ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ»

УТВЕРЖДАЮ
Первый проректор-проректор по учебной работе
_____ Н.Н. Сухих
«18» 09 2019 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки
20.03.01 Техносферная безопасность

Направленность программы (профиль)
Безопасность технологических процессов и производств

Квалификация выпускника
бакалавр

Форма обучения
очная

Санкт-Петербург
2019

1 Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» являются формирование у студентов знаний по основам информационной безопасности (ИБ), формирование умений и навыков применения полученных знаний в повседневной профессиональной деятельности.

Задачами освоения дисциплины «Информационная безопасность» являются:

– ознакомление с основным организационно-правовым обеспечением информационной безопасности;

– изучение различных видов угроз, принципов создания защищенных информационных систем;

– изучение обеспечения информационной безопасности в системах управления базами данных.

Дисциплина обеспечивает подготовку выпускника к экспертному, надзорному и инспекционно-аудиторскому виду профессиональной деятельности.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность» представляет собой дисциплину, относящуюся к Вариативной части Блока 1 Дисциплины.

Дисциплина «Информационная безопасность» базируется на результатах обучения, полученных при изучении дисциплин «Информатика» и «Информационные технологии на транспорте».

Дисциплина «Информационная безопасность» является обеспечивающей для дисциплины «Безопасность полетов», «Безопасность на воздушном транспорте».

Дисциплина «Информационная безопасность» изучается в 7 семестре.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

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

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
Владением культурой безопасности и рискориентированным мышлением, при котором вопросы безопасности и сохранения окру-	Знать: - положения информационной безопасности (ИБ) как составляющей культуры безопасности; - значение ИБ для снижения рисков техногенных прецедентов. Уметь:

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
жающей среды рассматриваются в качестве важнейших приоритетов в жизни и деятельности (ОК-7)	- определять необходимость усиления ИБ в целях повышения защищенности объектов воздушного транспорта. Владеть: - методикой оценки угроз ИБ на рабочем месте.
Способностью использования основных программных средств, умением пользоваться глобальными информационными ресурсами, владением современными средствами телекоммуникаций, способностью использовать навыки работы с информацией из различных источников для решения профессиональных и социальных задач (ОК-12)	Знать: - методы сбора, хранения и обработки информации, применяемые в профессиональной деятельности; - основные методы защиты процессов получения, хранения и переработки информации. Уметь: - использовать внешние носители информации для обмена данными между машинами; - создавать резервные копии, архивы данных и программ. Владеть: - средствами криптографической защиты информации.
Способностью учитывать современные тенденции развития техники и технологий в области обеспечения техносферной безопасности, измерительной и вычислительной техники, информационных технологий в своей профессиональной деятельности (ОПК-1)	Знать: - структуру локальных и глобальных компьютерных сетей; - основные виды атак на компьютерные системы; - основные средства и методы защиты компьютерных сетей. Уметь: - использовать средства защиты информации при работе в сети интернет. Владеть: - методами поиска и обмена информацией в глобальных и локальных компьютерных сетях.
способностью определять опасные, чрезвычайно опасные зоны, зоны приемлемого риска (ПК-17)	Знать: - признаки опасных зон в случае нарушения ИБ; - последствия нарушения ИБ на объектах воздушного транспорта. Уметь:

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
	- определять опасные зоны в случае нарушения ИБ. Владеть: - способностью построения систем защиты от нарушения ИБ.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 академических часа.

Наименование	Всего часов	Семестр 7
Общая трудоемкость дисциплины	144	144
Контактная работа:	42,5	42,5
лекции	14	14
практические занятия	28	28
семинары	–	–
лабораторные работы	–	–
Самостоятельная работа студента	75	75
Промежуточная аттестация:	27	27
контактная работа	0,5	0,5
самостоятельная работа по подготовке к зачёту с оценкой	26,5	26,5

5 Содержание дисциплины

5.1 Соотнесения тем дисциплины и формируемых компетенций

№ п/п	Темы дисциплины	Компетенции					Образовательные технологии	Оценочные средства
		Количество часов	ОК-7	ОК-12	ОПК-1	ПК-17		
1	Информационная безопасность (ИБ) деятельности общества. Организационное и правовое обеспечение ИБ.	16	+		+	+	ВК, Л, СРС, ПЗ	У, О

№ п/п	Темы дисциплины	Компетенции					Образовательные технологии	Оценочные средства
		Количество часов	ОК-7	ОК-12	ОПК-1	ПК-17		
2	Основы обеспечения ИБ жизнедеятельности общества и его структур.	24	+		+	+	Л, СРС, ПЗ	У, О
3	Основы технического обеспечение ИБ.	53		+	+		Л, СРС, ПЗ	У, О
4	Программно-аппаратные средства обеспечения ИБ в компьютерных системах.	24	+	+		+	Л, СРС, ПЗ	У, О
	Итого по дисциплине	117						
	Промежуточная аттестация	27						
	Всего по дисциплине	144						

Сокращения: Л – лекция, ПЗ – практическое занятие, СРС – самостоятельная работа студента, ВК – входной контроль, У – устный опрос, О – отчет о выполненной практической работе.

