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»

Трудоемкость: 3 зачетные единицы

Квалификация выпускника: Бакалавр

Форма обучения: очная

Год начала подготовки: 2014

И. о. заведующего кафедрой _____ Ю.И. Богатырева

Декан факультета _____ И.Ю. Реброва

СОДЕРЖАНИЕ

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

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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4).	***Выпускник знает:*** основные понятия, принципы, методы, средства, правовые основы и модели информационной безопасности; ***Умеет:*** формулировать и проектировать политику информационной безопасности в ИС; ***Владеет и (или) имеет опыт деятельности :*** навыками безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов.	В соответствии с учебным планом и планируемыми результатами освоения ОПОП

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП БАКАЛАВРИАТА

Дисциплина «Информационная безопасность» относится к дисциплинам базовой части учебного плана Блок 1. Дисциплины (модули).

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы	**Объем зачетных единиц / часов по формам обучения**	
	очная	**заочная**
Максимальная учебная нагрузка (всего)	3/108	
Контактная работа обучающихся с преподавателем (всего)	44	
в том числе:		
лекции	16	
лабораторные занятия (включая защиту отчета по лабораторным работам)	26	
контрольные работы	2	
другие виды контактной работы		
Самостоятельная работа студента (всего)	64	
в том числе:		
внеаудиторная самостоятельная работа по подготовке к лабораторным занятиям и защите отчета	10	
подготовка учебного проекта	20	

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

Наименование тем (разделов).	Количество академических или астрономических часов по видам учебных занятий			
	Занятия лекционного типа	Лабораторные работы	Другие виды работ	Самостоятельная работа обучающихся
Тема 1. Основные понятия информационной безопасности	2		4	6
Тема 2. Правовые основы информационной безопасности и защита интеллектуальной собственности	2		4	10
Тема 3. Виды информационных угроз и характеристики защищаемой информации	4		4	8
Тема 4. Программные средства защиты данных в ИС	2		4	8
Тема 5. Технические средства защиты и комплексное обеспечение безопасности ИС	2		2	10
Тема 6. Безопасности в сети Интернет	2		4	8
Тема 7. Политика информационной безопасности на предприятии	2		2	10
Контроль самостоятельной работы студентов		2	2	
Подготовка к зачету				4
ИТОГО	16	2	26	64

Тема 1. Основные понятия информационной безопасности

Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Модели безопасности. Понятие «национальная безопасность». Доктрина безопасности Российской Федерации.

Основные принципы обеспечения информационной безопасности.

Лабораторные работы с использованием электронных образовательных ресурсов: классификация информационной системы персональных данных.

Тема 2. Правовые основы информационной безопасности и защита интеллектуальной собственности

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.

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.

История создания правового института по охране авторского права. Субъекты авторского права. Права обладателей авторских прав. Авторские и патентные права. Ущерб от незаконного использования авторских и смежных прав. Интеллектуальная собственность.

Всемирная конвенция об авторском праве. Основные институты и понятия международного авторского права. Произведения, пользующиеся охраной.

Лабораторные работы с использованием электронных образовательных ресурсов: правовые аспекты деятельности в глобальной сети Интернет;

Тема 3. Виды информационных угроз и характеристики защищаемой информации

Факторы, риски угроз информационным ресурсам. Виды угроз и типы атак. Информационные войны. Информационное оружие. Анализ и оценивание угроз информационной безопасности личности в современном информационном обществе

Классификация компьютерных преступлений. Группы компьютерных преступлений. Хакерство в мире и в России. Закрытие информации как средство ее защиты от несанкционированного доступа.

Угрозы информационно-психологической безопасности личности и их основные источники. Сущность и современное состояние манипуляции сознанием и поведением людей. Информационная среда иллюзии и реальности.

Понятие о защищаемой информации. Виды защищаемой информации. Свойства информации как предмета защиты. Классификация информации по категории доступа. Виды информации. Понятие ценности информации. Перечень сведений, доступ к которым не может быть ограничен. Понятие конфиденциальной информации, ее виды.

Лабораторные работы с использованием электронных образовательных ресурсов: Работа с сетевыми экранами, программами: анти-спам анти-шпион. Основные принципы стенографии, кодирования и шифрования.

Тема 4. Программные средства защиты данных в ИС

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

Лабораторные работы с использованием электронных образовательных ресурсов: Способы защиты от вирусов. Антивирусные программы.

Тема 5. Технические средства защиты и комплексное обеспечение безопасности ИС

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.

Лабораторные работы с использованием электронных образовательных ресурсов: установка паролей, разграничение доступа. Развертывание защищенной VPN-сети средствами ViPNet.

Тема 6. Безопасности в сети Интернет

Классификация Интернет-угроз. Роль Интернета в мировом информационном пространстве. Понятие и виды сетевых атак. Основные угрозы в Интернете для информационных систем и сервисов. Защита и управление репутацией в Интернете. Антиспамовые средства.

