические средства для защиты персональных данных;</p> <p>Владеет и (или) имеет опыт деятельности: использования основных технических и программных средств для организации ИТ-инфраструктуры и управления информационной безопасностью.</p>	В соответствии с учебным планом и планируемыми результатами освоения ОПОП
Готовность к обеспечению информационной безопасности на уровне БД (ДПК-5)	<p>Выпускник знает: понятие персональных данных и способы их защиты;</p> <p>Умеет: осуществлять защиту персональных данных с использованием средств ИКТ;</p> <p>Владеет и (или) имеет опыт деятельности: обеспечения информационной безопасности на уровне баз данных.</p>	В соответствии с учебным планом и планируемыми результатами освоения ОПОП

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

Дисциплина «Информационные технологии в защите персональных данных» относится к дисциплинам по выбору вариативной части учебного плана Блока 1. Дисциплины (модули).

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	Объем зачетных единиц / часов по формам обучения
Максимальная учебная нагрузка (всего)	<i>108/3</i>
Контактная работа обучающихся с преподавателем (всего)	<i>22</i>
в том числе:	
лекции	<i>8</i>
практические работы	<i>12</i>
контрольные работы	<i>2</i>
Самостоятельная работа студента (всего)	<i>86</i>
в том числе:	
внеаудиторная самостоятельная работа по подготовке к лекционным занятиям	<i>20</i>
внеаудиторная самостоятельная работа по подготовке к практическим занятиям и защите отчета	<i>20</i>
подготовка к контрольной работе	<i>24</i>

выполнение заданий для самостоятельной работы в системе управления обучением MOODLE

22

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

Наименование тем (разделов).	Количество академических или астрономических часов по видам учебных занятий			
	Занятия лекционного типа	Практические занятия	Другие виды работ	Самостоятельная работа обучающихся
Тема 1. Понятие «персональные данные»	2		2	20
Тема 2. Правовые основы защиты персональных данных	2		4	10
Тема 3. Программные средства защиты персональной информации	2		2	20
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	2		4	12
Контроль самостоятельной работы студентов		2		24
ИТОГО	8	2	12	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

Система электронного дистанционного обучения MOODLE ТГПУ им. Л.Н. Толстого
<http://moodle.tsput.ru/course/view.php?id=16446>

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 «Способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-18)», «Готовность к обеспечению информационной безопасности на уровне БД (ДПК-5)» осуществляется в несколько этапов в соответствии с учебным планом и планируемыми результатами освоения ОПОП, соотнесенными с планируемыми результатами обучения по каждой дисциплине (модулю) и практике.

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

Дескриптор компетенций	Показатели оценивания	Критерии оценивания
------------------------	-----------------------	---------------------

Информационные технологии в защите персональных данных		Б1.В.ДВ.14.01
Знания	правовых основ для управления информационной безопасностью; понятий персональных данных и способы их защиты;	Отметка «зачтено» выставляется, если студент в целом за семестр набрал от 41 до 100 баллов (с учетом баллов, набранных на промежуточной аттестации (зачете)). Отметка «не зачтено» выставляется, если студент в целом за семестр набрал менее 41 балла (с учетом баллов, набранных на промежуточной аттестации (зачете)).
Умения	применять программные и технические средства для защиты персональных данных; осуществлять защиту персональных данных с использованием средств ИКТ;	
Навыки и опыт деятельности	использования основных технических и программных средств для организации ИТ-инфраструктуры и управления информационной безопасностью; обеспечения информационной безопасности на уровне баз данных.	

