

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

2017 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки

**25.03.04 Эксплуатация аэропортов и обеспечение полетов воздушных су-
дов**

Направленность программы (профиль)

Организация и обеспечение транспортной безопасности

Квалификация выпускника

бакалавр

Форма обучения:

очная

Санкт-Петербург

2017

1 Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» являются формирование у студентов знаний по основам информационной безопасности, 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 эксплуатационно-технологическому виду профессиональной деятельности.

2 Место дисциплины в структуре ОПОП ВО

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

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

Дисциплина «Информационная безопасность» является заключительной по формированию входящих в нее компетенций.

Дисциплина «Информационная безопасность» изучается в 5 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
готовностью пользоваться информацией, получаемой из глобальных компьютерных сетей (ОК-47);	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

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
	при работе в сети интернет; Владеть: - методами поиска и обмена информацией в глобальных и локальных компьютерных сетях.
готовностью работать с программными средствами общего назначения при решении профессиональных задач (ПК-8);	Знать: - основные нормативные и правовые акты в области ИБ; - основные определения и составляющие ИБ; Уметь: – соблюдать основные требования ИБ, в том числе защиты государственной тайны; Владеть: - техническими и программными средствами защиты информации при работе с компьютерными системами, включая приемы антивирусной защиты.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6 зачетные единицы, 216 академических часов.

Наименование	Всего часов	Семестр
		5
Общая трудоемкость дисциплины	216	216
Контактная работа:	114,5	114,5
лекции	56	56
практические занятия	56	56
семинары	–	–
лабораторные работы	–	–
курсовой проект (работа)	–	–
Самостоятельная работа студента	68	68
Промежуточная аттестация:	36	36
контактная работа	2,5	2,5
самостоятельная работа по подготовке к экзамену	33,5	33,5

5 Содержание дисциплины

5.1 Соотнесения тем (разделов) дисциплины и формируемых компетенций

№ п/п	Темы, РАЗДЕЛЫ дисциплины	КОЛИЧЕСТВО ЧАСОВ	Компетенции		Образовательные технологии	Оценочные средства
			ОК-47	ПК-8		
1.	Информационная безопасность (ИБ) деятельности общества. Организационное и правовое обеспечение ИБ.	20	+		Л, ПЗ	СРС, ВК, У
2.	Основы обеспечения ИБ жизнедеятельности общества и его структур.	40	+	+	Л, ПЗ	СРС, У, О
3.	Основы технического обеспечения ИБ.	40	+	+	Л, ПЗ	СРС, У, О
4.	Программно-аппаратные средства обеспечения ИБ в компьютерных системах.	40		+	Л, ПЗ	СРС, У, О
5.	Технические средства НСД, методы защиты и обнаружения.	40	+		Л, ПЗ	СРС, У, О
	Промежуточная аттестация	36				
	Итого по дисциплине	216				

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

5.2 Темы (разделы) дисциплины и виды

№ п/п	Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов

1	Информационная безопасность (ИБ) деятельности общества. Организационное и правовое обеспечение ИБ.	8	6			6		20
2	Основы обеспечения ИБ жизнедеятельности общества и его структур.	10	10			20		40
3	Основы технического обеспечения ИБ.	14	10			16		40
4	Программно-аппаратные средства обеспечения ИБ в компьютерных системах.	10	10			20		40
5	Технические средства НСД, методы защиты и обнаружения.	14	20			6		40
	Итого по дисциплине	56	56	0	0	68		180
	Промежуточная аттестация							36
	Всего по дисциплине							216

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

5.3 Содержание дисциплины

1. Информационная безопасность (ИБ) 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.

2. Основы обеспечения ИБ жизнедеятельности общества и его структур.

Информационное противоборство. Ее психологическая и техническая составляющие.

Угрозы информационной безопасности. Антивирусная защита в АС.

Построение систем защиты от угроз информации в АС..

3. Основы технического обеспечения ИБ.

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.