5.2 Темы дисциплины и виды занятий

№ п/п	Наименование темы дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
1	Информационная безопасность (ИБ) деятельности общества. Организационное и правовое обеспечение ИБ.	4	2	–	–	10	–	16

2	Основы обеспечения ИБ жизнедеятельности общества и его структур.	2	8	–	–	14	–	24
3	Основы технического обеспечения ИБ.	4	12	–	–	37	–	53
4	Программно-аппаратные средства обеспечения ИБ в компьютерных системах.	4	6	–	–	14	–	24
	Итого по дисциплине	14	28	–	–	75	–	117
Промежуточная аттестация								27
Всего по дисциплине								144

5.3 Содержание дисциплины

Тема1 Информационная безопасность деятельности общества

Организационное и правовое обеспечение ИБ. 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 автоматизированной системе (АС). Построение систем защиты от угроз информации в АС.

Тема 3 Основы технического обеспечение информационной безопасности

Криптографические методы защиты информации. Уязвимости компьютеров и компьютерных сетей. Основные виды атак на компьютерные системы. Сетевые средства экранирования в АС. Системы анализа защищенности. Системы обнаружения и предотвращения вторжений.

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

Обеспечение сохранности данных и защита ПЭВМ в АС. Информационная безопасность систем управления базами данных. Политика безопасности в АС. Принципы построения. СКЗИ в АС SecretNet и Сфера. Особенности, правила использования.

5.4 Практические занятия

Номер темы дисциплины	Тематика практических занятий	Трудоемкость (часы)
1	Практическое занятие №1. Стандарты информационной безопасности.	2
2	Практическое занятие № 2. Информационное противоборство. Проявления информационного противоборства.	2
2	Практическое занятие № 3. Антивирусные средства. Поиск и нейтрализация вирусных угроз в АС.	2
2	Практическое занятие № 4. Разработка систем защиты от угроз нарушения информации в АС.	2
2	Практическое занятие № 5. Средства криптографической защиты информации. Криптографические алгоритмы.	2
3	Практическое занятие № 6. Определение уязвимости компьютеров и компьютерной сети.	2
3	Практическое занятие № 7. Анализ атак на компьютерные системы.	2
3	Практическое занятие № 8. Использование сетевых средств экранирования в АС.	2
3	Практическое занятие № 9. Использование системы анализа защищенности	2
3	Практическое занятие № 10. Использование системы обнаружения и предотвращения вторжений.	2
3	Практическое занятие № 11. Настройка информационной безопасности в АС и системах управления базами данных.	2
4	Практическое занятие № 12. Разработка и использование политик безопасности в АС.	2
4	Практическое занятие № 13. СКЗИ SecretNet и Сфера. Особенности, правила использования.	2
4	Практическое занятие № 14. Настройка и использование СКЗИ SecretNet и Сфера.	2
Итого по дисциплине		28

5.5 Лабораторный практикум

Лабораторный практикум учебным планом не предусмотрен.

5.6 Самостоятельная работа

Номер темы дисциплины	Виды самостоятельной работы	Трудоемкость (часы)
1	1. Работа с основной и дополнительной литературой: [1, 2,3,5], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	6
1	1. Работа с основной и дополнительной литературой: [3,4,6], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	4
2	1. Работа с основной и дополнительной литературой: [1, 2,3,5], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	4
2	1. Работа с основной и дополнительной литературой: [1, 2,3,6], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	4
2	1. Работа с основной и дополнительной литературой: [2,3,4,6], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	6
3	1. Работа с основной и дополнительной литературой: [2,3,5], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	8
3	1. Работа с основной и дополнительной литерату-	8

Номер темы дисциплины	Виды самостоятельной работы	Трудоемкость (часы)
	рой: [2,3,4,6], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практичсскому занятию.	
3	1. Работа с основной и дополнительной литературой: [2,4,5], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	6
3	1. Работа с основной и дополнительной литературой: [1, 2,3,5], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	6
3	1. Работа с основной и дополнительной литературой: [2,3,5], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	8
4	1. Работа с основной и дополнительной литературой: [1, 2,3,5], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	6
4	1. Работа с основной и дополнительной литературой: [1, 2,4], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	5
4	1. Работа с основной и дополнительной литературой: [1, 2,3], программное обеспечение и интернет-ресурсы. 2. Подготовка к устному опросу [7–14]. 3. Подготовка к практическому занятию.	4
Итого по дисциплине		75

5.7 Курсовые работы

Курсовые работы учебным планом не предусмотрены.

