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: заочная

Год начала подготовки: 2017

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

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

Планируемые результаты освоения образовательной программы (код и название компетенции)	Планируемые результаты обучения	Этапы формирования компетенции в процессе освоения образовательной программы
способностью использовать базовые правовые знания в различных сферах деятельности (ОК-7);	**Выпускник знает:** основные нормативные правовые акты в области информационной безопасности и защиты информации; **Владеет и (или) имеет опыт деятельности:** навыками безопасного использования технических и программных средств защиты информации в образовательных организациях.	в соответствии с учебным планом и планируемыми результатами освоения ОПОП
способностью использовать приемы оказания первой помощи, методы защиты в условиях чрезвычайных ситуаций (ОК-9)	**Выпускник знает:** место и роль информационной безопасности в информационно-образовательной среде; **Умеет:** формулировать и проектировать политику информационной безопасности образовательных организаций;	в соответствии с учебным планом и планируемыми результатами освоения ОПОП
способностью решать задачи воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности (ПК-3);	**Выпускник знает:** место и роль информационной безопасности в системе национальной безопасности Российской Федерации **Умеет:** анализировать и оценивать угрозы информационной безопасности личности; **Владеет и (или) имеет опыт деятельности:** навыками организации и обеспечения режима защиты персональных данных в информационно-образовательной среде в учебной и внеучебной деятельности	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 Блока 1 вариативной части дисциплин направления.

Изучение данной дисциплины базируется на освоении студентами дисциплин «ИКТ в профессиональной деятельности», «Педагогика», «Психология».

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.

В результате освоения программы студенты приобретают теоретические и практические умения и навыки применения современных информационных технологий для использо-

вания в деятельности по защите информации, а также общее представление о современных концепциях информационной безопасности и защиты персональных данных.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Заочная форма обучения

Вид учебной работы	Объем зачетных единиц / часов по формам обучения
Максимальная учебная нагрузка (всего)	***108/3***
Контактная работа обучающихся с преподавателем (всего)	***10***
в том числе:	
Лекции	*4*
практические работы	*6*
Самостоятельная работа студента (всего)	***94***
в том числе:	
внеаудиторная самостоятельная работа по подготовке к лекционным занятиям	*20*
внеаудиторная самостоятельная работа по подготовке к практическим занятиям и защите отчета	*30*
подготовка к контрольной работе	*24*
выполнение заданий для самостоятельной работы в системе управления обучением MOODLE	*20*
Промежуточная аттестация в форме: зачета	**4**

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

Заочная форма обучения

Наименование тем (разделов).	Количество академических или астрономических часов по видам учебных занятий			
	Занятия лекционного типа	Занятия практического типа	Другие виды учебных занятий	Самостоятельная работа обучающихся
Тема 1. Основные понятия «информационной безопасности»	1	1		20
Тема 2. Правовые основы информационной безопасности и защита персональных данных	1	2		20
Тема 3. Программные средства защиты персональной информации	1	2		20
Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных	1	1		22
Контроль (зачет)			4	12
ИТОГО	4	6	4	94

Тема 1. Основные понятия «информационной безопасности»

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

Определение и эволюция понятия «информационная безопасность». Свойства и понятие информации. Базовые принципы обеспечения ИБ. Защита информации. Субъекты ИБ. Цели, задачи, направления информационной безопасности.

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

Тема 2. Правовые основы информационной безопасности и защиты персональных данных

Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание. Доктрина и стратегия информационной безопасности Российской Федерации. Основные нормативные руководящие документы, касающиеся государственной тайны, коммерческой и других видов тайн, нормативно-справочные документы. Правовая основа защиты персональных данных. Правовая основа использования электронной подписи.

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. Правовые аспекты деятельности в глобальной сети Интернет

Тема 3. Программные средства защиты персональной информации

Классификация вирусов. Каналы проникновения вирусов. Способы заражения. Современные антивирусные средства. Средства антивирусной защиты мобильных телефонов.

Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны.

Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи. Кодирование информации. Электронная цифровая подпись.

Планирование мероприятий по защите персональных данных. Угрозы безопасности персональных данных. Классификация информационных систем ПДн.

Практическое занятие №3. Способы защиты от вирусов. Антивирусные программы.

Тема 4. Технические средства защиты и комплексное обеспечение безопасности персональных данных

Средства контроля доступа в ИС. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации.