4. Программно-аппаратные средства обеспечения ИБ 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 ACSecretNet и Сфера. Особенности, правила использования.

5. Технические средства НСД, методы защиты и обнаружения.

Защита информации от утечки по техническим каналам.

Противодействие несанкционированному доступу к источникам конфиденциальной информации.

Аудит информационной безопасности.

5.4 Практические занятия (семинары)

№ п/п	Номер темы дисциплины	Тематика практических занятий (семинаров)	Трудоемкость (часы)
1.	1	Стандарты информационной безопасности.	2
2.	1	Нормативные акты, руководящие документы РФ в области ИБ.	2
3.	2	Информационное противоборство. Проявления информационного противоборства.	2
4.	2	Антивирусные средства.	2
5.	2	Поиск и нейтрализация вирусных угроз в АС.	2
6.	2	Разработка систем защиты от угроз нарушения информации в АС.	2
7.	2	Средства криптографической защиты информации.	2
8.	2	Криптографические алгоритмы.	2
9.	3	Определение уязвимости компьютеров и компьютерной сети.	2
10.	3	Анализ атак на компьютерные системы.	2
11.	3	Использование сетевых средств экранирования в АС.	2
12.	3	Использование системы анализа защищенности	2
13.	3	Использование системы обнаружения и предотвращения вторжений.	2
14.	3	Настройка параметров информационной безопасности в АС.	2
15.	3	Настройка параметров информационной безопасности в системах управления базами	2

№ п/п	Номер темы дисциплины	Тематика практических занятий (семинаров)	Трудоемкость (часы)
		данных.	
16.	4	Разработка и использование политик безопасности в АС.	2
17.	4	СКЗИ SecretNet и Сфера. Особенности, правила использования.	2
18.	4	Настройка и использование СКЗИ SecretNet и Сфера.	2
19.	5	Способы несанкционированного доступа.	2
20.	5	Технические средства НСД.	2
21.	5	Защита информации от утечки по визуальным каналам.	2
22.	5	Защита информации от утечки по визуальным каналам.	2
23.	5	Защита информации от утечки по акустическим каналам.	2
24.	5	Защита информации от утечки по материально-вещественным каналам.	2
25.	5	Защита информации от наблюдения и фотографирования.	2
26.	5	Противодействие незаконному подключению к линиям связи	2
27.	5	Защита от перехвата.	2
28.	5	Аудит выделенных помещений.	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	Нормативные акты, руководящие документы Российской Федерации в области информационной безопасности. [1, 3] Изучение, составление конспекта. Индивидуальное задание.	2
1	Обзор и сравнительный анализ стандартов информационной безопасности. [3] Изучение, составле-	4

Номер темы дисциплины	Виды самостоятельной работы	Трудоемкость (часы)
	ние конспекта. Индивидуальное задание.	
2	Угрозы информационной безопасности. Антивирусная защита в АС. [1, 3] Изучение, составление конспекта. Индивидуальное задание.	6
2	Построение систем защиты от угроз информации в информационных системах. [3] Изучение, составление конспекта.	6
2	Криптографические методы защиты информации. [2, 3] Изучение, составление конспекта. Индивидуальное задание.	8
3	Уязвимости компьютеров и компьютерных сетей. [2, 3] Изучение, составление конспекта.	2
3	Основные виды атак на компьютерные системы. [2, 3] Изучение, составление конспекта.	4
3	Сетевые средства экранирования в АС. [2] Изучение, составление конспекта. Индивидуальное задание.	4
3	Системы анализа защищенности. [2] Изучение, составление конспекта. Индивидуальное задание.	2
3	Системы обнаружения и предотвращения вторжений. [2] Изучение, составление конспекта. Индивидуальное задание.	4
4	Обеспечение сохранности данных и защита ПЭВМ в АС. Информационная безопасность систем управления базами данных. [1, 2] Изучение, составление конспекта.	6
4	Политика безопасности в АС. Принципы построения. [1, 2] Изучение, составление конспекта. Индивидуальное задание.	6
4	СКЗИ в АС SecretNet и Сфера. Изучение, составление конспекта. [1, 2, 3] Индивидуальное задание.	8
5	Технические средства доступа к конфиденциальной информации.	2
5	Защита от утечки по техническим каналам.	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. Мельников, В.П. и др. **Информационная безопасность и защита информации** [Текст]: учеб. пособие для студ. высш. учеб. заведений/В.П.Мельников, С.А. Клейманов, А.М. Петраков; под ред. С.А. Клейманова. – 2-е изд., стер. — М.: Издательский центр «Академия», 2007. — 336 с. — ISBN 978-5-7695-4148-3
2. Запечников, С.В. и др. **Информационная безопасность открытых систем** [Текст]: Учебник для вузов. В 2-х томах. М.: Горячая линия-Телеком, 2008. — 558 с.: ил. — ISBN 978-5-9912-0034-9/
3. Цирлов, В.Л. **Основы информационной безопасности** [Текст]: краткий курс. Ростов н/Д: Феникс, 2008.— 253, [1]с. – Профессиональное образование). — ISBN 978-5-222-13164-0.