6 Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1 Баранова, Е.К. и др. **Информационная безопасность и защита информации** [Текст]: учеб. пособ. для вузов / Е. К. Баранова, А. В. Бабаш, А. М. Петраков. - 2-е изд. - М. : РИОР-Инфра-М, 2014. - 256с. —ISBN 978-5-369-01218-5 — Количество экземпляров 15.

2 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, 2018. — 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 (дата обращения 16.01.2018).

3 Нестеров, С. А. **Информационная безопасность** [Электронный ресурс]: учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 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 (дата обращения 16.01.2018).

б) дополнительная литература:

4 Щеглов, А. Ю. **Защита информации** [Электронный ресурс]: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — М. : Издательство Юрайт, 2018. — 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 (дата обращения 16.01.2018).

5 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, 2018. — 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 (дата обращения 16.01.2018).

6 **Руководство по эксплуатации СКЗИ «Сфера».** [Текст]. — С-Пб.: ООО «Фирма «НИТА», 2015.— 57 с. Количество экземпляров-10.

в) перечень ресурсов информационно-телекоммуникационной сети «Интеренет»

7 **Фирма «НИТА»** [Электронный ресурс]: официальный сайт ООО «Фирма «НИТА». — Режим доступа: http://www.nita.ru. , свободный (дата обращения: 10.01.2018).

8 **Система поиска Google**[Электронный ресурс]. – Режим доступа: www.google.com. , свободный (дата обращения: 10.01.2018).

9 **Электронная библиотека** [Электронный ресурс]. – Режим доступа: www.wikipedia.org, свободный (дата обращения: 10.01.2018).

10 **Онлайн переводчик** [Электронный ресурс]. – Режим доступа: www.lingvo.ru. , свободный (дата обращения: 10.01.2018).

11 **InformationSecurity/Информационная безопасность** [Электронный ресурс]: официальный сайт журнала «InformationSecurity / Информационная безопасность» – Режим доступа: www.itsec.ru, свободный (дата обращения: 01.12.2017).

12 **Информационно-аналитический ресурс и виртуальная площадка для общения менеджеров и экспертов по информационной безопасности** [Электронный ресурс]. – Режим доступа: www.iso27000.ru, свободный (дата обращения: 01.12.2017).

13 **Федеральная служба по техническому и экспортному контролю (ФСТЭК России)** [Электронный ресурс] : официальный сайтФСТЭК РФ.– Режим доступа: http://fstec.ru, свободный (дата обращения: 01.12.2017).

14 **Справочно-правовая база Гарант** [Электронный ресурс]. – Режим доступа: http://www.garant.ru/ (Дата обращения 25.12.2017).

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

15 **Единое окно доступа к образовательным ресурсам** [Электронный ресурс]. – Режим доступа: http://window.edu.ru. ,свободный (дата обращения: 29.01.2018).

16 **Консультант Плюс** [Электронный ресурс]: официальный сайт компании Консультатнт Плюс. — Режим доступа: http://www.consultant.ru .,свободный (дата обращения: 29.01.2018).

17 **Электронная библиотека научных публикаций «eLIBRARY.RU»** [Электронный ресурс] — Режим доступа: http://elibrary.ru. , свободный (дата обращения: 29.01.2018).

18 **Электронно-библиотечная системa издательства «Лань»** [Электронный ресурс] — Режим доступа: http://e.lanbook.com. , свободный (дата обращения: 29.01.2018).

7 Материально-техническое обеспечение дисциплины

Компьютерный класс, оборудованный ПК, индивидуально для каждого студента с выходом в Интернет.

Инсталлированные изучаемые средства прикладного и инструментального ПО: MS Office, AdodeReader, MSVisio, X-Spider, Сфера.

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» предполагает использование следующих образовательных технологий: входной контроль, лекции, практические занятия и самостоятельная работа студента.

Входной контроль проводится в форме устных опросов с целью оценивания остаточных знаний по ранее изученным дисциплинам. Он осуществляется по вопросам дисциплин «Информатика», «Информационные технологии на транспорте» на которых базируется дисциплина «Информационная безопасность».

