МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНТРАНС РОССИИ)
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)
ФГБОУ ВО «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ»
(ФГБОУ ВО СПбГУ ГА)

УТВЕРЖДАЮ
Первый
проректор-проректор
по учебной работе
_____ Н. Н. Сухих
«30» августа 2017 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

Направление подготовки
01.03.04 Прикладная математика

Направленность программы (профиль)
Математическое и программное обеспечение систем управления

Квалификация выпускника:
бакалавр

Форма обучения:
очная

Санкт-Петербург
2017

1 Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность и защита информации» являются формирование у обучающихся знаний по основам информационной безопасности, а также приобретение ими умений и навыков применения полученных знаний в профессиональной деятельности.

Задачами освоения дисциплины «Информационная безопасность и защита информации» являются:

– формирование у обучающихся знаний различных видов угроз, принципов создания защищенных информационных систем;

– приобретение обучающимися умений применения основного организационно-правового обеспечения информационной безопасности;

– получение обучающимися навыков обеспечения информационной безопасности в системах управления базами данных.

Дисциплина обеспечивает подготовку выпускника к научно-исследовательскому виду деятельности.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» относится к вариативной части Блока 1 «Дисциплины (модули)» и является дисциплиной по выбору

Дисциплина «Информационная безопасность и защита информации» базируется на результатах обучения, полученных при изучении дисциплины «Программные и аппаратные средства информатики», «Программирования для электронно-вычислительных машин», «Базы данных».

Дисциплина «Информационная безопасность и защита информации» является обеспечивающей для дисциплины «Программирование в сети Internet», «Современные системы программирования».

Дисциплина «Информационная безопасность и защита информации» изучается в 6 семестре.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс освоения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
Готовность к самостоятельной работе (ОПК-1)	Знать: - современные законы, стандарты, методы и

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
	технологии в области защиты информации; Уметь: - использовать современные программно-аппаратные средства защиты информации; Владеть: – современными методами обеспечения защиты информации;
Готовность применять знания и навыки управления информацией (ПК-11);	Знать: - основные программные средства защиты информации при работе на компьютере и в сети Internet и их характеристики; Уметь: - использовать средства анализа защищенности компьютера и способы устранения уязвимостей; Владеть: - навыками поиска уязвимостей компьютера с помощью специальных программных средств и их устранения.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 академических часов.

Наименование	Всего часов	Семестр
		6
Общая трудоемкость дисциплины (модуля)	108	108
Контактная работа:	72,3	72,3
лекции	36	36
практические занятия	20	20
семинары		
лабораторные работы	16	16
курсовой проект (работа)	–	–
Самостоятельная работа студента	27	27
Промежуточная аттестация:	9	9
контактная работа	0,3	0,3
самостоятельная работа по подготовке к зачёту	8,7	8,7

5 Содержание дисциплины

5.1 Соотнесения тем (разделов) дисциплины и формируемых компетенций

Темы (разделы) дисциплины	Количество часов	Компетенции		Образовательные технологии	Оценочные средства
		ОПК-1	ПК-11		
Тема 1. Информационная безопасность деятельности общества. Организационное и правовое обеспечение информационной безопасности.	22	+	+	ВК, Л, ПЗ, ЛР, СРС	У
Тема 2. Основы обеспечения информационной безопасности жизнедеятельности общества и его структур.	27	+	+	Л, ПЗ, ЛР, СРС	У
Тема 3. Основы технического обеспечения информационной безопасности.	22	+	+	Л, ПЗ, ЛР, СРС	У
Тема 4. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных системах.	28	+	+	Л, ПЗ, ЛР, СРС	У
Всего за семестр	99				
Промежуточная аттестация	9				
Итого по дисциплине	108				

Л – лекция, ПЗ – практическое занятие, СРС – самостоятельная работа студента, ВК – входной контроль, У – устный опрос, ЛР – лабораторная работа.

