Факультет	Математики, физики и информатики	
Кафедра	Информатики и информационных технологий	
Направление	09.03.03 Прикладная информатика	
Направленность	Прикладная информатика в здравоохранении	
Информационная безопасность		Б1.Б.28

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 № 2 от 11 февраля 2016 г.

Рабочая программа дисциплины «Информационная безопасность»

Трудоемкость: 3 зачетные единицы

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Рассмотрена на заседании кафедры
информатики и информационных технологий
протокол № 4 от 24 декабря 2015 г.

Заведующий кафедрой _____А.В. Якушин

Одобрена на заседании Ученого совета факультета
Математики, физики и информатики
протокол № 6 от 21 января 2016 г.

Декан _____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:*** навыками безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов.	3 этап из 3 (8 семестр)

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП БАКАЛАВРИАТА

Дисциплина «Информационная безопасность» относится к базовой части образовательной программы. Изучение данной дисциплины осуществляется в 8 семестре. Освоение данной дисциплины базируется на знаниях математики и информатики, изученными студентами на этапе среднего образования; и изученных дисциплин в вузе, таких как: «Информатика и программирование», «Информационные системы и технологии», «Телекоммуникационные технологии». Изучение дисциплины «Информационная безопасность» может служить основой для дальнейшего освоения комплекса дисциплин специализации. К началу освоения данной дисциплины студенты должны владеть навыками работы на компьютере, знанием устройства персонального компьютера, основных методах хранения персональных данных в устройстве компьютера.

Дисциплина «Информационная безопасность» дает базовую основу для понимания, анализа и оценки основных проблем, связанных с обеспечением информационной безопасности информационных систем и сервисов, а также разработкой, внедрением и сопровождением средств информационной защиты.

В результате освоения программы студенты приобретают теоретические и практические умения и навыки применения современных информационных технологий для использования в деятельности по защите информации, а также общее представление о современных концепциях информационной безопасности и защите персональных данных.

3. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Очная форма обучения

Вид учебной работы	Объем зачетных единиц / часов по формам обучения
Максимальная учебная нагрузка (всего)	108/3
Контактная работа обучающихся с преподавателем (всего)	44
в том числе:	
лекции	16
лабораторные занятия (включая защиту отчета по лабораторным работам)	26
семинарские занятия	
практические занятия	
контрольные работы	
другие виды контактной работы (КСРС)	2
Самостоятельная работа студента (всего)	64
в том числе:	
внеаудиторная самостоятельная работа по подготовке к лекционным занятиям	
внеаудиторная самостоятельная работа по подготовке к лабораторным занятиям и защите отчета	30
внеаудиторная самостоятельная работа при подготовке к семинарским и/или практическим занятиям	
подготовка учебного проекта	
подготовка к контрольной работе	
выполнение заданий для самостоятельной работы в системе управления обучением MOODLE	30
выполнение курсового проекта (работы)	
подготовка к зачету	4
подготовка к экзамену	
другие виды самостоятельной работы студента	
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 типа	Лабораторные занятия	Другие виды учебных занятий	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	4		10
Контроль самостоятельной работы студентов			2	
Подготовка к зачету				4
ИТОГО	16	26	2	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.

Преподавание дисциплины предполагает использование следующего учебно-методического обеспечения.

Комплекта мультимедийных презентаций для лекционных занятий.

Теоретического курса и информационных приложений, размещенных в электронной образовательной среде MOODLe.

Комплекса тестовых заданий , заданий для лабораторных работ, размещенных в электронной образовательной среде MOODLe.

Виды самостоятельной работы обучающихся: выполнение заданий на лабораторные работы, тестирование.

При подготовке к занятиям и выполнении самостоятельной работы студентам доступны следующие учебно-методические ресурсы, перечисленные в п.7 рабочей программы, а также электронный учебный ресурс размещенный в среде электронного обучения ТГПУ им. Л.Н. Толстого (http://moodle.tsput.ru)

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 течение трех этапов освоения

основной образовательной программы.

Первый этап формирования компетенции осуществляется в процессе освоения дисциплины «Телекоммуникационные технологии».