Лекция как образовательная технология представляет собой устное, системтически 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.

По дисциплине «Информационная безопасность» планируется проведение как информационных, так и проблемных лекций. Информационные лекции направлены на систематизированное изложение накопленных и актуальных научных знаний. Проблемные лекции активизируют интеллектуальный потенциал и мыслительную деятельность студентов, которые приобретают умение вести дискуссию. В ходе проблемной лекции преподаватель включает в процесс изложения материала серию проблемных вопросов. Как правило, это сложные, ключевые для темы вопросы. Студенты приглашаются для размышлений и поиску ответов на них по мере их постановки.

Ведущим методом в лекции выступает устное изложение учебного материала, который сопровождается одновременной демонстрацией слайдов, созданных в среде PowerPoint, при необходимости привлекаются открытые Интернет-ресурсы, а также демонстрационные и наглядно-иллюстрационные материалы.

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. На практических занятиях по дисциплине «Информационная безопасность» студенты обучаются выстраиванию эффективной коммуникации, навыкам групповой работы, приемам решения предлагаемых задач, а также овладевают умениями и навыками оценки полученных решений.

Практические занятия по дисциплине «Информационная безопасность» проводятся в компьютерных классах, в которых студенты выполняют практические задания с использованием Интернет-ресурсов и компьютерной техники, необходимых для сбора, обработки и анализа необходимой информации.

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 докладов и подготовку к письменной аудиторной работе и к тесту.

В рамках изучения дисциплины «Информационная безопасность» предполагается использовать в качестве информационных технологий среду MSOffice: Word 2007, Excel 2007, PowerPoint 2007.

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

Фонд оценочных средств дисциплины «Информационная безопасность» 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, так и промежуточной аттестации в форме зачета с оценкой.

Фонд оценочных средств дисциплины «Информационная безопасность» для текущего контроля включает: устные опросы и отчет о выполненной практической работе.

Устный опрос проводится на практических занятиях с целью контроля усвоения теоретического материала, излагаемого на лекции и освоенного в результате выполнения самостоятельной работы. 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.

Отчет о выполненной практической работе составляется по итогам выполнения практического задания на практическом занятии. Перечень освещаемых вопросов определяется заданием на практическую работу.

Промежуточная аттестация по итогам освоения дисциплины проводится в виде зачета с оценкой в 7 семестре. Этот вид промежуточной аттестации позволяет оценить уровень освоения студентом компетенций за весь период изучения дисциплины. Зачет с оценкой предполагает устные ответы на 2 теоретиче-

ских вопроса из перечня вопросов, вынесенных на промежуточную аттестацию, а также решение практического задания.

9.1 Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов

Раздел (тема) / Вид учебных занятий (оценочных заданий),позволяющих студенту продемонстрировать достигнутый уровень сформированности компетенций	Количество баллов (из общего расчета 100 баллов на дисциплину)		Срок контроля (№ недели с начала семестра)	Примечание
	миним.	максим.		
Обязательные виды занятий				
Практическая работа № 1.				
Стандарты информационной безопасности.	3,211	5	2	
Итого баллов по разделу (теме)	3,211	5		
Практическая работа № 2.				
Информационное противоборство. Проявления информационного противоборства.	3,211	5	4	
Практическая работа № 3.				
Антивирусные средства. Поиск и нейтрализация вирусных угроз в АС.	3,211	5	4	
Практическая работа № 4.				
Разработка систем защиты от угроз нарушения информации в АС.	3,211	5	6	
Практическая работа № 5.				
Средства криптографической защиты информации. Криптографические алгоритмы.	3,211	5	8	
Итого баллов по разделу (теме)	12,844	20		
Практическая работа № 6.				
Определение уязвимости компьютеров и компьютерной сети.	3,211	5	8	
Практическая работа № 7.				
Анализ атак на компьютерные системы.	3,211	5	8	
Практическая работа № 8.				
Использование сетевых средств экранирования в АС.	3,211	5	8	
Практическая работа № 9.				

