

	Факультет	Математики, физики и информатики	
	Кафедра	Информатики информационных технологий	
	Направление подготовки	02.03.02 Фундаментальная информатика и информационные технологии	
	Направленность (профиль)	Открытые информационные системы	
	Информационная безопасность и защита 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 «Информационная безопасность и защита персональных данных»

Трудоемкость: 3 зачетные единицы

Квалификация выпускника: Бакалавр

Форма обучения: очная

Год начала подготовки: 2014

И. о. заведующего кафедрой информатики и ИТ



Ю.И. Богатырева

Декан факультета МФиИ



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.....	4
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.....	6
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине.....	7
6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.....	7
6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.....	7
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.....	8
6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.....	1
2	
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	15
7.1. Основная литература.....	15
7.2. Дополнительная литература.....	15
9. Методические указания для обучающихся по освоению дисциплины.....	16
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.....	18
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.....	19
12. Аннотация рабочей программы дисциплины.....	19
13. Лист регистрации изменений к рабочей программе дисциплины.....	21

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 использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4)	<p>Выпускник знает: основные понятия, принципы, методы, средства, правовые основы и модели информационной безопасности;</p> <p>умеет: формулировать и проектировать политику информационной безопасности в ИС;</p> <p>владеет: навыками безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов.</p>	В соответствии с учебным планом и планируемыми результатами освоения ОПОП
Способность решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива (ПК-4)	<p>Выпускник знает: понятие персональных данных и способы их защиты;</p> <p>умеет: осуществлять защиту персональных данных с использованием средств ИКТ;</p> <p>владеет: навыками использования основных технических и программных средств для защиты персональных данных на предприятии и в организациях.</p>	В соответствии с учебным планом и планируемыми результатами освоения ОПОП

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП БАКАЛАВРИАТА

Дисциплина «Информационная безопасность и защита персональных данных» относится к дисциплинам по выбору вариативной части учебного плана. 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)	3/108
Контактная работа обучающихся с преподавателем (всего)	22
в том числе:	
лекции	8
практические занятия	12
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 при подготовке к семинарским и/или практическим занятиям	30
выполнение заданий для самостоятельной работы в системе управления обучением MOODLE	30
подготовка к зачету	4
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	Практические занятия	Другие виды работ	Самостоятельная работа
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	
Подготовка к зачету				4
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

Основной целью изучения дисциплины «Информационная безопасность» является приобретение студентами теоретических сведений, практических умений и навыков применения современных информационных технологий для использования в профессиональной деятельности по защите информации. В результате освоения дисциплины у обучаемых должно быть сформировано общее представление о современных концепциях информационной безопасности, знакомство с различными методами защиты информации от несанкционированного доступа, приобретение практических навыков работы с современными аппаратными и программными средствами защиты информации.

Преподавание дисциплины должно включать в себя следующие образовательные технологии:

- 1) Организация лекций с использованием презентаций, выполненных с применением мультимедийных технологий;
- 2) Проведение лабораторных работ с использованием электронных образовательных ресурсов;
- 3) Использование проблемно-ориентированного междисциплинарного подхода;
- 4) Создание информационного образовательного портала по дисциплине в виде электронного курса, размещенного в LMS MOODLE;
- 5) Внедрение технологий дистанционного обучения для выполнения заданий самостоятельной работы в LMS MOODLE;
- 6) Электронные интерактивные способы взаимодействия преподавателя и студентов путем организации Интернет-форума в LMS MOODLE.

Контроль текущей успеваемости осуществляется в форме тестирования в Moodle по следующим темам:

1. Понятие и классификация угроз информационной безопасности.
2. Виды программного и аппаратного обеспечения по защите информации в ИС.
3. Информационная безопасность на предприятии.

При организации самостоятельной работы бакалавров используются современные информационные и коммуникационные технологии для создания, формирования и администрирования электронных образовательных ресурсов.

Изучение и анализ информационных ресурсов в научных библиотеках и сети Интернет по следующим направлениям:

- составление библиографии по проблемам информатики;
- анализ и рецензирование публикации (в том числе электронных) источников по своей предметной области;
- составление аннотированного списка научно-исследовательской литературы по актуальным проблемам дисциплины;
- конспектирование и реферирование первоисточников и научно-исследовательской литературы по тематическим блокам преподаваемой дисциплины.

Типовые задания для самостоятельной работы:

- подготовка реферата;
- подготовка эссе;
- работа с первоисточниками;
- подготовка докладов;
- решение исследовательских задач;
- составление понятийного тезауруса;
- подготовка презентации;
- составление аннотированного списка литературы по одной из тем;

- выполнение индивидуального проекта.