Второй этап формирования компетенции осуществляется в процессе освоения дисциплины «Технологии программирования».

Третий этап формирования компетенции осуществляется в процессе освоения дисциплин «Информационная безопасность».

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

Дескриптор компетенций	Показатели оценивания	Критерии оценивания
Знания	основных понятий, принципов, методов, средств, правовых основ и моделей 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	умения формулировать и проектировать политику информационной безопасности в ИС;	
Навыки	навыки безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов.	

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 – 60	0 – 40	61-100	Зачтено
0 – 21	0 – 40	0 – 60	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

Примерные тестовые задания, размещенные в среде Moodle

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

Образцы заданий к лабораторным работам:

- 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

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.

Итоговая рейтинговая оценка по дисциплине складывается из следующих составляющих:

1) В течении семестра за выполнение заданий по курсу студент может максимально получить 40 баллов.;

2) Обязательной формой текущей аттестации знаний является итоговое тестирование 20 баллов.

3) На зачёте ответ студента может быть максимально оценен в 40 баллов.

При этом, для получения положительной итоговой оценки на зачете необходимо получить не менее 60% по каждой составляющей и выполнить все лабораторные работы. Шкала перевода баллов в оценку: до 60 - «не зачтено»; 61 - 100 - «зачтено».

№ п/п	Критерии оценивания	Максимальное количество баллов	Баллы, полученные студентом
1.	Выполнение заданий:	60	
1.1.	Лабораторные работы.	40	
1.2.	Тестирование	20	
3.	Зачет	40	
	ИТОГО:	100	

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

7.1. Основная литература

1. 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.

2. 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

3. Закон РФ «О безопасности» от 05.03.1992 №2446-1 (ред.02.03.2007) // Ведомости Верховного Совета РФ. 1992. №15. Ст. 769.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-Ф.3 // Собрание законодательства РФ. 2006. №31. Ст. 3448.

5. Богатырева Ю.И. Защита детей от вредной информации. Умное подмосковье. Портал правительства Московской области URL: http://smartmosreg.ru/courses/course/79 (дата обращения 12.01.2014).

6. Богатырева Ю.И. Организация безопасного информационного пространства школьников в Интернете: методические рекомендации для бакалавров и магистров направления 050100 Педагогическое образование, учителей, учащихся и их родителей / Ю.И. Богатырева, А.Н. Привалов, С.В Пазухина. – Тула: Изд–во ТулГУ, 2013. – 96 с.

7. Доктрина информационной безопасности РФ. Совм. Изд. Ред. «Российская газета» Международной академии информатизации. –М.: Информациология, 2000.

8. Информационная безопасность [Текст] : учебное пособие для студентов учреждений среднего профессионального образования / Т. Л. Партыка, И. И. Попов. - 3-е изд., перераб. и доп. - М : Форум, 2008. - 432 с. : ил. - ISBN 9785911342463

9. Методы и средства защиты информации в компьютерных системах [Текст] : учебник для вузов / П. Б. Хорев. - [Б. м.] : Академия, 2005. - 256 с. - ISBN 5769518391

10. Модели безопасности компьютерных систем [Текст] : учеб.пособ.для студ.вузов / П. Н. Девянин. - [Б. м.] : Академия, 2005. - 144 с. - ISBN 5769520531

11. 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

12. Основы информационной безопасности [Текст] : курс лекций для студ.вузов / В. А. Галатенко, 2-е изд.,испр. - [Б. м.] : ИНТУИТ.РУ, 2004. - 264 с. - ISBN 5955600159

13. Основы информационной безопасности [Текст] : учеб.пособ.для студ.вузов / С. П. Растор-

гуев. - 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 лабораторных 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, по-

нятий, 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 лабораторных занятий по данной дисциплине является закрепление теоретических знаний, полученных при изучении дисциплины и формирование и развитие умений и навыков.

При подготовке к лабораторному 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 заданий к лабораторным работам 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 лабораторной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению. 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;
9) Применение эвристических и проблемно-поисковых технологий по изучаемому курсу;
10) Использование активных и диалоговых технологий;

Тематика лабораторных работ по дисциплине.