Раздел (тема) / Вид учебных занятий (оценочных заданий),позволяющих студенту продемонстрировать достигнутый уровень сформированности компетенций	Количество баллов (из общего расчета 100 баллов на дисциплину)		Срок контроля (№ недели с начала семестра)	Примечание
	миним.	максим.		
Использование системы анализа защищенности	3,211	5	10	
Практическая работа № 10.				
Использование системы обнаружения и предотвращения вторжений.	3,211	5	10	
Практическая работа № 11.				
Настройка информационной безопасности в АС и системах управления базами данных.	3,211	5	12	
Итого баллов по разделу (теме)	19,266	30		
Практическая работа № 12.				
Разработка и использование политик безопасности в АС.	3,211	5	12	
Практическая работа № 13.				
Настройка и использование СКЗИ SecretNet и Сфера.	3,211	5	14	
Практическая работа № 14.				
СКЗИ SecretNet и Сфера. Особенности, правила использования.	3,211	5	14	
Итого баллов по разделу (теме)	9,633	15		
Итого по обязательным видам занятий	45	70		
Зачет с оценкой	15	30		
Итого по дисциплине	60	100		
Научные публикации по теме дисциплины	10	10		
Участие в конференциях по теме дисциплины	10	10		
Итого дополнительно премиальных баллов		20		
Всего по дисциплине (для рейтинга)	80	120		
*) – разделы (темы) могут не выделяться, а их названия не приводиться; **) – может вводиться для дополнительного стимулирования текущей работы студента в семестре.				
Перевод баллов балльно-рейтинговой системы в оценку по 5-ти балльной				

Раздел (тема) / Вид учебных занятий (оценочных заданий),позволяющих студенту продемонстрировать достигнутый уровень сформированности компетенций	Количество баллов (из общего расчета 100 баллов на дисциплину)		Срок контроля (№ недели с начала семестра)	Примечание
	миним.	максим.		
«академической» шкале				
Количество баллов по БРС	Оценка (по 5-ти балльной «академической» шкале)			
90 и более	5 - «отлично»			
70÷89	4 - «хорошо»			
60÷69	3 - «удовлетворительно»			
менее 60	2 - «неудовлетворительно»			

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

В процессе преподавания дисциплины «Информационная безопасность» для текущей аттестации обучающихся используются показатели, характеризующие текущую учебную работу студентов:

- устные опросы по теме практического занятия – 2,5 балла;
- отчет о выполненной практической работе – 2,5 балла.

Сроки промежуточной аттестации определяются графиком учебного процесса. По дисциплине «Информационная безопасность» предусмотрен зачет с оценкой. К зачету с оценкой допускаются студенты, выполнившие все требования учебной программы. Зачет с оценкой принимается преподавателем, ведущим занятия в данной группе по данной дисциплине, а также лектором данного потока.

Зачет с оценкой проводится в объеме материала рабочей программы дисциплины, по билетам в устной форме и путем выполнения практического задания в специально подготовленных учебных классах. Перечень вопросов, выносимых на зачет с оценкой, обсуждаются на заседании кафедры и утверждаются заведующим кафедры. Предварительное ознакомление студентов с билетами запрещается.

Вызванный студент - после доклада о прибытии для сдачи зачет с оценкой, представляет преподавателю свою зачетную книжку, берет билет, получает чистые листы для записей и после разрешения садится за рабочий стол для подготовки. На подготовку к ответу студенту предоставляется до 30 минут. Общее время подготовки и ответа не должно превышать одного часа. В учебном классе, где принимается зачет, могут одновременно находиться студенты из расчета не более четырех на одного преподавателя.

По готовности к ответу или по вызову преподавателя студент отвечает на вопросы билета. После ответа студента преподаватель имеет право задать ему дополнительные вопросы в объеме учебной программы.

В итоге проведенного зачета с оценкой студенту выставляется оценка. Преподаватель несет личную ответственность за правильность выставленной оценки и оформления итоговой ведомости и зачетной книжки.

Зачет с оценкой позволяет оценить уровень освоения компетенций за период изучения дисциплины в 7 семестре и предполагает ответы на 2 устных вопроса и одного практического задания (см. п. 9.6).

9.3 Темы курсовых работ по дисциплине

Курсовые работы учебным планом не предусмотрены.

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

«Информатика»:

1 Состав и типы компьютеров. Программное и аппаратное обеспечение персонального компьютера. Системы счисления.

2 Процессор. Память. Устройства ввода/вывода.

3 Локальные и глобальные компьютерные сети.

4 Операционная система MS Windows. Управление системой файлов.

5 Состав и назначение пакета MS Offis. Подготовка документов в MS Word.Обработка данных в MS Excel.

6 Виды программ, алгоритмы. Свойства алгоритма. Способы записи алгоритма.

7 Интегрированная среда VisualBasic. Формы, элементы управления, меню. Алфавит языка. Константы, переменные. Стандартные типы данных. Стандартные функции. Линейная структура программы: ввод, вычисление, вывод. Операторы.

8 Условный оператор if. Логические выражения. Операторы цикла. Вложенные циклы.

9 Понятие массива. Объявление массивов. Динамические массивы. Элементы массива, индексы. Методы инициализации массивов.