б) дополнительная литература:

4. Ярочкин, В.И. **Информационная безопасность** [Текст]: Учебник для вузов. — М.: Академический проект, 2006-4-е изд. — 544 с. — ISBN 5-8291-0740-6.
5. Прохода, А.Н. **Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов.** — М.: Горячая линия-Телеком, 2007.— 180 с.: ил.— ISBN 5-93517-302-6.
6. Сердюк, В.А. **Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий** [Текст]. — М.: Высшая Школа Экономики (Государственный Университет), 2011.— 576 с. — ISBN 978-5-7598-0698-1.
7. Руководство по эксплуатации СКЗИ «Сфера». [Текст]. — С-Пб.: ООО «Фирма «НИТА», 2015.— 57 с.

в) перечень ресурсов информационно-телекоммуникационной сети

«Интернет»

8. **Фирма «НИТА»** [Электронный ресурс]: официальный сайт ООО «Фирма «НИТА». — Режим доступа : <http://www.nita.ru>, свободный (дата обращения: 01.02.2015).
9. Система поиска **Google**[Электронный ресурс]. — Режим доступа:www.google.com, свободный (дата обращения: 01.02.2015).
10. **Электронная библиотека** [Электронный ресурс]. — Режим доступа:www.wikipedia.org, свободный (дата обращения: 01.02.2015).
11. **Онлайн переводчик** [Электронный ресурс]. — Режим доступа:www.lingvo.ru. , свободный (дата обращения: 01.02.2015).
12. **InformationSecurity/Информационная безопасность** [Электронный ресурс]: официальный сайтжурнала «InformationSecurity/Информационная

безопасность» – Режим доступа:www.itsec.ru, свободный (дата обращения: 01.02.2015).

13. **Информационно-аналитический ресурс и виртуальная площадка для общения менеджеров и экспертов по информационной безопасности** [Электронный ресурс]. – Режим доступа: www.iso27000.ru, свободный (дата обращения: 01.02.2015).
14. **Федеральная служба по техническому и экспортному контролю (ФСТЭК России)** [Электронный ресурс] : официальный сайт ФСТЭК РФ.– Режим доступа: <http://fstec.ru>, свободный (дата обращения: 01.02.2015).
15. **Справочно-правовая база Гарант** [Электронный ресурс]. – Режим доступа: <http://www.garant.ru/> (Дата обращения 25.12.2015).

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

16. **Единое окно доступа к образовательным ресурсам** [Электронный ресурс]. – Режим доступа: <http://window.edu.ru>, свободный (дата обращения: 29.03.2015).
17. **Консультант Плюс** [Электронный ресурс]: официальный сайт компании Консультант Плюс. — Режим доступа: <http://www.consultant.ru/>, свободный (дата обращения: 29.03.2015).
18. **Электронная библиотека научных публикаций «eLIBRARY.RU»** [Электронный ресурс] — Режим доступа: <http://elibrary.ru/>, свободный (дата обращения: 29.03.2015).
19. **Электронно-библиотечная система издательства «Лань»** [Электронный ресурс] — Режим доступа: <http://e.lanbook.com/>, свободный (дата обращения: 29.03.2015).