Перечень семинарских занятий

1. Классификация информационной системы персональных данных.
2. Организация парольной защиты.
3. Построение системы защиты ПК от негативных последствий работы в сети Интернет.
4. Применение криптографических средств для защиты конфиденциальной информации на компьютере.
5. Использование программных средств защиты ПК
6. Настройка браузеров для безопасной работы в Интернете.

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 компетенций «Способность использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4)», «Способность решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива (ПК-4)» 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
Знания	понятия персональных данных и способов 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)).
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 – 70	20 – 30	41-100	Зачтено
0 – 20	0 – 20	0 – 40	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

Темы индивидуальных проектных заданий

1. Информация, относящаяся к государственной тайне
2. Биометрические системы идентификации
3. Безопасность и конфиденциальность в Интернете
4. Понятие о персональных данных
5. Информация, составляющая коммерческую тайну
6. Объекты информационной безопасности в предметной области
7. Информационная среда иллюзии или реальности
8. Случайные и целенаправленные угрозы нарушения сохранности информации
9. Понятие дезинформации
10. Риски информационной безопасности
11. Информационное оружие
12. Информационные войны
13. Технические средства промышленного шпионажа
14. Классы безопасности
15. Аудит информационной безопасности
16. История хакерства
17. Хакерство в России
18. Правовые механизмы защиты информации на разных уровнях
19. Понятие и применение электронной цифровой подписи
20. Манипуляции сознанием
21. Программы родительского контроля
22. Средства антивирусной защиты мобильных устройств

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.

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
- McAfee 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:

- Определить дату выпуска антивирусных баз, при необходимости обновить их. Рассмотреть различные способы обновления антивирусных баз.
- Изучить интерфейс представленного антивирусного программного обеспечения Kaspersky Internet Security
- Проанализировать назначение каждого компонента, входящего в состав KIS, произвести настройку каждого компонента на оптимальный уровень защиты.
- Провести полную проверку компьютера на наличие вредоносного программного обеспечения. В случае обнаружения вредоносных программ, оформить отчет, в котором описать вредоносную программу, предложить методы защиты.
- Составить подробное описание основных классов вирусов.

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

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 70 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 - 30 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:

Учебная работа	Мах балл
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 тестирования	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 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	20
		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	
Промежуточная аттестация	Зачет	Критерий оценивания 1	5	20
		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, представленной в приложении 1.

	Мах 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. 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

7.2. Дополнительная литература

1. Основы защиты информации [Текст] : учебное пособие для студентов вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М : Академия, 2008. - 256 с. - ISBN 9785769557613
2. Основы информационной безопасности [Текст] : учеб.пособ.для студ.вузов / С. П. Расторгуев. - М : Академия, 2007. - 192 с. - ISBN 9785769530982

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

- 1 Российское образование [Электронный ресурс] : федеральный портал / ФГУ ГНИИ ИТТ "Информика". - М. : [б. и.], 2002. - Загл. с титул. экрана. - Б. ц. URL: www.edu.ru
- 2 Единое окно доступа к образовательным ресурсам [Электронный ресурс] : информационная система / ФГУ ГНИИ ИТТ "Информика". - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. ц. URL: <http://window.edu.ru>
- 3 Руконт [Электронный ресурс] : национальный цифровой ресурс / ООО «Агентство Книга-Сервис». - М. : [б. и.], 2011. - Загл. с титул. Экрана URL: <http://www.rucont.ru>
- 4 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
- 5 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
- 6 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
- 7 Научно-информационный портал ВИНИТИ [Электронный ресурс] : информационный ресурс / ВИНИТИ РАН. - М. : [б. и.], 2004. - Загл. с титул. экрана. - Б. ц. URL: <http://science.viniti.ru>

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:

- 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.

№	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

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);
- организационно-методическое обеспечение (электронные учебные и учебно-методические материалы, компьютерное тестирование, использование электронных мультимедийных презентаций при проведении лабораторных работ);

- 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.

Компетенции:

Способность использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4);

Способность решать задачи профессиональной деятельности в составе научно-исследовательского и производственного коллектива (ПК-4).

В результате освоения дисциплины студент должен приобрести:

Знания:

основных понятий, принципов, методов, средств, правовых основ и моделей информационной безопасности;

понятия персональных данных и способов их защиты;

Умения:

формулировать и проектировать политику информационной безопасности в ИС;

осуществлять защиту персональных данных с использованием средств ИКТ;

Навыки:

безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов;

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

2. Место дисциплины в структуре ОПОП.

Дисциплина «Психологические основы программирования» относится к дисциплинам по выбору вариативной части учебного плана. Изучение данной дисциплины осуществляется в 7 семестре.

3. Объем дисциплины: 3 зачетные единицы.

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

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

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

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 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.

7 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.

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