10 Понятие процедуры и функции. Синтаксис процедур и функций в VB. Передача параметров.

«Информационные технологии»:

1 Телекоммуникационные технологии.

2 Требования, предъявляемые к сети и разделяемые ресурсы.

3 Характеристики работы сети.

4 Определение локальных вычислительных сетей (ЛВС) и основные особенности их применения, ЛВС с централизованным и децентрализованным управлением.

5 Требования, предъявляемые к функциональным устройствам ЛВС.

6 Основные методы доступа в ЛВС и протоколы передачи данных.

7 Глобальная сеть Internet. Основные характеристики сети.

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

Критерии оценивания компетенций	Показатели оценивания компетенций	Описание шкалы оценивания
владением культурой безопасности и рискориентированным мышлением, при котором вопросы безопасности и сохранения окружающей среды рассматриваются в качестве важнейших приоритетов в жизни и деятельности (ОК-7);		Ответ студента на вопрос оценивается и квалифицируется баллами в соответствии со следующими критериями: *Оценка 9-10 баллов* - ответ построен логично в соответствии с планом; - обнаружено максимально глубокое знание терминов, понятий, категорий, концепций и теорий; - обнаружен аналитический подход в освещении различных концепций; - сделаны содержательные выводы; - продемонстрировано знание обязательной и дополнительной литературы. - студент активно работал на практических занятиях, выполнил все предусмотренные программой задания и проявил творческое, ответственное отношение к обучению по дисциплине. *Оценка 7-8 баллов* - ответ построен в соответствии с планом; - представлены различные подходы к проблеме,
Знать: - основные положения ИБ как составляющей культуры безопасности; - значение ИБ для снижения рисков техногенных прецедентов;	Имеет устойчивые знания об основных положения ИБ как составляющих культуры безопасности; значении ИБ для снижения рисков техногенных прецедентов;	
Уметь: - определять уровень риска возникновения техногенных прецедентов;	Способен определять необходимость усиления ИБ в целях повышения защищенности объектов воздушного транспорта;	
Владеть: - методикой оценки угроз ИБ на рабочем месте;	Владеет методикой оценки угроз ИБ на рабочем месте	
способностью использования основных программных средств, умением пользоваться глобальными информационными ресурсами, владением современными средствами телекоммуникаций, способностью использовать навыки работы с информацией из различных источников для решения профессиональных и социальных задач (ОК-12);		
Знать: - методы сбора, хранения и обработки информации, применяемые в профессиональной деятельности;	Имеет устойчивые знания о методах сбора, хранения и обработки информации, применяемые в профессиональной деятельности;	

Критерии оценивания компетенций	Показатели оценивания компетенций	Описание шкалы оценивания
		но их обоснование недостаточно полно; - выдвигаемые положения обоснованы, однако наблюдается непоследовательность анализа; - выводы правильны; - продемонстрировано знание обязательной и дополнительной литературы. -студент активно работал на практических занятиях, выполнил все предусмотренные программой задания. *Оценка 5-6 баллов* - ответ недостаточно логически выстроен; - план ответа соблюдается непоследовательно; - недостаточно раскрыты понятия, категории, концепции, теории; - продемонстрировано знание обязательной литературы. -студент выполнил все предусмотренные программой задания. *Оценка менее 5 баллов* - не раскрыты профессиональные понятия, категории, концепции, теории; - научное обоснование проблем подменено рассуждениями обыденно-повседневного характера; - ответ содержит ряд
Уметь: - использовать внешние носители информации для обмена данными между машинами; - создавать резервные копии, архивы данных и программ;	Способен использовать внешние носители информации для обмена данными между машинами; Способен создавать резервные копии, архивы данных и программ;	
Владеть: - средствами криптографической защиты информации.	Владеет средствами криптографической защиты информации.	
способностью учитывать современные тенденции развития техники и технологий в области обеспечения техносферной безопасности, измерительной и вычислительной техники, информационных технологий в своей профессиональной деятельности (ОПК-1);		
Знать: - структуру локальных и глобальных компьютерных сетей; - основные виды атак на компьютерные системы; - основные средства и методы защиты компьютерных сетей;	Имеет устойчивые знания о: - структуре локальных и глобальных компьютерных сетей; - основных видах атак на компьютерные системы; - основных средствах и методах защиты компьютерных сетей;	
Уметь: - использовать средства защиты информации при работе в сети интернет;	Способен использовать средства защиты информации при работе в сети интернет	
Владеть: - методами поиска и обмена информацией в глобальных и локальных компьютерных сетях.	Владеет методами поиска и обмена информацией в глобальных и локальных компьютерных сетях.	
способностью определять опасные, чрезвычайно		