5.2 Темы (разделы) дисциплины и виды

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
Тема 1. Информационная безопасность деятельности общества. Организационное и правовое обеспечение информационной безопасности.	8	4	-	4	6	-	22
Тема 2. Основы обеспечения информационной безопасности жизнедеятельности общества и его структур.	10	6	-	4	7	-	27
Тема 3. Основы технического обеспечение информационной	8	4	-	4	6	-	22

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
безопасности.							
Тема 4. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных системах.	10	6	-	4	8	-	28
Всего по дисциплине	36	20	-	16	27	-	99
Промежуточная аттестация							9
Всего по дисциплине							108

Л – лекция, ПЗ – практическое занятие, С □ семинар, ЛР – лабораторная работа, СРС – самостоятельная работа студента, КР – курсовая работа (проект).

5.3 Содержание дисциплины

Тема 1. Информационная безопасность деятельности общества. Организационное и правовое обеспечение информационной безопасности.

Основные определения и составляющие информационной безопасности. Единые критерии безопасности информационных систем. Нормативные акты, руководящие документы Российской Федерации в области информационной безопасности. Обзор и сравнительный анализ стандартов информационной безопасности.

Тема 2. Основы обеспечения информационной безопасности жизнедеятельности общества и его структур.

Информационное противоборство. Ее психологическая и техническая составляющие. Угрозы информационной безопасности. Антивирусная защита в автоматизированных системах. Построение систем защиты от угроз информации в автоматизированных системах. Симметричная и асимметричная системы шифрования. Электронная цифровая подпись. Сертификация систем информационной защиты. Компьютерные вирусы и организация антивирусной защиты.

Тема 3. Основы технического обеспечение информационной безопасности.

Криптографические методы защиты информации. Алгоритмические основы криптографических систем. Уязвимости компьютеров и компьютерных сетей. Основные виды атак на компьютерные системы. Сетевые средства экранирования в автоматизированных системах. Системы анализа защищенности. Основы использования и характеристики систем обнаружения вторжений. Основы использования и характеристики систем предотвращения вторжений. Комплексные системы защиты от вторжений.

Тема 4. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных системах.

Обеспечение сохранности данных и защита персональным электронно-вычислительных машин в автоматизированных системах. Информационная безопасность систем управления базами данных. Политика безопасности в АС. Принципы построения политики безопасности. Комплекс средств защиты информации в автоматизированной системе SecretNet и Сфера. Особенности, состав, правила использования. Назначение и алгоритм работы подсистем, входящих в комплекс средств защиты информации. Администрирование в комплексе средств защиты информации, реагирование на инциденты информационной безопасности.

5.4 Практические занятия (семинары)

Номер темы дисциплины	Тематика практических занятий (семинаров)	Трудоемкость (часы)
1	Практическая работа 1. Стандарты информационной безопасности.	2
	Практическая работа 2. Информационное противоборство. Проявления информационного противоборства.	2
2	Практическая работа 3. Информационно-манипулятивные технологии.	2
	Практическая работа 4. Антивирусные средства. Поиск и нейтрализация вирусных угроз в автоматизированных системах.	2
	Практическая работа 5. Информационные угрозы в автоматизированных системах. Способы защиты.	2
3	Практическая работа 6. Средства криптографической защиты информации. Криптографические алгоритмы.	2
	Практическая работа 7. Использование сетевых средств экранирования в автоматизированных системах.	2
4	Практическая работа 8. Разработка и использование политик безопасности при работе в сетевых структурах.	2
	Практическая работа 9. Разработка и использование политик безопасности в автоматизированных системах.	2
	Практическая работа 10. Комплекс средств защиты информации Secret Net и Сфера. Особенности, правила использования.	2
Итого по дисциплине		20

5.5 Лабораторный практикум

Номер темы дисциплины	Тематика практических занятий (семинаров)	Трудоемкость (часы)
1	Лабораторная работа 1. Исследование систем защиты от угроз нарушения информации в автоматизированных системах.	2
	Лабораторная работа 2. Исследование защищенных электронных документов.	2
2	Лабораторная работа 3. Исследование атак на компьютерные системы.	2
	Лабораторная работа 4. Исследование системы анализа защищенности	2
3	Лабораторная работа 5. Исследование принципов и механизмов обнаружения и предотвращения вторжений.	2
	Лабораторная работа 6. Исследование систем обнаружения и предотвращения вторжений.	2
4	Лабораторная работа 7. Исследование настроек информационной безопасности в АС и системах управления базами данных.	2
	Лабораторная работа 8. Исследование СУБД в области информационной безопасности.	2
Итого по дисциплине		16