№	Наименование лабораторных работ	Объем в часах
1	Классификация информационной системы персональных данных.	2
2	Организация парольной защиты.	2
3	Построение системы защиты ПК от негативных последствий работы в сети Интернет.	2
4	Применение криптографических средств для защиты конфиденциальной информации на компьютере.	2
5	Развертывание защищенной VPN-сети средствами ViPNet.	2
6	Использование программных средств защиты ПК	2
7	Способы защиты от вирусов. Антивирусные программы.	2
8	Настройка браузеров для безопасной работы в Интернете.	2
9	Безопасность и конфиденциальность в Интернете.	2
10	Рабочее пространство Web 2.0: новые возможности, новые риски.	4
11	Средства анализа веб-контента.	4
	Итого	26

Типовые задания для самостоятельной работы по дисциплине

1. Опишите современную концепцию информационной безопасности
2. Охарактеризуйте направления обеспечения безопасности (правовая, организационная и инженерно-техническая защита)
3. Опишите возможные угрозы для конфиденциальной информации
4. Составьте перечень законов относящихся к информационной безопасности и защите информации, включая конфиденциальное делопроизводство.
5. Весь список разделите на следующие группы законов:
6. 1) участие в международном обмене и доступ к мировым ресурсам;
7. 2) внутригосударственные законы о защите информации

3) законы, постановления, инструкции, акты о защищенном документообороте

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

Материально-техническое обеспечение дисциплины «Информационная безопасность»:

1. Специально оборудованные аудитории и компьютерные классы: персональные компьютеры (модели: Intel Pentium4, AMD Athlon, AMD Duron), мультимедийные проекторы, аудиовизуальные устройства;
2. Программное обеспечение в соответствии с программой курса;
3. Методические пособия и литература в библиотеке университета и на кафедре.
4. Студентам обеспечен доступ к сети Internet.

Перечень лицензионного программного обеспечения, используемого при освоении дисциплины:

1. Подписка Microsoft DreamSpark Premium - Сублицензионный договор № S-2042626/M18 от 04.06.2013:

1.1. Средства для разработки и проектирования Visual Studio 2008, 2010, 2012 и 2013 Professional Editions;

1.2. Операционная система Windows 7 Professional;
1.3. Операционная система Windows 8 Pro;
1.4. Операционная система Windows 8.1 Pro;
1.5. Отдельные программы из Office 2007, Office 2010, Office 2013 (в том числе Access, Visio, Project и др.);

При чтении лекций по всем темам активно используется компьютерная техника для демонстрации слайдов с помощью программного приложения Microsoft Power Point. На лабораторных занятиях студенты представляют презентации, подготовленные с помощью программного приложения Microsoft Power Point, подготовленные ими в часы самостоятельной работы.

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 определяется в рабочих программах дисциплин и подлежит ежегодному обновлению:

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. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц. URL: http://www.mathnet.ru
5. 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
6. 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
7. 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
8. 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

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

1. Учебные аудитории для проведения занятий лекционного типа, оборудованные мультимедийными средствами обучения.
2. Учебные аудитории для проведения лабораторных занятий.
3. Компьютерные классы с доступом в интернет для работы с информационно-правовыми системами, в том числе «Гарант» и с доступом к электронно-библиотечной системе.
4. Аудитории для самостоятельной работы студентов, оснащенные компьютерной техникой, имеющей доступ к информационно-телекоммуникационной сети «Интернет», электронной информационно-образовательной среде ТГПУ им. Л.Н. Толстого, внутривузовскому сетевому окружению.

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: 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 «Информационная безопасность» относится к дисциплинам базовой части образовательной программы.

3. Объем дисциплины 3 зачетные единицы.
4. Образовательный процесс осуществляется на русском языке.

Разработчик: Богатырева Ю.И., д.п.н., доцент кафедры И и ИТ

13. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

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

2) Обновлен п.10 «Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем» на основании действующих лицензионных соглашений

Заведующий кафедрой ИиИТ _____ А.В. Якушин

«26» августа 2016 г..