Общие подходы к построению парольных систем. Выбор паролей. Хранение паролей. Передача пароля по сети. Механизмы идентификации и аутентификации. Локальная и сетевая аутентификация и авторизация. Способы аутентификации.

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.

Практическое занятие №4 Планирование мероприятий по защите персональных данных в образовательной организации.

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

Основной целью изучения дисциплины «Информационная безопасность и защита персональных данных» 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 (http://moodle.tsput.ru/course/view.php?id=10597);
5) Внедрение технологий дистанционного обучения для выполнения заданий самостоятельной работы в LMS MOODLE (http://moodle.tsput.ru/course/view.php?id=10597);
6) Электронные интерактивные способы взаимодействия преподавателя и студентов путем организации Интернет-форума в LMS MOODLE (http://moodle.tsput.ru/course/view.php?id=10597).

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 в образовательной организации.

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.

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

Формирование компетенций 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	основные нормативные правовые акты в области информационной безопасности и защиты информации; место и роль информационной безопасности в информационно-образовательной среде; место и роль информационной безопасности в системе национальной безопасности Российской Федерации**;**	Отметка «зачтено» выставляется, если студент в целом за семестр набрал от 51 до 100 баллов (с учетом баллов, набранных на промежуточной аттестации (зачете)). Отметка «не зачтено» выставляется, если студент в целом за семестр набрал менее 51 балла (с учетом баллов, набранных на промежуточной аттестации (зачете)).
Умения	формулировать и проектировать политику информационной безопасности образовательных организаций; анализировать и оценивать угрозы информационной безопасности личности;	
Навыки	навыками безопасного использования технических и программных средств защиты информации в образовательных организациях; навыками организации и обеспечения режима защиты персональных данных в информационно-образовательной среде в учебной и внеучебной деятельности.	

способностью использовать базовые правовые знания в различных сферах деятельности (ОК-7)

Планируемые результаты обучения	**Критерии оценивания с весовым коэффициентом**	**Показатели оценивания**				
		1	2	3	4	5

Выпускник знает основные нормативные правовые акты в области информационной безопасности и защиты информации;	когнитивный – 0.4	Знает понятие информационной безопасности на интуитивном уровне	Знает понятие информационной безопасности, модели, принципы и средства ИБ на интуитивном уровне	Знает понятие ИБ, методы и средства	Знает понятие, принципы, методы и модели ИБ, частично знаком с правовыми основами	Знает понятия, принципы, методы, средства, правовые основы и модели информационной безопасности
анализировать и оценивать угрозы информационной безопасности личности;	деятельностный – 0,2	не умеет анализировать и оценивать угрозы информационной безопасности личности;	частично может анализировать и оценивать угрозы информационной безопасности личности;	несистематично может анализировать и оценивать угрозы информационной безопасности личности;	демонстрирует умение анализировать и оценивать угрозы информационной безопасности личности;	способен анализировать и оценивать угрозы информационной безопасности личности;
владеет навыками безопасного использования технических и программных средств защиты информации в образовательных организациях	деятельностный – 0,4	не владеет навыками безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов	частично владеет навыками безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов	несистематично может осуществлять использование технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов	демонстрирует умение безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов	способен осуществлять безопасное использование технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов

способностью использовать приемы оказания первой помощи, методы защиты в условиях чрезвычайных ситуаций (ОК-9)

Планируемые результаты обучения	**Критерии оценивания с весовым коэффициентом**	**Показатели оценивания**				
		1	2	3	4	5
Выпускник знает место и роль информационной безопасности в информа-ционно-образовательной среде;	когнитивный – 0.4	Знает место информационной безопасности на интуитивном уровне	Знает место и роль информационной безопасности на интуитивном уровне	Знает частично место информационной безопасности	Знает частично роль и место информационной безопасности	Знает место и роль информационной безопасности в информационно-образовательной среде
формулировать и проектировать политику информационной безопас-	деятельностный – 0,6	не умеет формулировать и проектировать политику информаци-	частично может формулировать и проектировать политику информа-	несистематично может формулировать и проектировать политику	демонстрирует умение формулировать и проектировать политику	способен формулировать и проектировать политику информаци-

ности образовательных организаций		онной безопасности образовательных организаций	ци-онной безопасности образовательных организаций	информационной безопасности образовательных организаций	информационной безопасности образовательных организаций	онной безопасности образовательных организаций

способностью решать задачи воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности (ПК-3)						
Планируемые результаты обучения	**Критерии оценивания с весовым коэффициентом**	**Показатели оценивания**				
		1	2	3	4	5
Выпускник знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации	когнитивный – 0.4	Знает место информационной безопасности на интуитивном уровне	Знает место и роль информационной безопасности на интуитивном уровне	Знает частично место информационной безопасности	Знает частично роль и место информационной безопасности	Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации
умеет анализировать и оценивать угрозы информационной безопасности личности	деятельностный – 0,2	не умеет анализировать и оценивать угрозы информационной безопасности личности;	частично может анализировать и оценивать угрозы информационной безопасности личности;	несистематично может анализировать и оценивать угрозы информационной безопасности личности;	демонстрирует умение анализировать и оценивать угрозы информационной безопасности личности;	способен анализировать и оценивать угрозы информационной безопасности личности;
Владеет навыками организации и обеспечения режима защиты персональных данных в информационно-образовательной среде в учебной и внеучебной деятельности	деятельностный – 0,4	не владеет организации и обеспечения режима защиты персональных дан-ных	частично владеет навыками организации и обеспечения режима защиты персональных данных	несистематично может осуществлять организациию и обеспечениие режима защиты персональных данных в информационно-образовательной среде в учебной и внеучебной деятельности	демонстрирует умение организации и обеспечения режима защиты персональных данных в информационно-образовательной среде в учебной и внеучебной деятельности	способен к организации и обеспечению режима защиты персональных данных в информационно-образовательной среде в учебной и внеучебной деятельности

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

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

Практическое занятие №2. Правовые аспекты деятельности в глобальной сети Интернет

Практическое занятие №3. Способы защиты от вирусов. Антивирусные программы. Сравнение функций родительского контроля в составе антивирусных программ

Практическое занятие №4. Планирование мероприятий по защите персональных данных в образовательной организации.

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, 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.

Примерный 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:

- 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. Роль информации в современном мире. Понятие о защищаемой информации.
2. Теория информационной безопасности. Основные направления.
3. Обеспечение ИБ и направления защиты.
4. Требования к системе и политике ИБ.
5. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
6. Доктрина информационной безопасности РФ.
7. Защита государственной тайны в РФ.
8. Защита коммерческой тайны в РФ.
9. Защита персональных данных в РФ.
10. Защита служебной и профессиональной тайны в РФ.
11. Процедуры сертификации и аттестации в РФ.
12. Понятие о защищаемой информации. Свойства информации.
13. Угрозы информации. Классификация угроз.

14. Угрозы нарушения конфиденциальности информации. Особенности и примеры реализации угроз.
15. Угрозы нарушения целостности информации. Особенности и примеры реализации угроз.
16. Угроза нарушения доступности информации. Особенности и примеры реализации угрозы.
17. Источники угроз. Классификация источников угроз.
18. Идентификация и аутентификация. Использование парольной защиты. Недостатки парольной защиты.
19. Понятие электронной подписи.
20. Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия.
21. Организация внутриобъектового режима предприятия. Организация охраны.
22. Криптографические меры обеспечения информационной безопасности. Классификация криптографических алгоритмов.
23. Программно-аппаратные защиты информации. Межсетевые экраны, их функции и назначения.
24. Программно-аппаратные защиты информации. Антивирусные средства, их функции и назначения.
25. Особенности защиты беспроводных и мобильных подключений.

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

Рейтинг по дисциплине «Информационная безопасность и защита персональных данных»

Итоговая оценка за дисциплину состоит из следующих составляющих:

1) Текущий контроль (общий вес 70 баллов): до 12 баллов - посещение лекций; до 26 баллов - выполнение практических работ (выполнение индивидуальных лабораторных заданий, самостоятельная работа)

2) Итоговый контроль заключается в проведении зачета (общий вес - 30 баллов): тестирования, ответы на контрольные вопросы. Если зачет принимается тестированием, полученный процент ответов представляет собой 40% итоговой оценки. Зачет может быть проведен в форме публичной защиты проектов по темам выбранного профиля обучения. 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 баллов по каждой составляющей и выполнить все практические задания.

Если задание выполнено с ошибками или незакончено количество баллов снижается. В случае несвоевременного представления решенного задания количество баллов уменьшается в 2 раза.

Шкала перевода баллов в оценку: до 50 баллов - «не зачтено»; 51 - 100 - «зачтено».