5.6 Самостоятельная работа

Номер темы дисциплины	Виды самостоятельной работы	Трудоемкость (часы)
1	Изучение теоретического материала [1-5]. Подготовка к устному опросу [6-11]	6
2	Изучение теоретического материала [1-5]. Подготовка к устному опросу [6-11]	7
3	Изучение теоретического материала [1-5]. Подготовка к устному опросу [6-11]	6
4	Изучение теоретического материала [1-5]. Подготовка к устному опросу [6-11]	8
Итого по дисциплине		27

5.7 Курсовые работы (проекты)

Курсовые работы (проекты) учебным планом не предусмотрены

6 Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1 Нестеров, С. А. **Информационная безопасность** [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. — М.: Издательство Юрайт, 2017. — 321 с. — (Серия: Университеты России). — ISBN 978-5-534-00258-4 — Режим доступа: https://biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7/informacionnaya-bezopasnost — Загл. с экрана

2 Щеглов, А. Ю. **Защита информации** [Электронный ресурс]: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — М.: Издательство Юрайт, 2017. — 309 с. — (Серия: Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5 — Режим доступа: https://biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E/zaschita-informacii-osnovy-teorii — Загл. с экрана

3 Полякова, Т. А. и др. **Организационное и правовое обеспечение информационной безопасности** [Электронный ресурс]: учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под ред. Т. А. Поляковой, А. А. Стрельцова. — М.: Издательство Юрайт, 2017. — 325 с. — (Серия: Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8 — Режим доступа: https://biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti — Загл. с экрана.

б) дополнительная литература:

4 Запечников, С. В. **Криптографические методы защиты информации** [Электронный ресурс]: учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М.: Издательство Юрайт, 2017. — 309 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-534-02574-3 — Режим доступа: https://biblio-online.ru/book/B27D8A2B-F86C-4F18-9F21-3E0695C0A4C0/kriptograficheskie-metody-zaschity-informacii — Загл. с экрана

5 Казарин, О. В. **Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов** / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2017. — 312 с. — (Серия: Специалист). — ISBN 978-5-9916-9043-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/395848

в) перечень ресурсов информационно-телекоммуникационной сети «Интернет»:

6 **Information Security/Информационная безопасность** [Электронный ресурс]: официальный сайт журнала «Information Security/Информационная безопасность» – Режим доступа: https://www.itsec.ru , свободный (дата обращения: 15.08.2017).

г) программное обеспечение (лицензионное), базы данных, информационно-справочные и поисковые системы:

9. **Единое окно доступа к образовательным ресурсам** [Электронный ресурс]. – Режим доступа: http://window.edu.ru/ свободный (дата обращения: 15.08.2017).

10. **Электронная библиотека научных публикаций «eLIBRARY.RU»** [Электронный ресурс] — Режим доступа: http://elibrary.ru/ (дата обращения: 15.08.2017).

11. **Электронно-библиотечная система издательства «Лань»** [Электронный ресурс] — Режим доступа: http://e.lanbook.com/ (дата обращения: 15.08.2017).

7 Материально-техническое обеспечение дисциплины

Компьютерные классы (ауд. 801, 803), оборудованные персональными компьютерами, с выходом в сеть Интернет.

Инсталлированные изучаемые средства прикладного и инструментального программного обеспечения: MS Office, антивирус «Лаборатории Касперского»

Доска для записей при чтении лекции, проведении практических занятий.

Проекционное оборудование для сопровождения лекций и практических занятий.

8 Образовательные и информационные технологии

Дисциплина «Информационная безопасность и защита информации» предполагает использование следующих образовательных технологий: входной контроль, лекции, практические занятия и самостоятельная работа студента.

Входной контроль проводится преподавателем в начале изучения дисциплины с целью коррекции процесса усвоения студентами дидактических единиц. Он осуществляется по вопросам дисциплин, на которых базируется дисциплина «Информационная безопасность и защита информации» (п.2).