Информационная безопасность | Б1.Б.28

Программа составлена в соответствии с требованиями ФГОС ВО.

Разработчик (и):

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Информационная безопасность»

Состав:

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ С УКАЗАНИЕМ ЭТАПОВ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

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: навыками безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов.	3 этап из 3 (8 семестр)

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 течение трех этапов освоения основной образовательной программы.

Первый этап формирования компетенции осуществляется в процессе освоения дисциплины «Телекоммуникационные технологии».

Второй этап формирования компетенции осуществляется в процессе освоения дисциплины «Технологии программирования».

Третий этап формирования компетенции осуществляется в процессе освоения дисциплин «Информационная безопасность».

2. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Дескриптор компетенций	Показатели оценивания	Критерии оценивания
Знания	основных понятий, принципов, методов, средств, правовых основ и моделей 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	умения формулировать и проектировать политику информационной безопасности в ИС;	
Навыки	навыки безопасного использования технических и программных средств защиты информации для эксплуатации и сопровождения информационных систем и сервисов.	

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 – 60	0 – 40	61-100	Зачтено
0 – 21	0 – 40	0 – 60	Не зачтено

3. КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ В ПРОЦЕССЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

.

3.1. Вопросы к зачету

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.

Критерии оценки зачета по дисциплине

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.

3.2. Тестовые задания

3.2.1. Список тествых заданий

Вопрос 1
Элементы знака охраны авторского права:
Выберите один или несколько ответов:
a. буквы Р в окружности или круглых скобках
b. наименование охраняемого объекта

c. буквы С в окружности или круглых скобках
d. наименования (имени) правообладателя
e. года первого выпуска программы
Вопрос 2
Типы троянов:
Выберите один или несколько ответов:
a. шутки
b. логические бомбы
c. вирусные мистификации
d. утилиты скрытого удаленного управления
e. похитители паролей
f. дефрагментаторы дисков
g. клавиатурные шпионы
Вопрос 3
?Основные угрозы доступности информации:
Выберите один или несколько ответов:
a. хакерская атака
b. непреднамеренные ошибки пользователей
c. перехват данных
d. злонамеренное изменение данных
e. отказ программного и аппаратно обеспечения
Вопрос 4
Главное преимущество встроенного в Microsoft Windows XP (с установленным Service Pack 2) брандмауэра по сравнению с устанавливаемыми отдельно персональными брандмауэрами
Выберите один ответ:
a. отсутствие необходимости отдельно покупать его и устанавливать
b. более ясный и интуитивно понятный интерфейс
c. возможность более точно задавать исключения
d. наличие более полного функционала
Вопрос 5
Антиспамовая программа, установленная на домашнем компьютере, служит для …
Выберите один ответ:
a. обеспечения регулярной доставки антивирусной программе новых антивирусных баз
b. защиты компьютера от хакерских атак
c. защиты компьютера от нежелательной и/или не запрошенной корреспонденции
d. корректной установки и удаления прикладных программ
Вопрос 6
В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …
Выберите один или несколько ответов:
a. соблюдение конфиденциальности информации ограниченного доступа
b. соблюдение норм международного права в сфере информационной безопасности
c. реализацию права на доступ к информации
d. разработку методов и усовершенствование средств информационной безопасности
e. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
f. выявление нарушителей и привлечение их к ответственности
Вопрос 7
Преимущества сигнатурного метода антивирусной проверки над эвристическим
Выберите один ответ:
a. существенно менее требователен к ресурсам
b. более надежный

c. позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы
d. не требует регулярного обновления антивирусных баз
Вопрос 8
Методы повышения достоверности входных данных
Выберите один или несколько ответов:
a. Отказ от использования данных
b. Проведение комплекса регламентных работ
c. Использование вместо ввода значения его считывание с машиночитаемого носителя
d. Замена процесса ввода значения процессом выбора значения из предлагаемого множества
e. Введение избыточности в документ первоисточник
f. Многократный ввод данных и сличение введенных значений
Вопрос 9
Выполнение вредоносной программой, относящейся к классическим утилитам дозвона, вызывает …
Выберите один ответ:
a. материальные проявления
b. косвенные проявления
c. явные проявления
d. скрытые проявления
Вопрос 10
Концепция системы защиты от информационного оружия не должна включать…
Выберите один ответ:
a. процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей
b. механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
c. признаки, сигнализирующие о возможном нападении
d. средства нанесения контратаки с помощью информационного оружия
Вопрос 11
Брандмауэр (firewall) – это программа, …
Выберите один ответ:
a. которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл подробную статистику сетевой активности
b. реализующая простейший антивирус для скриптов, использующихся в Интернет активных элементах
c. на основе которой строится система кэширования загружаемых веб-страниц
d. которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил
Вопрос 12
Свойство вируса, позволяющее называться ему загрузочным – способность …
Выберите один ответ:
a. подсвечивать кнопку Пуск на системном блоке
b. заражать загрузочные дискеты и компакт-диски
c. вызывать перезагрузку компьютера-жертвы
d. заражать загрузочные сектора жестких дисков
Вопрос 13
Информация, составляющая государственную тайну не может иметь гриф…
Выберите один ответ:
a. «особой важности»
b. «для служебного пользования»
c. «совершенно секретно»
d. «секретно»
Вопрос 14

Разделы современной криптографии:
Выберите один или несколько ответов:
a. Симметричные криптосистемы
b. Управление передачей данных
c. Управление паролями
d. Криптосистемы с дублированием защиты
e. Криптосистемы с открытым ключом
f. Управление ключами
g. Системы электронной подписи
Вопрос 15
Скрытые проявлениям вирусного заражения:
Выберите один или несколько ответов:
a. неожиданно появляющееся всплывающее окно с приглашением посетить некий сайт
b. наличие на рабочем столе подозрительных ярлыков
c. наличие в оперативной памяти подозрительных процессов
d. наличие на компьютере подозрительных файлов
e. подозрительная сетевая активность
f. неожиданное уведомление антивирусной программы об обнаружении вируса
Вопрос 16
Обязательные свойства любого современного антивирусного комплекса
Выберите один или несколько ответов:
a. интегрироваться в браузер
b. не мешать выполнению основных функций компьютера
c. быть кроссплатформенным (работать под управлением любой операционной системы)
d. не занимать канал Интернет
e. надежно защищать от вирусов
f. не занимать много системных ресурсов
Вопрос 17
Ограничения, которые накладывает отсутствие на домашнем компьютере постоянного выхода в Интернет
Выберите один ответ:
a. невозможность запуска антивирусной проверки в режиме реального времени
b. ложные срабатывания в работе персонального брандмауэра
c. трудности с регулярным автоматическим получением новых антивирусных баз
d. невозможность использовать антиспамовую программу в режиме реального времени
Вопрос 18
Защита информации обеспечивается применением антивирусных средств
Выберите один ответ:
a. не всегда
b. нет
c. да
Вопрос 19
Вирус – это программа, способная…
Выберите один ответ:
a. нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети
b. уничтожить диск компьютера
c. создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты, при этом дубликаты сохраняют способность к дальнейшему распространению
d. нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети: прямо или посредством других программ и/или приложения
Вопрос 20

Суть компрометации информации
Выберите один ответ:
a. несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
b. внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
c. внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений
Вопрос 21
К формам защиты информации не относится…
Выберите один или несколько ответов:
a. страховая
b. аналитическая
c. правовая
d. организационная
e. инженерно-техническая
Вопрос 22
Типы методов антивирусной защиты
Выберите один или несколько ответов:
a. практические
b. теоретические
c. программные
d. организационные
e. технические
Вопрос 23
Преднамеренная угроза безопасности информации
Выберите один ответ:
a. наводнение
b. повреждение кабеля, по которому идет передача, в связи с погодными условиями
c. ошибка разработчика
d. кража
Вопрос 24
Стадии жизненного цикла классического трояна:
Выберите один или несколько ответов:
a. активация
b. подготовка копий
c. внедрение копий
d. поиск объектов для заражения
e. выполнение вредоносных действий
f. проникновение на чужой компьютер
Вопрос 25
Антивирусные базы можно обновить на компьютере, не подключенном к Интернет.
Выберите один ответ:
a. да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы
b. да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором
c. нет
Вопрос 26

Необходимость модуля обновления для любого современного антивирусного средства – для …
Выберите один ответ:
a. подключения антивирусных баз к антивирусной программе
b. обеспечения взаимодействия операционной системы с антивирусным комплексом
c. взаимодействия антивирусной программы с сайтом компании-производителя
d. доставки сигнатур на компьютеры всех пользователей, использующих соответствующую антивирусную программу
Вопрос 27
Трояны классифицируются по …
Выберите один ответ:
a. методу маскировки
b. типу вредоносной нагрузки
c. методу распространения
d. методу размножения
Вопрос 28
Задача, выполняющая модуль планирования, входящий в антивирусный комплекс
Выберите один ответ:
a. настройки параметров уведомления пользователя о важных событиях в жизни антивирусного комплекса
b. определения областей работы различных задач поиска вирусов
c. определения параметров взаимодействия различных компонентов антивирусного комплекса
d. настройка расписания запуска ряда важных задач (проверки на вирусы, обновления антивирусных баз и пр.)
Вопрос 29
Вид действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – …
Выберите один ответ:
a. кража
b. искажение
c. пассивная угроза
d. модификация
e. активная угроза
Вопрос 30
Подозрительная сетевая активность может быть вызвана …
Выберите один или несколько ответов:
a. сетевым червем
b. логической бомбой
c. трояном
d. P2P-червем
Вопрос 31
Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности:
Выберите один ответ:
a. уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer
b. уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer
c. возможность одновременно работать в нескольких окнах
d. возможность установить отличную от www.msn.com стартовую страницу
Вопрос 32
Логические бомбы относятся к классу …
Выберите один ответ:

a. условно опасных программ
b. макровирусов
c. сетевых червей
d. троянов
e. файловых вирусов
Вопрос 33
Основные угрозы конфиденциальности информации:
Выберите один или несколько ответов:
a. карнавал
b. перехват данных
c. блокирование
d. переадресовка
e. злоупотребления полномочиями
Вопрос 34
Деятельность клавиатурных шпионов
Выберите один ответ:
a. передают злоумышленнику марку и тип используемой пользователем клавиатуры
b. находясь в оперативной памяти следят за вводимой пользователем информацией и по команде злоумышленника производят нужную ему замену одних символов (или групп символов) другими
c. находясь в оперативной памяти следят за вводимой информацией и как только пользователь введет кодовое слово, клавиатурный шпион начинает выполнять вредоносные действия, заданные автором
d. находясь в оперативной памяти записывают все, что пользователь вводит с клавиатуры и передают
e. переписывает пароли туда, откуда их может без особого труда извлечь злоумышленник.
Вопрос 35
К классу условно опасных относятся программы …
Выберите один ответ:
a. характеризующиеся способностью при срабатывании заложенных в них условий выполнять какое-либо действие, например, удаление файлов, в остальное время они безвредны
b. последствия выполнения которых нельзя предугадать
c. о которых нельзя однозначно сказать, что они вредоносны
d. которые можно выполнять только при наличии установленного антивирусного программного обеспечения
Вопрос 36
Утечка информации – это …
Выберите один ответ:
a. это бесконтрольный выход конфиденциальной информации за пределы организации или
b. процесс уничтожения информации
c. процесс раскрытия секретной информации
d. круга лиц, которым она была доверена
e. непреднамеренная утрата носителя информации
Вопрос 37
Сервисы безопасности:
Выберите один или несколько ответов:
a. идентификация и аутентификация
b. экранирование
c. кэширование записей
d. регулирование конфликтов
e. обеспечение безопасного восстановления
f. шифрование
g. инверсия паролей
h. контроль целостности