Основные психолого-педагогические приемы и средства по обеспечению информационной безопасности в Интернете. Технологии виртуального взаимодействия. Виды

зависимостей. Интернет-зависимость как одно из негативных воздействий глобальной сети. Влияние социальных сетей на адаптацию молодежи

Лабораторные работы с использованием электронных образовательных ресурсов: настройка браузеров для безопасной работы в Интернете; безопасность и конфиденциальность в Интернете..

Тема 7. Политика информационной безопасности на предприятии

Концепция информационной безопасности. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в информационных система и сервисах.

Правовые нормы и стандарты по лицензированию и сертификации.

Служба информационной безопасности предприятия. Состав, цели и задачи службы информационной безопасности предприятия.

Контроль доступа к документам, электронной почте и Web-трафику.

Лабораторные работы с использованием электронных образовательных ресурсов: Рабочее пространство Web 2.0: новые возможности, новые риски. Средства анализа веб-контента. Защита проектов по дисциплине.

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 (http://moodle.tsput.ru/course/view.php?id=15588) 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 лабораторных работ

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. Развертывание защищенной VPN-сети средствами ViPNet.
6. Использование программных средств защиты ПК
7. Способы защиты от вирусов. Антивирусные программы.
8. Настройка браузеров для безопасной работы в Интернете.
9. Безопасность и конфиденциальность в Интернете.
10. Рабочее пространство Web 2.0: новые возможности, новые риски.
11. Средства анализа веб-контента.

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

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

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

Формирование компетенции «Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4)» осуществляется в несколько этапов в соответствии с учебным планом и планируемыми результатами освоения ОПОП, соотнесенными с планируемыми результатами обучения по каждой дисциплине 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 понятия, принципы, методы, средства, правовые основы и модели информационной безопасности.	Отметка «зачтено» выставляется, если студент в целом за семестр набрал от 61 до 100 баллов (с учетом баллов, набранных на промежуточной аттестации (зачете)). Отметка «незачтено» выставляется, если студент в целом за семестр набрал менее 61 балла (с учетом баллов, набранных на промежуточной аттестации (зачете)).
Умения	формулировать и проектировать политику информационной безопасности в ИС.	
Навыки и (или) опыт деятельности	навыками безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов.	

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, 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»

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.	Правовые аспекты деятельности в глобальной сети Интернет	2	2
2.	Безопасность и конфиденциальность в Интернете	2	2
3.	Способы защиты от вирусов. Антивирусные программы	2	4
4.	Установка паролей, разграничение доступа	2	4
5.	Работа с сетевыми экранами, программами: анти-спам анти-шпион	2 Сам. работа	4
6.	Основные принципы стенографии, кодирования и шифрования	2	4
7.	Сравнение функций родительского контроля в составе антивирусных программ	2 Сам.раб.	2
8.	Составление каталога Интернет-ресурсов, полезных для воспитания, образования и развития детей	2	4
9.	Посещение лекций	12	12
10.	Выполнение заданий в LMS Moodle	Сам. работа	14
11.	Выполнение и защита индивидуального проекта «Принципы комплексного подхода к обеспечению информационной безопасности»	Сам. работа	18
Итого		**28**	**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. 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 рабочей 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.

2. 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.

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

Комплект лицензионного программного обеспечения

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

Современные профессиональные базы данных и информационные справочные системы

1. Компьютерная информационно-правовая система «Гарант» - регистрационный номер клиента 71-70685-000033.
2. Официальный интернет-портал правовой информации http://pravo.gov.ru.
3. Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.
4. Портал "Информационно-коммуникационные технологии в образовании" http://www.ict.edu.ru.

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

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

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

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

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

12. АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ.

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

В результате освоения дисциплины у студента должна быть сформирована следующие компетенции: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4)

В результате освоения дисциплины студент должен приобрести:

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

умения формулировать и проектировать политику информационной безопасности в ИС;

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

2.Место дисциплины в структуре ОПОП.

Дисциплина «Технологии визуализации данных» относится к дисциплинам по выбору вариативной части учебного плана.

3. Объем дисциплины: 3 зачетные единицы.

4.Образовательный процесс осуществляется на русском языке.

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

13. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

2016-2017 учебный год

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

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

2017-2018 учебный год

Обновлен состав необходимого комплекта лицензионного программного обеспечения.

1. Операционная система Microsoft Windows XP Professional Russian – Лицензия № 16698685 от 08.08.2003 г.
2. Операционная система Microsoft Windows Professional 7 Russian – Лицензия №48497058 от 13.05.2011 г., договор № Пр/16/6 от 05 апреля 2016 года.
3. Операционная система Microsoft Windows 10 Professional Russian - контракт № ПР/ФЕН/15/18 от 23.10.2015 г., договор № Пр/16/6 от 05 апреля 2016 года.
4. Программное обеспечение Microsoft Office Enterprise 2007 Russian - Лицензия №46138962 от 16.11.2009 г.
5. Программное обеспечение Microsoft Office 2013 Professional - контракт № 405535 от 2 ноября 2015 года, контракт № ПР/ФЕН/15/18 от 23.10.2015 г.
6. Программа для распознавания текста 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