Лекция как образовательная технология представляет собой устное, систематически последовательное изложение преподавателем учебного материала с целью организации целенаправленной познавательной деятельности студентов по овладению знаниями, умениями и навыками читаемой дисциплины. В лекции делается акцент на реализацию главных идей и направлений в изучении дисциплины, дается установка на последующую самостоятельную работу.

Практические занятия – это метод репродуктивного обучения, обеспечивающий связь теории и практики, содействующий выработке у студентов умений и навыков применения знаний, полученных на лекции и в ходе самостоятельной работы. Практические занятия как образовательная технология помогают студентам систематизировать, закрепить и углубить знания теоретического характера, полученные в ходе изучения дисциплины.

Практические занятия по дисциплине «Информационная безопасность и защита информации» проводятся в компьютерных классах, в которых студенты

выполняют задания с использованием Интернет-ресурсов и компьютерной техники, необходимых для сбора, обработки и анализа необходимой информации.

Лабораторная работа позволяет организовать учебную работу с реальными информационными объектам. Лабораторная работа как образовательная технология реализует следующие функции: овладение системой средств и методов практического исследования обучающимися, развитие творческих исследовательских умений обучающихся и расширение возможностей использования теоретических знаний для решения практических задач.

Самостоятельная работа студента проявляется в систематизации, планировании, контроле и регулировании его учебно-профессиональной деятельности, а также собственные познавательно-мыслительные действия без непосредственной помощь и руководства со стороны преподавателя. Основной целью самостоятельной работы студента является формирование навыка самостоятельного приобретения им знаний по некоторым несложным вопросам теоретического курса, закрепление и углубление полученных знаний, умений и навыков во время лекций и практических занятий. Самостоятельная работа подразумевает выполнение студентом поиска, анализа информации, проработку на этой основе учебного материала, подготовку к устному опросу, а также подготовку к практическим и лабораторным занятиям.

В рамках изучения дисциплины «Информационная безопасность и защита информации» предполагается использовать в качестве информационных технологий среду MS Office, антивирус «Лаборатории Касперского».

9 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины (модуля)

Фонд оценочных средств дисциплины «Информационная безопасность и защита информации» представляет собой комплекс методических и контрольных измерительных материалов, предназначенных для определения качества результатов обучения и уровня сформированности компетенций обучающихся в ходе освоения данной дисциплины. В свою очередь, задачами использования фонда оценочных средств являются осуществление как текущего контроля успеваемости студентов в виде устного опроса, так и промежуточной аттестации в форме зачета.

Устный опрос проводится на практических занятиях в течение 10 минут с целью контроля усвоения теоретического материала, излагаемого на лекции. Перечень вопросов определяется уровнем подготовки учебной группы, а также индивидуальными особенностями обучающихся. Также устный опрос проводится для входного контроля по вопросам, перечисленным в п. 9.4.

Промежуточная аттестация по итогам освоения дисциплины проводится в виде зачета в 6 семестре. Этот вид промежуточной аттестации позволяет оценить уровень освоения студентом компетенций за весь период изучения дисциплины. Зачет предполагает устные ответы на 2 теоретических вопроса из пе-

речня вопросов, вынесенных на промежуточную аттестацию, а также решение практического задания.