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

Проверка преподавателем выполненных студентами индивидуальных проектов и заданий, размещенных в LMS MOODLE

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

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

а) Создание фрагментов

б) 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 обучающихся 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, объединенных 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. Используются 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

6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) 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:

	Макс балл
Учебная работа	
Тема 1. Понятие «персональные данные»	10
Тема 2. Правовые основы защиты персональных данных	10
Тема 3. Программные средства защиты персональной информации	10
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	10
Контроль самостоятельной работы и выполнение заданий в LMS Moodle	20
Зачет	30
Итого	100

2) Обязательной формой текущей аттестации знаний является срезовая контрольная работа. Максимальная оценка на срезовой контрольной работе 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 веса коэффициента)
Тема 1. Понятие «персональные данные»	Опрос индивидуально задание	Критерий оценивания 1	5	10
		Критерий оценивания 4	5	
Тема 2. Правовые основы защиты персональных данных	индивидуально задание	Критерий оценивания 4	10	10
Тема 3. Программные средства защиты персональной информации	Опрос индивидуально задание	Критерий оценивания 2	5	10
		Критерий оценивания 3	5	
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	Опрос индивидуально задание	Критерий оценивания 3	10	20
		Критерий оценивания 4	10	
Контроль самостоятельной работы студентов	Контрольная работа Выполнение заданий в LMS Moodle	Критерий оценивания 3	10	20
		Критерий оценивания 4	10	

Информационные технологии в защите персональных данных			Б1.В.ДВ.14.01	
Промежуточная аттестация	Зачет	Критерий оценивания 1	5	30
		Критерий оценивания 2	5	
		Критерий оценивания 3	10	
		Критерий оценивания 4	10	
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.

	Мак 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 обеспечение безопасности персональных данных	20	5
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

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2017. — 325 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. <https://www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847>

7.2. Дополнительная литература:

1. Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2017. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. <https://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1>

2. Основы информационной безопасности. [Электронный ресурс] : учеб. пособие / Е.Б. Белов [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2006. — 544 с. — Режим доступа: <http://e.lanbook.com/book/5121> — Загл. с экрана.

3. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. [Электронный ресурс] : учеб. пособие / А.А. Афанасьев [и др.]. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 550 с. — Режим доступа: <http://e.lanbook.com/book/5114> — Загл. с экрана.

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

1. 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>
2. 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>
3. 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
4. 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
5. 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

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Дисциплина «Информационные технологии в защите персональных данных» направлена на формирование у студентов теоретических знаний в области защиты персональных данных, формирование представления о способах и средствах защиты с использованием информационных технологий в образовании и будущей профессиональной деятельности; подготовка студентов к применению полученных знаний и навыков в профессиональной деятельности, проектированию и разработке комплексной системы защиты персональных данных. Для успешного освоения дисциплины следует использовать материал, выложенный в MOODLE, в котором дается необходимая теория, приводятся методы решения типовых задач, задачи для контрольных работ, индивидуальные задания. В системе MOODLE приводится текущий рейтинг студентов, и даются задания для его повышения. Для более глубокого изучения материала используется другая литература из приведенного списка.

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.

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

При осуществлении образовательного процесса по дисциплине используются информационные технологии, охватывающие ресурсы (компьютеры, программное обеспечение и сети), необходимые для управления информацией (создание, хранение, управление, передача и поиск информации):

- технические средства: компьютерная техника и средства связи (ноутбук, проектор, экран, USB-накопители и т.п.);
- коммуникационные средства (проверка домашних заданий и консультирование посредством электронной почты, личного кабинета студента и преподавателя, видеотрансляций);
- организационно-методическое обеспечение (электронные учебные и учебно-методические материалы, компьютерное тестирование, использование электронных мультимедийных презентаций при проведении практических занятий);
- программное обеспечение (Microsoft Office (Excel, Power Point, Word и т.д.), Skype, поисковые системы, электронная почта и т.п.);
- среда электронного обучения ТГПУ им. Л.Н. Толстого <http://moodle.tsput.ru>.

Комплект лицензионного программного обеспечения

1. Операционная система Microsoft Windows XP Professional Russian – Лицензия № 16698685 от 08.08.2003 г.
2. Программное обеспечение Microsoft Office XP Professional Win32 Russian– Лицензия № 16698685 от 08.08.2003 г.
3. Программное обеспечение Microsoft Office Enterprise 2007 Russian - Лицензия №46138962 от 16.11.2009 г.
4. Операционная система Microsoft Windows Professional 7 Russian – Лицензия №48497058 от 13.05.2011 г.
5. Программа для распознавания текста ABBYY FineReader 9.0 Corporate Edition лицензионный сертификат - код позиции AF90-3U1V25-102, ABBYY FineReader 9.0 Corporate Edition Volume License Concurrent от 28 июля 2009 г.
6. Электронный словарь ABBYY Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, ABBYY Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.
7. Комплексная Система Антивирусной Защиты Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 500-999 Node 2 year Educational Renewal License – Лицензия № 1894-150512-101810 от 12-05-2015 г.

Современные профессиональные базы данных и информационные справочные системы

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. Портал "Информационно-коммуникационные технологии в образовании" <http://www.ict.edu.ru>.

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

Реализация дисциплины обеспечена материально-технической базой, соответствующей действующим противопожарным нормам и правилам.

Дисциплина обеспечена специальными помещениями для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещениями для самостоятельной работы. Аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Учебные помещения для проведения занятий лекционного и семинарского типа оборудованы мультимедийным демонстрационным оборудованием, для демонстрации учебно-наглядных пособий, обеспечивающих тематические иллюстрации, соответствующие рабочей учебной программе дисциплины.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ТГПУ им. Л.Н. Толстого, внутривузовское сетевое окружение.

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 следующие компетенции: способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью (ПК-18); готовностью к обеспечению информационной безопасности на уровне БД (ДПК-5).

В результате освоения дисциплины студент должен приобрести:

знания правовых основ для управления информационной безопасностью; понятий персональных данных и способы их защиты;

умения применять программные и технические средства для защиты персональных данных; осуществлять защиту персональных данных с использованием средств ИКТ;

навыки использования основных технических и программных средств для организации ИТ-инфраструктуры и управления информационной безопасностью; обеспечения информационной безопасности на уровне баз данных.

2. Место дисциплины в структуре ОПОП.

Дисциплина «Информационные технологии в защите персональных данных» относится к дисциплинам по выбору вариативной части учебного плана.

3. Объем дисциплины: 3 зачетные единицы.

4. Образовательный процесс осуществляется на русском языке.

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

13. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ**2016-2017 учебный год**

В рабочую программу внесены изменения в части обновления состава лицензионного программного обеспечения, профессиональных баз данных и информационно-справочных систем, к которым должен быть обеспечен доступ обучающимся.

Решение ученого совета университета, протокол №2 от 16 февраля 2017 г.

2017-2018 учебный год

Обновлен состав необходимого комплекта лицензионного 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 года.
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 года.
4. Программное обеспечение Microsoft Office Enterprise 2007 Russian - Лицензия №46138962 от 16.11.2009 г.
5. Программное обеспечение Microsoft Office 2013 Professional - контракт № 405535 от 2 ноября 2015 года, контракт № ПР/ФЕН/15/18 от 23.10.2015 г.
6. Программа для распознавания текста АБВУ FineReader 9.0 Corporate Edition лицензионный сертификат - код позиции AF90-3U1V25-102, АБВУ FineReader 9.0 Corporate Edition Volume License Concurrent от 28 июля 2009 г.
7. Электронный словарь АБВУ Lingvo X3 Европейская версия - Код позиции AL14-2U1V05-102, АБВУ Lingvo x3 Европейская версия. Именная лицензия Concurrent от 28 июля 2009 г.
8. Комплексная Система Антивирусной Защиты Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 500-999 Node 2 year Educational Renewal License – Лицензия № 17E0-170518-102844-823-690 от 18-05-2017 г.

Обновлен состав современных профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ обучающимся.

1. Компьютерная информационно-правовая система «Гарант» - регистрационный номер клиента 71-70685-000033.
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>.
5. Web of Science Core Collection – политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных <http://webofscience.com>.
6. Полнотекстовый архив ведущих западных научных журналов на российской платформе Национального электронно-информационного консорциума (НЭИКОН) <http://neicon.ru>.
7. Базы данных издательства Springer <https://link.springer.com>.

Изменения к рабочей программе дисциплины утверждены на заседании Ученого совета университета, протокол № 8 от 31 августа 2017 г.

Программа составлена в соответствии с требованиями ФГОС ВО.

Разработчик:

Фамилия, имя, отчество	Учёная степень	Учёное звание	Должность
Богатырева Юлия Игоревна	д.п.н	доцент	профессор кафедры информатики и информационных технологий