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 преподавателем в начале изучения дисциплины с целью коррекции процесса усвоения студентами дидактических единиц. Он осуществляется по вопросам дисциплины «Информатика», на которой базируется дисциплина «Информационная безопасность».

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.

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 управленческих задач, а также овладевают умениями и навыками оценки управленческих решений.

Практические занятия по дисциплине «Информационная безопасность» проводятся в компьютерных классах, в которых студенты выполняют 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 помощи 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 экзамена.

Фонд оценочных средств дисциплины «Информационная безопасность» для текущего включает: устные опросы, доклады, письменную аудиторную работу и десятиминутный тест.

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.

Доклад □ это продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической или учебно-исследовательской темы. Доклады студентов занимают не больше 10 минут и могут проводиться в форме презентаций в среде MSOfficePowerPoint.

Промежуточная аттестация по итогам освоения дисциплины проводится в виде экзамена в 5 семестре. Этот вид промежуточной аттестации позволяет оценить уровень освоения студентом компетенций за весь период изучения дисциплины. Экзамен предполагает устные ответы на 2 теоретических 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)	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.	масим.		
	Обязательные виды занятий				
1	Практическая работа № 1.				
	Стандарты информационной	1	2	1	

Раздел (тема)	Раздел (тема) / Вид учебных занятий (оценочных зада- ний), позволяющих студенту продемонстрировать дости- нутый уровень сформирован- ности компетенций	Количество баллов (из об- щего расчета 100 баллов на дисциплину)		Срок контроля (№ недели с начала семестра)	Примечание
		миним.	масим.		
	безопасности.				
1	Практическая работа № 2.				
	Нормативные акты, руководя- щие документы РФ в области ИБ.	1	2	1	
	Итого баллов по разделу (те- ме)	2	4		
2	Практическая работа № 3.				
	Информационное противобор- ство. Проявления информаци- онного противоборства.	1	2	2	
2	Практическая работа № 4.				
	Антивирусные средства.	1	2	2	
2	Практическая работа № 5.				
	Поиск и нейтрализация вирус- ных угроз в АС.	1	2	3	
2	Практическая работа № 6.				
	Разработка систем защиты от угроз нарушения информации в АС.	1	2	4	
2	Практическая работа № 7.				
	Средства криптографической защиты информации.	1	2	5	
2	Практическая работа № 8.				
	Криптографические алгоритмы.				
	Итого баллов по разделу (те- ме)	5	10		
3	Практическая работа № 9.				
	Определение уязвимости ком- пьютеров и компьютерной сети.	1	2	6	
3	Практическая работа № 10.				
	Анализ атак на компьютерные системы.	1	2	7	
3	Практическая работа № 11.				
	Использование сетевых средств экранирования в АС.	1	2	8	
3	Практическая работа № 12.				

Раздел (тема)	Раздел (тема) / Вид учебных занятий (оценочных зада- ний), позволяющих студенту продемонстрировать достиг- нутый уровень сформирован- ности компетенций	Количество баллов (из об- щего расчета 100 баллов на дисциплину)		Срок контроля (№ недели с начала семестра)	Примечание
		миним.	масим.		
	Использование системы анализа защищенности	1	2	9	
3	Практическая работа № 13.				
	Использование системы обна- ружения и предотвращения вторжений.	1	2	10	
3	Практическая работа № 14.				
	Настройка параметров инфор- мационной безопасности в АС.	1	2	11	
3	Практическая работа № 15.				
	Настройка параметров инфор- мационной безопасности в сис- темах управления базами дан- ных.	1	2	12	
	Итого баллов по разделу (те- ме)	14	28		
4	Практическая работа № 16.				
	Разработка и использование по- литик безопасности в АС.	1	2	13	
4	Практическая работа № 17.				
	Настройка и использование СКЗИ SecretNet и Сфера.	1	2	14	
4	Практическая работа № 18.				
	СКЗИ SecretNet и Сфера. Осо- бенности, правила использова- ния.	1	2	15	
	Итого баллов по разделу (те- ме)	3	6		
5	Практическая работа № 19.				
	Способы несанкционированно- го доступа.	1	2	16	
5	Практическая работа № 20.				
	Технические средства НСД.	1	2	17	
5	Практическая работа № 21.				
	Защита информации от утечки по визуальным каналам.	1	2	18	
5	Практическая работа № 22.				