Критерии оценивания компетенций	Показатели оценивания компетенций	Описание шкалы оценивания
опасные зоны, зоны приемлемого риска (ПК-17);		серьезных неточностей; - выводы поверхностны или неверны; - не продемонстрировано знание обязательной литературы. -студент не активно работал на практических занятиях, не выполнил все предусмотренные программой задания.
Знать: - степень опасности зон на объсктах воздушного транспорта в случае нарушения ИБ	Имеет устойчивые знания о степени опасности зон на объектах воздушного транспорта в случае нарушения ИБ	
Уметь: - определять степень опасности зон на объектах воздушного транспорта в случае нарушения ИБ	Способен определять степень опасности зон на объектах воздушного транспорта в случае нарушения ИБ	
Владеть: - навыками определения степени опасности зон на объектах воздушного транспорта в случае нарушения ИБ	Владеет навыками определения степени опасности зон на объектах воздушного транспорта в случае нарушения ИБ	

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

Примерный перечень вопросов текущего контроля в форме 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 ТСПИ.
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.

Примерный перечень практических заданий

1 Определить сетевые параметры компьютера и сети используя сетевые утилиты командной строки в операционной среде Windows.

2 Настроить права пользователей в операционной среде Windows.
3 Использовать программу PGP для осуществления защищенного документооборота и шифрования файлов.
4 Использовать системный реестр для контроля и коррекции настроек в операционной среде Windows.
5 Использовать служебные средства Windows для анализа, восстановления и проверки работы системы.

Примерный перечень вопросов к зачету с оценкой для проведения промежуточного контроля по дисциплине

Теоретические вопросы

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.

Практические задания

1 Установка и настройка антивирусного программного пакета.
2 Шифрование файлов с помощью программы PGP.
3 Анализ уязвимостей с помощью программы X-Spider.
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 ОС Windows и его восстановление.
7 Настройка параметров парольной защиты для повышения защищенности от попыток его дискредитации.

10 Методические рекомендации для обучающихся по освоению дисциплины

Приступая в 7 семестре к изучению дисциплины «Информационная безопасность», обучающемуся необходимо внимательно ознакомиться с тематическим планом занятий и списком рекомендованной литературы. Также ему следует уяснить, что уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях и практических занятиях. Также в этом процессе важное значение имеет самостоятельная работа, направленная на вовлечение обучающегося в самостоятельную познавательную деятельность и формирование у него методов организации такой деятельности с целью формирования самостоятельности мышления, способностей к профессиональному саморазвитию, самосовершенствованию и самореализации в современных условиях социально-экономического развития.

Основными видами аудиторной работы студентов являются лекции и практические занятия. На первом занятии преподаватель осуществляет входной контроль по вопросам дисциплины «Информатика» (п. 9.4), и «Информационные технологии» на которой базируется дисциплина «Информационная безопасность» (п. 2).

В ходе лекции преподаватель излагает и разъясняет основные, наиболее сложные понятия, а также соответсвующие теоретические и практические проблемы, дает задания и рекомендации для практических занятий, а также указания по выполнению обучающимся самостоятельной работы.

Задачами лекций являются:

ознакомление обучающихся с целями, задачами и структурой дисциплины «Информационная безопасность», ее местом в системе наук и связями с другими дисциплинами;

– краткое, но по существу, изложение комплекса основных научных понятий, подходов, методов, принципов данной дисциплины;

– краткое изложение наиболее существенных положений, раскрытие особенно сложных, актуальных вопросов, освещение дискуссионных проблем;

– определение перспективных направлений дальнейшего развития научного знания в области информационной безопасности.

Значимым фактором полноценной и плодотворной работы обучающегося на лекции является культура ведения конспекта. Принципиально неверным, но получившим в наше время достаточно широкое распространение, является отношение к лекции как к «диктанту», который обучающийся может аккуратно и дословно записать. Слушая лекцию, необходимо научиться выделять и фиксировать ее ключевые моменты, записывая их более четко и выделяя каким-либо способом из общего текста.

Полезно применять какую-либо удобную систему сокращений и условных обозначений (из известных или выработанных самостоятельно, например, менеджмент обозначать большой буквой М). Применение такой системы поможет значительно ускорить процесс записи лекции. Конспект лекции предпочтительно писать в одной тетради, а не на отдельных листках, которые потом могут за-

теряться. Рекомендуется в конспекте лекций оставлять свободные места, или поля, например, для того, чтобы была возможность записи необходимой информации при работе над материалами лекций.