Вопрос 38
Наиболее эффективное средство для защиты от сетевых атак
Выберите один ответ:
a. использование антивирусных программ
b. использование только сертифицированных программ-броузеров при доступе к сети Интернет
c. использование сетевых экранов или «firewall»
d. посещение только «надёжных» Интернет-узлов
Вопрос 39
Использование брандмауэров относят к …
Выберите один ответ:
a. организационным
b. практическим
c. техническим
d. теоретическим
e. методам антивирусной защиты.
Вопрос 40
Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …
Выберите один ответ:
a. с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
b. способна противостоять только информационным угрозам, как внешним так и внутренним
c. способна противостоять только внешним информационным угрозам
d. с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
Вопрос 41
К какому типу Использование инструкций по работе за компьютером, введенные в отдельно взятом компьютерном классе, можно отнести к …
Выберите один ответ:
a. методам антивирусной защиты
b. организационным
c. практическим
d. техническим
e. теоретическим
Вопрос 42
Основная задача, которую решает антивирусная проверка в режиме реального времени
Выберите один ответ:
a. предоставление возможности глубокой проверки заданных объектов
b. обеспечение непрерывности антивирусной проверки
c. обеспечение взаимодействия между пользователем и антивирусной программой
d. обеспечение невмешательства в процесс деятельности других программ
Вопрос 43
Преимущества эвристического метода антивирусной проверки над сигнатурным
Выберите один или несколько ответов:
a. не требует регулярного обновления антивирусных баз
b. позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы
c. существенно менее требователен к ресурсам
d. более надежный
Вопрос 44
Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
Выберите один ответ:

a. перехвата или подмены данных на путях транспортировки
b. поставки неприемлемого содержания
c. вмешательства в личную жизнь
d. внедрения агрессивного программного кода в рамках активных объектов Web-страниц
e. несанкционированного управления удаленным компьютером
Вопрос 45
Средства защиты объектов файловой системы основаны на…
Выберите один ответ:
a. определении прав пользователя на операции с файлами и каталогами
b. ограничении прав пользователя
c. задании атрибутов файлов и каталогов, независящих от прав пользователей
d. определении допустимых операций с файлами и каталогами

3.2.2. Критерии оценки тестовых заданий

При тестировании число всех верных ответов берется за 100%.

Для оценки тестов применяется следующая методика баллов за данный вид работы:

Процент выполненных тестов умножается на максимальное количество баллов, определяемое бально-рейтинговой системой по дисциплине.

3.3. Содержание и типовые задания к лабораторным работам

Тематика лабораторных работ по дисциплине.

№	Наименование лабораторных работ	Объем в часах
1	Классификация информационной системы персональных данных.	2
2	Организация парольной защиты.	2
3	Построение системы защиты ПК от негативных последствий работы в сети Интернет.	2
4	Применение криптографических средств для защиты конфиденциальной информации на компьютере.	2
5	Развертывание защищенной VPN-сети средствами ViPNet.	2
6	Использование программных средств защиты ПК	2
7	Способы защиты от вирусов. Антивирусные программы.	2
8	Настройка браузеров для безопасной работы в Интернете.	2
9	Безопасность и конфиденциальность в Интернете.	2
10	Рабочее пространство Web 2.0: новые возможности, новые риски.	4
11	Средства анализа веб-контента.	4
	Итого	26

Образцы заданий к лабораторным работам:

- 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.

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

.

Описание балльно-рейтинговой системы по дисциплине.

Итоговая рейтинговая оценка по дисциплине складывается из следующих составляющих:

1) В течении семестра за выполнение заданий по курсу студент может максимально получить 40 баллов.;

2) Обязательной формой текущей аттестации знаний является итоговое тестирование 20 баллов.

3) На зачёте ответ студента может быть максимально оценен в 40 баллов.

При этом, для получения положительной итоговой оценки на зачете необходимо получить не менее 60% по каждой составляющей и выполнить все лабораторные работы. Шкала перевода баллов в оценку: до 60 - «не зачтено»; 61 - 100 - «зачтено».

№ п/п	Критерии оценивания	Максимальное количество баллов	Баллы, полученные студентом
1.	Выполнение заданий:	60	
1.1.	Лабораторные работы.	40	
1.2.	Тестирование	20	
3.	Зачет	40	
	ИТОГО:	100	