Раздел (тема)	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.	масим.		
	Защита информации от утечки по визуальным каналам.	1	2	19	
5	Практическая работа № 23.				
	Защита информации от утечки по акустическим каналам.	1	2	20	
5	Практическая работа № 24.				
	Защита информации от утечки по материально-вещественным каналам.	1	2	21	
5	Практическая работа № 25.				
	Защита информации от наблюдения и фотографирования.	1	2	22	
5	Практическая работа № 26.				
	Противодействие незаконному подключению к линиям связи	1	2	23	
5	Практическая работа № 27.				
	Защита от перехвата.	1	2	24	
5	Практическая работа № 28.				
	Аудит выделенных помещений.	1	2	25	
	Итого баллов по разделу (теме)	10	20		
	Итого по обязательным видам занятий	28	56		
	<i>Экзамен</i>	32	44		
	<i>Итого по дисциплине</i>	60	100		
	Научные публикации по теме дисциплины	10	10		
	Участие в конференциях по теме дисциплины	10	10		
	Прочее				
	Итого дополнительно премиальных баллов				
	Всего по дисциплине (для рейтинга)	80	120		
	<p>*) – разделы (темы) могут не выделяться, а их названия не приводиться;</p> <p>**) – может вводиться для дополнительного стимулирования текущей работы студента в семестре.</p>				

Раздел (тема)	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.	масим.		
Перевод баллов балльно-рейтинговой системы в оценку по 5-ти балльной «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

Посещение лекционного занятия обучающимся лекционного занятия оценивается в 1 балл. Ведение лекционного конспекта – 0,5 баллов. Активное участие в обсуждении дискуссионных вопросов в ходе лекции – до 0,5 баллов.

Посещение практического занятия с ведением конспекта оценивается в 2 балла. Доклад – до 0,5 балла. Участие в обсуждении доклада – до 0,5 балла. Письменная аудиторная работа □ от 2 до 3 баллов. Успешное написание десятиминутного теста: более 50 % и до 75 % правильных ответов – 1 балл, более 75 % – 1,5 балла.

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

Обеспечивающие дисциплины «Информатика», «Операционные системы и сети».

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 Office. 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.

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

Этапы формирования компетенций соответствуют последовательности семестров, в которых формируется данная компетенция. Исходя из этого имеет смысл использовать следующие укрупненные формулировки для указания этапов:

1. Начальный этап - указанная компетенция появляется в качестве одного из результатов обучения некоторой дисциплины в первый раз с начала обучения в университете.
2. Промежуточный этап - указанная компетенция уже появлялась в качестве одного из результатов обучения некоторых дисциплин в предыдущие семестры.
3. Конечный этап - указанная компетенция появляется в качестве одного из результатов обучения последний раз.

За основу оценивания уровня сформированности компетенций мы примем уровни усвоения деятельности человека, разработанные В.П. Беспалько (Беспалько В.П. Слагаемые педагогической технологии. - М.: Педагогика, 1989. - 192 с.: ил. ISBN 5-7155-0099-0, стр. 55):

1 уровень. Если в задаче заданы цель, ситуация и действия по ее решению, а от студента требуется дать заключение о соответствии всех трех компонентов в структуре задачи, это **деятельность по узнаванию**. Студенты могут ее выполнять только при повторном восприятии ранее усвоенной информации об объектах, процессах или действиях с ними. Это **алгоритмическая деятельность «с подсказкой»**.