При ведении конспекта лекции необходимо четко фиксировать рубрикацию материала – разграничение разделов, тем, вопросов, параграфов и т. п. Обязательно следует делать специальные пометки, например, в случаях, когда какое-либо определение, положение, вывод остались неясными, сомнительными. Иногда обучающийся не успевает записать важную информацию в конспект.

Тогда необходимо сделать соответствующие пометки в тексте, чтобы не забыть, восполнить эту информацию в дальнейшем.

Качественно сделанный конспект лекций поможет обучающемуся в процессе самостоятельной работы и при подготовке к сдаче зачета с оценкой.

Практические занятия по дисциплине «Информационная безопасность» проводятся в соответствии с п. 5.4 по отдельным группам. Цели практических занятий: закрепить теоретические знания, полученные студентом на лекциях и в результате самостоятельного изучения соответствующих разделов рекомендуемой литературы; приобрести начальные практические умения работы в различных областях обеспечения защиты информации.

Темы практических занятий заранее сообщаются обучающимся для того, чтобы они имели возможность подготовиться и проработать соответствующие теоретические вопросы дисциплины. В начале каждого практического занятия преподаватель:

– кратко доводит до обучающихся цели и задачи занятия, обращая их внимание на наиболее сложные вопросы по изучаемой теме;

– проводит устный опрос обучающихся, в ходе которого также обсуждаются дикуссионные вопросы.

На практических занятиях обучающиеся выполняют практические задания, готовят письменный отчет, конспектируют новую информацию и обсуждают результаты выполненного практического задания. Преподаватель в этом процессе может выступать в роли консультанта или модератора.

По итогам практических занятий преподаватель выставляет полученные обучающимся баллы, согласно п. 9.1 и п. 9.2.

В современных условиях перед студентом стоит важная задача – научиться работать с массивами информации. Обучающимся необходимо развивать в себе способность и потребность использовать доступные информационные возможности и ресурсы для поиска нового знания и его распространения. Обучающимся необходимо научиться управлять своей исследовательской и познавательной деятельностью в системе «информация – знание – информация». Прежде всего, для достижения этой цели, в вузе организуется самостоятельная работа обучающихся. Кроме того, современное обучение предполагает, что существенную часть времени в освоении учебной дисциплины обучающийся проводит самостоятельно. Принято считать, что такой метод обучения должен способствовать творческому овладению обучающимися специальными знаниями и навыками.

Самостоятельная работа обучающегося весьма многообразна и содержательна. Она включает следующие виды занятий (п. 5.6):

– работу с основной и дополнительной литературой, программным обеспечением и интернет-ресурсами, составление конспекта;

– подготовку к устному опросу по теме практического занятия (перечень типовых вопросов для текущего контроля в п. 9.6);

– подготовку к практичсскому занятию.

Систематичность занятий предполагает равномерное, в соответствии с пп. 5.2, 5.4 и 5.6, распределение объема работы в течение всего предусмотренного учебным планом срока овладения дисциплиной «Информационная безопасность» (дисциплина изучается в течение 7-го семестра). Такой подход позволяет избежать дефицита времени, перегрузок, спешки и т. п. в завершающий период изучения дисциплины. Последовательность работы означает преемственность и логику в овладении знаниями по дисциплине «Информационная безопасность». Данный принцип изначально заложен в учебном плане при определении очередности изучения дисциплин. Аналогичный подход применяется при определении последовательности в изучении тем дисциплины.

Завершающим этапом самостоятельной работы является подготовка к сдаче зачета с оценкой по дисциплине, предполагающая интеграцию и систематизацию всех полученных при изучении учебной дисциплины знаний.

Зачет с оценкой (промежуточная аттестация по итогам освоения дисциплины «Информационная безопасность») позволяет определить уровень освоения обучающимся компетенций (п. 9.5) за период изучения данной дисциплины. Зачет с оценкой предполагает ответы на 2 теоретических вопроса из перечня вопросов, вынесенных на промежуточную аттестацию, а также решение практического задания (п. 9.6).

34

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 20.03.01 «Техносферная безопасность».

Программа рассмотрена и утверждена на заседании кафедры № 8 «Прикладной математики и информатики

«9» 04 2019 года, протокол № 9.

Разработчик:

к.п.н. Самойлов В.А.

ученая степень, ученое звание, фамилия и инициалы разработчика

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

д.т.н., профессор Балясников В.В.

ученая степень, ученое звание, фамилия и инициалы руководителя ОПОП

Программа одобрена на заседании Учебно-методического совета Университета «16» 04 2019 года, протокол № 6.