9.1 Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов

6 семестр

Тема/вид учебных занятий (оценочных заданий), позволяющих студенту продемонстрировать достигнутый уровень сформированности компетенций	Количество баллов		Срок контроля (порядковый номер недели с начала семестра)	Примечание
	минимальное значение	максимальное значение		
Контактная работа				
Аудиторные занятия				
Лекция 1 (Тема 1)	1,25	1,5	1-18	
Практическое занятие 1	1,25	1,5	1-18	
Лекция 2 (Тема 1)	1,25	1,5	1-18	
Лабораторная работа 1	1,25	3,5	1-18	
Лекция 3 (Тема 1)	1,25	1,5	1-18	
Практическое занятие 2	1,25	1,5	1-18	
Лекция 4 (Тема 1)	1,25	1,5	1-18	
Лабораторная работа 2	1,25	3,5	1-18	
Лекция 5 (Тема 2)	1,25	1,5	1-18	
Практическое занятие 3	1,25	1,5	1-18	
Лекция 6 (Тема 2)	1,25	1,5	1-18	
Лабораторная работа 3	1,25	3,5	1-18	
Лекция 7 (Тема 2)	1,25	1,5	1-18	
Практическое занятие 4	1,25	1,5	1-18	
Лекция 8 (Тема 2)	1,25	1,5	1-18	
Лабораторная работа 4	1,25	3,5	1-18	
Лекция 9 (Тема 2)	1,25	1,5	1-18	
Практическое занятие 5	1,25	1,5	1-18	
Лекция 10 (Тема 3)	1,25	1,5	1-18	
Лабораторная работа 5	1,25	3,5	1-18	
Лекция 11 (Тема 3)	1,25	1,5	1-18	
Практическое занятие 6	1,25	1,5	1-18	
Лекция 12 (Тема 3)	1,25	1,5	1-18	
Лабораторная работа 6	1,25	3,5	1-18	
Лекция 13 (Тема 3)	1,25	1,5	1-18	
Практическое занятие 7	1,25	1,5	1-18	
Лекция 14 (Тема 4)	1,25	1,5	1-18	
Лабораторная работа 7	1,25	3,5	1-18	
Лекция 15 (Тема 4)	1,25	1,5	1-18	
Практическое занятие 8	1,25	1,5	1-18	
Лекция 16 (Тема 4)	1,25	1,5	1-18	
Лабораторная работа 8	1,25	3,5	1-18	
Лекция 17(Тема 4)	1,25	1,5	1-18	
Практическое занятие 9	1,25	1,5	1-18	
Лекция 18 (Тема 14)	1,25	1,5	1-18	

Тема/вид учебных занятий (оценочных заданий), позволяющих студенту продемонстрировать достигнутый уровень сформированности компетенций	Количество баллов		Срок контроля (порядковый номер недели с начала семестра)	Примечание
	минимальное значение	максимальное значение		
Итого по обязательным видам занятий	**45**	**70**		
Зачет	**15**	**30**		
Итого по дисциплине	**60**	**100**		
Премиальные виды деятельности (для учета при определении рейтинга)				
Участие в конференции по темам дисциплины		10		
Научная публикация по темам дисциплины		10		
Итого дополнительно премиальных баллов		**20**		
Всего по дисциплине для рейтинга		**120**		

Перевод баллов балльно-рейтинговой системы в оценку по «академической» шкале

Количество баллов по БРС	Оценка
60 и более	«зачтено»
менее 60	«не зачтено»

9.2 Методические рекомендации по проведению процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Посещение лекционного занятия обучающимся с ведением лекционного конспекта оценивается в 1,25 баллов. Ответы на вопросы в ходе устного опроса – до 0,25 баллов.

Посещение практического занятия с ведением конспекта оценивается от 1,25 до 1,5 баллов.

Посещение лабораторного занятия с ведением конспекта оценивается в 1,25 балла. Выполнение лабораторной работы - до 2,25 баллов.

9.3 Темы курсовых работ (проектов) по дисциплине

Написание курсовых работ (проектов) учебным планом не предусмотрено.

9.4 Контрольные вопросы для проведения входного контроля остаточных знаний по обеспечивающим дисциплинам

1. Информация. Классификация информации.
2. Дайте определение понятию информационный процесс.

3. Основные принципы работы компьютера. Процессор. Память, внешние устройства.

4. Какие типы программных модулей существуют?

5. Что такое база данных?

6. Что такое система управления базами данных? Каково отличие базы данных от системы управления базами данных?

7. Какие модели данных вы знаете? Привести пример.

8. Понятие текстового файла. Алгоритмы обработки текстовых файлов. Применение текстовых файлов при программировании решений прикладных задач.

9. Понятие бинарного файла. Алгоритмы обработки бинарных файлов. Применение бинарных файлов при программировании решений прикладных задач.

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

Критерий	Этапы формирования	Показатель
Готовность к самостоятельной работе (ОПК-1)		
Знать: - современные законы, стандарты, методы и технологии в области защиты информации;	1 этап формирования	- перечисляет основные программные средства защиты информации при работе на компьютере и их характеристики;
	2 этап формирования	- раскрывает особенности основных видов информации в сети Internet с учетом потенциальных угроз информационной безопасности;
Уметь: - использовать современные программно-аппаратные средства защиты информации;	1 этап формирования	- называет основные признаки потенциально опасных сайтов в сети Internet;
	2 этап формирования	– демонстрирует знания по определению потенциально опасных сайтов и настройке браузера при работе с ними;
Владеть: – современными методами обеспечения защиты информации;	1 этап формирования	- составляет алгоритм определения потенциально опасных сайтов;
	2 этап формирования	– применяет навыки подготовки браузера к безопасной работе в сети Internet;

Критерий	Этапы формирования	Показатель
Готовностью применять знания и навыки управления информацией (ПК-11)		
Знать: - основные программные средства защиты информации при работе на компьютере и в сети Internet и их характеристики;	1 этап формирования	- описывает основные принципы работы программных средств защиты информации при работе на компьютере;
	2 этап формирования	- формулирует методы расчета и инструментального контроля показателей технической защиты информации;
Уметь: - использовать средства анализа защищенности компьютера и способы устранения уязвимостей;	1 этап формирования	- воспроизводит правила использования средств анализа защищенности компьютера и способы устранения уязвимостей;
	2 этап формирования	- анализирует возможность и необходимость применения средств анализа защищенности компьютера для устранения уязвимостей;
Владеть: - навыками поиска уязвимостей компьютера с помощью специальных программных средств и их устранения.	1 этап формирования	– описывает основные приемы работы со средствами анализа защищенности компьютера;
	2 этап формирования	– применяет средства анализа защищенности компьютера и средства антивирусной защиты при работе на компьютере;

Характеристики шкалы оценивания приведены ниже.

1. Максимальное количество баллов за зачет – 30. Минимальное (зачетное) количество баллов («зачет сдан») – 15 баллов.
2. При наборе менее 15 баллов – зачет не сдан по причине недостаточного уровня знаний.
3. Зачетная оценка выставляется как сумма набранных баллов за ответы на вопросы билета и за решение задачи.
4. Ответы на вопросы билета оцениваются следующим образом:

– *1 балл*: отсутствие продемонстрированных знаний и компетенций в рамках образовательного стандарта (нет ответа на вопрос) или отказ от ответа;

– *2 балла*: нет удовлетворительного ответа на вопрос, демонстрация фрагментарных знаний в рамках образовательного стандарта, незнание лекционного материала;

– 3 *балла*: нет удовлетворительного ответа на вопрос, много наводящих вопросов, отсутствие ответов по основным положениям вопроса, незнание лекционного материала;

– *4 балла*: ответ удовлетворительный, оценивается как минимально необходимые знания по вопросу, при этом студентом продемонстрировано хотя бы минимальное знание всех разделов вопроса в пределах лекционного материала. При этом студентом демонстрируется достаточный объем знаний в рамках образовательного стандарта;

– *5 баллов*: ответ удовлетворительный, достаточные знания в объеме учебной программы, ориентированные на воспроизведение; использование научной (технической) терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

– *6 баллов*: ответ удовлетворительный, студент достаточно ориентируется в основных аспектах вопроса, демонстрирует полные и систематизированные знания в объеме учебной программы;

– *7 баллов*: ответ хороший (достаточное знание материала), но требовались наводящие вопросы, студент демонстрирует систематизированные, глубокие и полные знания по всем разделам учебной программы;

– *8 баллов*: ответ хороший, ответом достаточно охвачены все разделы вопроса, единичные наводящие вопросы; студент демонстрирует способность самостоятельно решать сложные проблемы в рамках учебной программы;

– *9 баллов*: систематизированные, глубокие и полные знания по всем разделам учебной программы; студент демонстрирует способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках учебной программы;

– *10 баллов*: ответ на вопрос полный, не было необходимости в дополнительных (наводящих вопросах); студент демонстрирует систематизированные, глубокие и полные знания по всем разделам учебной программы, а также по основным вопросам, выходящим за ее пределы.

5. Решение задачи оценивается следующим образом:

– *10 баллов*: задание выполнено на 91-100 %, решение и ответ аккуратно оформлены, выводы обоснованы, дана правильная и полная интерпретация выводов, студент аргументированно обосновывает свою точку зрения, уверенно и правильно отвечает на вопросы преподавателя;

– *9 баллов*: задание выполнено на 86-90 %, решение и ответ аккуратно оформлены, выводы обоснованы, дана правильная и полная интерпретация выводов, студент аргументированно обосновывает свою точку зрения, правильно отвечает на вопросы преподавателя;

– *8 баллов*: задание выполнено на 81-85 %, ход решения правильный, незначительные погрешности в оформлении; правильная, но не полная интерпретация выводов, студент дает верные, но не полные ответы на вопросы преподавателя, испытывает некоторые затруднения в интерпретации полученных выводов;

– *7 баллов*: задание выполнено на 74-80 %, ход решения правильный, значительные погрешности в оформлении; правильная, но не полная интерпретация выводов, студент дает правильные, но не полные ответы на вопросы преподавателя, испытывает определенные затруднения в интерпретации полученных выводов;

– *6 баллов*: задание выполнено 66-75 %, подход к решению правильный, есть ошибки, оформление с незначительными погрешностями, неполная интерпретация выводов, не все ответы на вопросы преподавателя правильные, не способен интерпретировать полученные выводы;

– *5 баллов*: задание выполнено на 60-65 %, подход к решению правильный, есть ошибки, значительные погрешности при оформлении, неполная интерпретация выводов, не все ответы на вопросы преподавателя правильные, не способен интерпретировать полученные выводы;

– *4 балла*: задание выполнено на 55-59 %, подход к решению правильный, есть ошибки, значительные погрешности при оформлении, неполная интерпретация выводов, не все ответы на вопросы преподавателя правильные, не способен интерпретировать полученные выводы;

– *3 балла*: задание выполнено на 41-54 %, решение содержит грубые ошибки, неаккуратное оформление работы, неправильная интерпретация выводов, студент дает неправильные ответы на вопросы преподавателя;

– *2 балла*: задание выполнено на 20-40 %, решение содержит грубые ошибки, неаккуратное оформление работы, выводы отсутствуют; не может прокомментировать ход решения задачи, дает неправильные ответы на вопросы преподавателя;

– *1 балл*: задание выполнено менее, чем на 20 %, решение содержит грубые ошибки, студент не может прокомментировать ход решения задачи, не способен сформулировать выводы по работе.

9.6 Типовые контрольные задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины

Типовые вопросы для проведения текущего контроля успеваемости в виде устного опроса

1. Принципы и методы выявления технических каналов утечки информации.
2. Классификация технических средств выявления каналов утечки информации.
3. Принцип работы нелинейных локаторов.
4. Технические средства контроля двухпроводных линий.
5. Методы защиты информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации.
6. Методы защиты речевой информации в помещении.
7. Методы защиты телефонных линий.
8. Модели воздействия программных закладок на компьютеры.
9. Способы защиты от программных закладок.
10. Способы определения программных закладок.

Перечень примерных вопросов к зачёту для проведения промежуточной аттестации по итогам освоения дисциплины

1. Доктрина информационной безопасности. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
2. Доктрина информационной безопасности. Особенности обеспечения информационной безопасности Российской Федерации в области науки и техники.
3. Идентификация и аутентификация.
4. Криптографические методы обеспечения конфиденциальности информации.
5. Принципы обеспечения целостности информации.
6. Построение систем защиты от угроз нарушения доступности.
7. Стандарты в информационной безопасности.
8. Технические каналы утечки речевой информации.
9. Программные закладки Модели воздействия программных закладок на компьютеры.
10. Аппаратно-программные средства защиты информации от НСД
11. СЗИ «Сфера». Назначение, составляющие комплекса.

Типовые практические задания для промежуточной аттестации в форме зачёта

1. Установка и настройка антивирусного программного пакета.
2. Шифрование файлов с помощью программы PGP.
3. Анализ уязвимостей с помощью антивируса «Лаборатории Касперского»
4. Использование заданного симметричного способа шифрования для шифрования сообщения.
5. Настройка и использование заданной программы предотвращения и обнаружения вторжения.
6. Создание резервной копии системного реестра для операционной системы Windows и его восстановление.
7. Настройка параметров парольной защиты для повышения защищенности от попыток его дискредитации.
8. Установка и настройка незнакомого антивирусного программного пакета или известного за ограниченное время.
9. Расшифровка сообщения путем подбора ручных симметричных способов шифрования.
10. Разработка и настройка параметров парольной защиты для повышения защищенности от попыток его дискредитации в условной организации.

10 Методические рекомендации для обучающихся по освоению дисциплины

Важнейшей частью образовательного процесса дисциплины «Информационная безопасность и защита информации» являются учебные занятия. В ходе занятий осуществляется теоретическое обучение студентов, привитие им необходимых умений и практических навыков по дисциплине.

Основными видами учебных занятий по дисциплине являются лекции, практические занятия и лабораторные работы. Виды учебных занятий определяются рабочей программой дисциплины.

Лекции являются одним из важнейших видов учебных занятий и составляют основу теоретической подготовки обучающихся по дисциплине «Информационная безопасность и защита информации». Они должны давать систематизированные основы научных знаний по дисциплине, концентрировать внимание студентов на наиболее сложных, проблемных вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

Каждая лекция должна представлять собой устное изложение лектором основных теоретических положений изучаемой дисциплины или отдельной темы как логически законченное целое и иметь конкретную целевую установку. Лекции должны носить, как правило, проблемный характер. Основным методом в лекции выступает устное изложение лектором учебного материала.

Порядок изложения материала лекции отражается в плане ее проведения.

Особое место в лекционном курсе по дисциплине занимают вводная и заключительная лекции.

Вводная часть лекции должна задавать общую характеристику изучаемой дисциплины, подчеркивать новизну проблем, указывать ее роль и место в системе изучения других дисциплин, кратко знакомить студентов с содержанием и структурой курса, а та же с организацией учебной работы по нему.

Заключительная лекция должна давать научно-практическое обобщение изученной дисциплины, показывать перспективы развития изучаемой области знаний, навыков и практических умений.

Практические задания по дисциплине имеют цель:

- углубление, расширение и конкретизацию теоретических знаний, полученных на лекции, до уровня, на котором возможно их практическое использование;

- экспериментальное подтверждение положений и выводов, изложенных в теоретическом курсе, и усиление доказательности обучения;

- проверку теоретических знаний.

Практическим занятиям предшествует лекции и целенаправленная самостоятельная подготовка студентов, поэтому практические занятия нужно начинать с краткого обзора цели занятия, напоминания о его связи с лекциями, и формирования контрольных вопросов-заданий, которые должны быть решены на данном занятии.

Лабораторные работы по дисциплине проводятся в соответствии с п. 5.5. Лабораторные работы направлены на обобщение, систематизацию и закрепление теоретических знаний по конкретным темам дисциплины «Информационная безопасность и защита информации» и на развитие аналитических и конструктивных умений обучающихся.

При изучении тем дисциплины «Информационная безопасность и защита информации» обучающимся необходимо: ознакомиться с изложенным теоретическим материалом; акцентировать внимание на основных понятиях каждой конкретной темы; пройти тестирование (входной и текущий контроль); выполнить задания на самостоятельную работу; подготовиться к сдаче промежуточной аттестации в виде зачёта.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 01.03.04 «Прикладная математика».

Программа рассмотрена и утверждена на заседании кафедры
№8 Информатики

«12» января 2017 года, протокол № 7.

Разработчики

к. п. н. Самойлов В. А.
(ученая степень, ученое звание, фамилия и инициалы разработчиков)

Заведующий кафедрой № 8 Прикладной математики и информатики

к.т.н., доцент Далингер Я.М.
(ученая степень, ученое звание, фамилия и инициалы заведующего кафедрой)

Программа согласована:

Руководитель ОПОП

к.т.н., доцент Далингер Я.М.
(ученая степень, ученое звание, фамилия и инициалы руководителя ОПОП)

Программа рассмотрена и одобрена на заседании Учебно-методического совета Университета «15» февраля 2017 года, протокол № 5.

С изменениями и дополнениями от «30» августа 2017 года, протокол № 10 (в соответствии с Приказом от 5 апреля 2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – про-граммам бакалавриата, программам специалитета, программам магистратуры»).