2 уровень. Если в задаче заданы цель и ситуация, а от студента требуется применить ранее усвоенные действия по ее решению, это **репродуктивное алгоритмическое действие**. Студент выполняет его, самостоятельно воспроизводя и применяя информацию о ранее усвоенной ориентировочной основе выполнения данного действия. Такая задача называется «**типовой**», **воспроизводимой по памяти**.

3 уровень. Если в задаче задана цель, но неясна ситуация, в которой цель может быть достигнута, а от студента требуется дополнить (уточнить) ситуацию и применить ранее усвоенные действия для решения данной нетиповой задачи, это **продуктивное действие эвристического типа**. Студент в процессе выполнения задания добывает субъективно новую информацию (только для себя новую) в ходе самостоятельной трансформации известной ориентировочной основы действия (ООД) типового и построения субъективно новой ООД для решения нетиповой задачи. Это **эвристическая деятельность, выполненная не по готовому алгоритму или правилу**, а по созданному или преобразованному в ходе самого действия, например, решение конкретной задачи или выполнение конкретного проекта по известному общему методу путем самостоятельного приспособления к условиям задачи, результат решения которой предскажем лишь в общем виде.

4 уровень. Если в задаче известна лишь в общей форме цель деятельности, а поиску подвергаются и подходящая ситуация и действия, ведущие к достижению цели, это **продуктивное действие творческого типа**, в результате которого создается объективно новая ориентировочная основа деятельности. В процессе выполнения деятельности добывается объективно новая информация. Человек действует «без правил», но в известной ему области, создавая новые правила действия, **творческая (исследовательская) деятельность**.

При определении показателя «**Знание**» в качестве объекта оценивания будет выступать ответ на вопрос повествовательного, фактографического или описательного характера. Критерии оценивания соответствуют указанным выше уровням в предположении, что 1 уровень это «удовлетворительно», 2 – «хорошо», а третий – «отлично».

При оценивании показателя «**Умение**» в качестве объекта оценивания выступает какое-либо практическое действие или решение задачи. Критерии оценивания соответствуют 1-3 уровням с выставлением оценок аналогично представленному выше.

При оценивании показателя «**Владение**» объекты оценивания аналогичны при оценивании «**Умения**», но существует ограничение по времени выполнения задания.

4 уровень (творческий) не входит в стандартную шкалу оценивания, однако может быть учтен при оценивании индивидуально.

Показатель	Критерий	Шкала оценивания
Знание – ответы на вопросы повествователь-	Узнавание – выбор известного и типового	Удовлетворительно (6-7 баллов)

ного, фактографического или описательного характера	<p>Репродуктивный ответ - воспроизведение известного и типового</p> <p>Продуктивный ответ - ответ с элементами синтеза, анализа, классификации не по изученным шаблонам</p>	<p>Хорошо (7-8 баллов)</p> <p>Отлично (9-10 баллов)</p>
Умение – выполнение заданных действий	<p>Действие с подсказкой – выполнение действий по заданному алгоритму</p> <p>Репродуктивное действие – выполнение типовых действий</p> <p>Продуктивное действие – выполнение действий с неполными исходными данными</p>	<p>Удовлетворительно (6-7 баллов)</p> <p>Хорошо (7-8 баллов)</p> <p>Отлично (9-10 баллов)</p>
Владение – уверенное выполнение заданных действий или выполнение заданных действий за ограниченное время	<p>Действие с подсказкой – уверенное выполнение заданных действий или выполнение действий по заданному алгоритму за ограниченное время</p> <p>Репродуктивное действие – уверенное выполнение типовых действий или их выполнение за ограниченное время</p> <p>Продуктивное действие – уверенное выполнение действий с неполными исходными данными или выполнение их за ограниченное время</p>	<p>Удовлетворительно (6-7 баллов)</p> <p>Хорошо (7-8 баллов)</p> <p>Отлично (9-10 баллов)</p>

Характеристики шкалы оценивания приведены ниже.