№ п/п	Содержание занятия	количество часов	баллы
1.	Основные понятия ИБ	1	2
2.	Правовые аспекты деятельности в глобальной сети Интернет	1	2
3.	Безопасность и конфиденциальность в Интернете	1	2
4.	Способы защиты от вирусов. Антивирусные	1	2

	программы		
5.	Установка паролей, разграничение доступа	1	4
6.	Работа с сетевыми экранами, программами: анти-спам анти-шпион	1 Сам. работа	4
7.	Основные принципы стенографии, кодирования и шифрования	2	4
8.	Сравнение функций родительского контроля в составе антивирусных программ	1 Сам.раб.	2
9.	Составление каталога Интернет-ресурсов, полезных для воспитания, образования и развития детей	1	4
10.	Посещение лекций	4	12
11.	Выполнение заданий в LMS Moodle	Сам. работа	14
12.	Выполнение и защита индивидуального проекта «Принципы комплексного подхода к обеспечению информационной безопасности»	Сам. работа	18
Итого		**10**	**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

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

3. 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

4. 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. 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
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. Научная педагогическая электронная библиотека [Электронный ресурс] : сетевая информационно-поисковая система РАО / Российская Академия образования ; ФГНУ «Научная

педагогическая библиотека имени К. Д. Ушинского» . - М. : [б. и.], [2000]. - Загл. с титул. экрана. - Б. ц.
URL: http://elib.gnpbu.ru/

4. 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
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
6. 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
7. Российское образование [Электронный ресурс] : федеральный портал / ФГУ ГНИИ ИТТ "Информика". - М. : [б. и.], 2002. - Загл. с титул. экрана. - Б. ц. URL: www.edu.ru
8. Руконт [Электронный ресурс] : национальный цифровой ресурс / ООО «Агентство Книга-Сервис». - М. : [б. и.], 2011. - Загл. с титул. Экрана URL: http://www.rucont.ru
9. 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
10. 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

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 за-висит 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.

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 лекционных и практических занятий); - программное обеспечение (Microsoft Office (Excel, Power Point, Word и т.д.), Skype, по- исковые системы, электронная почта и т.п.);
- среда электронного обучения ТГПУ им. Л.Н. Толстого http://moodle.tsput.ru.

При осуществлении образовательного процесса по дисциплине информационно-коммуникационные технологии используются для подготовки отчетов к практическим занятиям и выполнения самостоятельной работы.

При организации самостоятельной работы современные информационные и коммуникационные технологии используются для обращения к электронным образовательным ресурсам.

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

• составление библиографии;

• анализ и рецензирование публикации (в том числе электронных) источников по своей предметной области;

• составление аннотированного списка научно-исследовательской литературы;

• конспектирование и реферирование первоисточников и научно-исследовательской литературы по тематическим блокам дисциплины.

Дисциплина обеспечена комплектом 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.

У обучающихся имеется доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых ежегодно обновляется:

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 осуществляется на соответствующей материально-технической базе. Так, обучение по дисциплине проходит в специальных помещениях для проведения занятии лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также в помещениях 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 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 должны быть сформированы следующие компетенции:

способностью использовать базовые правовые знания в различных сферах деятельности (ОК-7);

способностью использовать приемы оказания первой помощи, методы защиты в условиях чрезвычайных ситуаций (ОК-9)

способностью решать задачи воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности (ПК-3);

2. Место дисциплины в структуре ООП.

Дисциплина «Информационная безопасность и защита персональных данных» относится к дисциплинам Блока 1 вариативной части дисциплин направления.

Изучение данной дисциплины базируется на освоении студентами дисциплин «ИКТ в профессиональной деятельности», «Педагогика», «Психология».

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. Планируемые результаты обучения по дисциплине.

В результате освоения дисциплины студент должен приобрести:

знания: основные нормативные правовые акты в области информационной безопасности и защиты информации; место и роль информационной безопасности в информационно-образовательной среде; место и роль информационной безопасности в системе национальной безопасности Российской Федерации**;**

умения: формулировать и проектировать политику информационной безопасности образовательных организаций; анализировать и оценивать угрозы информационной безопасности личности;

навыки: навыками безопасного использования технических и программных средств защиты информации в образовательных организациях; навыками организации и обеспечения режима защиты персональных данных в информационно-образовательной среде в учебной и внеучебной деятельности

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

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 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