1. Максимальное количество баллов за экзамен – 30. Минимальное (зачетное) количество баллов («экзамен сдан») – 18 баллов.

2. При наборе менее 18 баллов – экзамен не сдан по причине недостаточного уровня знаний.

3. Экзаменационная оценка выставляется как сумма набранных баллов за ответы на вопросы и задания билета теоретического и практического характера (по 10 баллов на один вопрос или задание).

4. Билет состоит из одного теоретического вопроса, соответствующего показателю «Знание», одного практического задания, соответствующего показателю «Умение» и одного практического задания, соответствующего показателю «Владение».

5. Ответы на вопросы и задания билета оцениваются в соответствии с предложенным подходом В.П. Беспалько:

«неудовлетворительно» - при наборе за ответы не более 17 баллов (критерии оценивания ниже 1 уровня);

«3 - удовлетворительно» - при наборе за ответы от 18 до 21 баллов (критерии оценивания 1 уровня);

«4 - хорошо» - при наборе за ответы от 22 до 26 баллов (критерии оценивания 2 уровня);

«5 – отлично» - при наборе за ответы от 27 до 30 баллов (критерии оценивания 3 уровня);

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

Примерный перечень вопросов к экзамену для проведения промежуточного контроля по дисциплине

Показатель «Знание»

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.

2. Примерный перечень практических заданий к экзамену для проведения промежуточного контроля по дисциплине

Показатель «Умение»

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.

Показатель «Владение»

1. Установка и настройка незнакомого антивирусного программного пакета или известного за ограниченное время.
2. Нахождение зашифрованных файлов с помощью программы PGP и их расшифровка.
3. Расшифровка сообщения путем подбора ручных симметричных способов шифрования.
4. Разработка и настройка параметров парольной защиты для повышения защищенности от попыток его дискредитации в условной организации.

3. Примерный перечень вопросов текущего контроля

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.

10 Методические рекомендации для обучающихся по освоению дисциплины

Приступая в 5 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), на которой базируется дисциплина «Информационная безопасность» (п. 2).

В ходе лекции преподаватель излагает и разъясняет основные, наиболее сложные понятия, а также соответствующие 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.

Темы лекций и рассматриваемые в ходе их вопросы приведены в п. 5.3.

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 затеряться. 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 рубрикации 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 экзамена.

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:

- кратководит 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 дискуссионные вопросы.

На практических занятиях обучающиеся представляют самостоятельно подготовленные доклады, в том числе в виде презентаций, которые выполнены в MS PowerPoint, конспектируют новую информацию и обсуждают эти доклады. Преподаватель в этом процессе может выступать в роли консультанта или модератора.

По итогам лекций и практических занятий преподаватель выставляет в журнал полученные обучающимся баллы, согласно п. 9.1 и п. 9.2. Отсутствие студента на занятиях или его неактивное участие в них может быть компенсировано самостоятельным выполнением дополнительных заданий и представлением их на проверку преподавателю в установленные им сроки.

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. Обучаю-

щимся 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):

- самостоятельный поиск, анализ информации и проработка учебного материала;
- подготовку к устному опросу (перечень типовых вопросов для текущего контроля в п. 9.6).

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 5-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 экзамена по дисциплине, предполагающая интеграцию и систематизацию всех полученных при изучении учебной дисциплины знаний.

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

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВПО по направлению подготовки 25.03.04 «Эксплуатация аэропортов и обеспечение полетов воздушных судов».

Программа рассмотрена и утверждена на заседании кафедры №8 «Прикладной математики и информатики» «13» января 2015 года, протокол № 6

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 разработчиков)

Программа рассмотрена и одобрена на заседании Учебно-методического совета Университета «21» 01 2015 года, протокол № 4

С изменениями и дополнениями от «30» августа 2017 года, протокол №10

(в соответствии с Приказом от 05 апреля 2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры).