



**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)**

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

УТВЕРЖДАЮ



/ Ю.Ю. Михальчевский

2021 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки (специальность)

25.03.03 Аэронавигация

Направленность программы (профиль, специализация)

Организация авиационной безопасности

Квалификация выпускника

бакалавр

Форма обучения

очная

Санкт-Петербург

2021

1 Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» являются формирование у студентов теоретических знаний, практических умений и навыков по основам информационной безопасности, применения их в повседневной профессиональной деятельности

Задачами освоения дисциплины «Информационная безопасность» являются:

- изучение основ организационно-правового обеспечения информационной безопасности;
- изучение различных видов угроз, принципов создания защищенных информационных систем, баз данных;
- изучение технических средств определения и защиты от нарушений ИБ;
- формирование умений и навыков использования средств информационной безопасности при работе в компьютерных системах;
- формирование умений и навыков безопасного использования при использовании локальных и глобальных сетей.

Дисциплина обеспечивает подготовку выпускника к осуществлению эксплуатационно-технологической и сервисной деятельности.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность» представляет собой дисциплину, относящуюся к обязательной части блока 1

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

Дисциплина «Информационная безопасность» является обеспечивающей для дисциплин: «Автоматизированные системы управления на воздушном транспорте», «Автоматизация и управление технологическими процессами и производствами на воздушном транспорте».

Дисциплина «Информационная безопасность» изучается в 5-6 семестрах.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

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

ОПК-1; ОПК-2; ОПК-6, ПК-1, ПК-6

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК-1	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
ИД ¹ _{ОПК1}	Ориентируется в пакете прикладных программ, работает со стандартными программными средствами.
ИД ² _{ОПК1}	Выбирает и использует стандартные программные средства для решения поставленных задач в том числе и в сфере профессиональной деятельности.
ОПК-2	Способен формулировать и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ИД ¹ _{ОПК2}	Применяет современные библиотечно – информационные технологии для поиска, сбора и анализа информации, необходимой для решения типовых задач, в том числе и в профессиональной сфере.
ОПК-6	Способен использовать основные законы математических и естественнонаучных дисциплин (модулей) в профессиональной деятельности, в том числе с использованием стандартных программных средств
ИД ² _{ОПК6}	Использует основные законы математики и естественных наук, в том числе для решения профессиональных задач, применяет стандартные программные средства.
ИД ² _{ОПК6}	Соблюдает требования информационной безопасности при сборе и интерпретации данных с применением информационно – коммуникационных технологий в процессе решения типовых задач, в том числе и в профессиональной сфере.
ПК-1	Способен принимать и реализовывать решения в сфере профессиональной деятельности
ИД ¹ _{ПК1}	Выявляет, формулирует и решает проблемы, возникающие в профессиональной деятельности.
ИД ² _{ПК1}	Реализует принятые решения, оценивает последствия их реализации в сфере профессиональной деятельности.
ПК-6	Способен идентифицировать опасности и оценивать риски в профессиональной деятельности

ИД ¹ _{ПК6}	Идентифицирует опасности, возникающие в сфере профессиональной деятельности.
--------------------------------	--

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 8 зачетных единиц, 288 академических часов.

Наименование	Всего часов	Семестры	
		5	6
Общая трудоемкость дисциплины	288	144	144
Контактная работа, всего	119	44,5	74,5
лекции	50	14	36
практические занятия	64	28	36
семинары	—	—	—
лабораторные работы	—	—	—
курсовой проект (работа)	—	—	—
Самостоятельная работа студента	102	66	36
Промежуточная аттестация:	72	36	36
контактная работа	5	2,5	2,5
самостоятельная работа по подготовке к зачету с оценкой, экзамену	67	33,5	33,5

5 Содержание дисциплины

5.1 Соотнесения тем дисциплины и формируемых компетенций

Темы дисциплины	Количество часов	Компетенции					Образовательные технологии	Оценочные средства
		ОПК-1	ОПК-2	ОПК-6	ПК-1	ПК-6		
Тема 1 Информационная безопасность (ИБ) деятельности общества. Организационное и правовое обеспечение ИБ.	40	+			+	+	ВК, Л, ИЛ, СРС, ПЗ	У
Тема 2 Основы обеспечения ИБ жизнедеятельности общества и его структур.	42	+	+				Л, ИЛ, СРС, ПЗ	У

Тема 3 Основы технического обеспечения ИБ.	44	+	+	+	+	Л, ИЛ, СРС, ПЗ	У
Тема 4 Программно-аппаратные средства обеспечения ИБ в компьютерных системах.	44	+	+	+	+	Л, ИЛ, СРС, ПЗ	У
Тема 5 Технические средства НСД, методы защиты и обнаружения.	46			+	+	Л, ИЛ, СРС, ПЗ	У
Итого по семестру	216						
Промежуточная аттестация	72						
Итого по дисциплине	288						

Сокращения: Л – лекция, ИЛ – интерактивная лекция, ПЗ – практическое занятие, СРС – самостоятельная работа студента, ВК – входной контроль, У – устный опрос.

5.2 Темы дисциплины и виды

Наименование темы (раздела) дисциплины	Л	ПЗ	ЛР	СРС	Всего часов
Тема 1 Информационная безопасность (ИБ) деятельности	10	10		20	40
Наименование темы (раздела) дисциплины	Л	ПЗ	ЛР	СРС	Всего часов
общества. Организационное и правовое обеспечение ИБ.					
Тема 2 Основы обеспечения ИБ жизнедеятельности общества и его структур.	10	12		20	42
Тема 3 Основы технического обеспечения ИБ.	10	14		20	44
Тема 4 Программно-аппаратные средства обеспечения ИБ в компьютерных системах.	10	14		20	44
Тема 5 Технические средства НСД, методы защиты и обнаружения.	10	14		22	46
<i>Итого за 5-6 семестры</i>	50	64		102	216
Промежуточная аттестация					72
Всего по дисциплине					288

Сокращения; Л – лекция, ИЛ – интерактивная лекция, ПЗ – практическое занятие, СРС – самостоятельная работа студента, ЛР – лабораторная работа

5.3 Содержание дисциплины

Тема 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.

Тема 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. Симметричная и асимметричная системы шифрования. Электронная цифровая подпись. Сертификация систем информационной защиты. Компьютерные вирусы и организация антивирусной защиты.

Тема 3 Основы технического обеспечения ИБ.

Криптографические методы защиты информации. Алгоритмические основы криптографических систем. Уязвимости компьютеров и компьютерных сетей.

Основные виды атак на компьютерные системы. Сетевые средства экранирования в АС. 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 ИБ в компьютерных системах.

Обеспечение сохранности данных и защита ПЭВМ в АС. Информационная безопасность систем управления базами данных. Политика безопасности в АС. Принципы построения политики безопасности. Комплекс средств защиты информации (КСЗИ) в АС SecretNet и Сфера. Особенности, состав, правила использования. Назначение и алгоритм работы подсистем, входящих в КСЗИ. Администрирование в КСЗИ, реагирование на инциденты информационной безопасности.

Тема 5 Технические средства НСД, методы защиты и обнаружения

Защита информации от утечки по техническим каналам. Физические принципы, лежащие в основе использования и передачи информации по техническим каналам. Физические принципы, лежащие в основе несанкционированного доступа к информации. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Структура, принципы работы, технические характеристики и правила использования технических средств поиска и противодействия НСД. Аудит информационной безопасности.

5.4 Практические занятия

Номер темы дисциплины	Тематика практических занятий	Трудоемкость (часы)
5семестр		
1	Практическое задание №1. Стандарты информационной безопасности.	5
1	Практическое задание №2. Нормативные акты, руководящие документы РФ в области ИБ.	5
2	Практическое задание №3. Информационное противоборство. Проявления информационного противоборства.	6
2	Практическое задание №4. Поиск и нейтрализация вирусных угроз в АС.	6
3	Практическое задание №5. Определение уязвимости компьютеров и компьютерной сети.	2
3	Практическое задание №6. Анализ атак на компью-	4

Номер темы дисциплины	Тематика практических занятий	Трудоемкость (часы)
	терные системы.	
3	Практическое задание №7. Использование сетевых средств экранирования в АС.	4
3	Практическое задание №8. Использование системы анализа защищенности	4
8 семестр		
4	Практическое задание №9. Разработка и использование политик безопасности в АС.	2
4	Практическое задание №10. Программно-аппаратные средства защиты при работе в глобальной и локальной сети.	4
4	Практическое задание №11. Технические средства хранения и защиты конфиденциальной информации.	4
4	Практическое задание №12. Технические средства обеспечения защищенного документооборота.	4
5	Практическое задание №13. Технические средства НСД.	6
5	Практическое задание №14. Защита информации от утечки и перехвата. Аудит выделенных помещений.	8
Итого по дисциплине		64

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, 7- 17] Изучение, составление конспекта. Индивидуальное задание.	10
1	Обзор и сравнительный анализ стандартов информационной безопасности. [3, 7-17] Изучение, составление конспекта. Индивидуальное задание.	10
2	Угрозы информационной безопасности. Антивирусная защита в АС. [1, 3, 7-17] Изучение, состав-	8

Номер темы дисциплины	Виды самостоятельной работы	Трудоемкость (часы)
	ление конспекта. Индивидуальное задание.	
2	Построение систем защиты от угроз информации в информационных системах. [3, 7-17] Изучение, составление конспекта.	6
2	Криптографические методы защиты информации. [2, 3, 7-17] Изучение, составление конспекта. Индивидуальное задание.	6
3	Уязвимости компьютеров и компьютерных сетей. [2, 3, -17] Изучение, составление конспекта.	2
3	Основные виды атак на компьютерные системы. [2, 3, 7-17] Изучение, составление конспекта.	2
3	Сетевые средства экранирования в АС. [1,2, 4, 5, 7 - 17] Изучение, составление конспекта. Индивидуальное задание.	2
3	Системы анализа защищенности. [1 - 12] Изучение, составление конспекта. Индивидуальное задание.	2
3	Системы обнаружения и предотвращения вторжений. [1 - 12] Изучение, составление конспекта. Индивидуальное задание.	2
4	Обеспечение сохранности данных и защита ПЭВМ в АС. Информационная безопасность систем управления базами данных. [1- 6] Изучение, составление конспекта.	8
4	Политика безопасности в АС. Принципы построения. [1 - 6] Изучение, составление конспекта. Индивидуальное задание.	6
4	СКЗИ в ACSecretNet и Сфера. Изучение, составление конспекта. [1 - 6] Индивидуальное задание.	6
5	Технические средства доступа к конфиденциальной информации.	6
5	Защита от утечки информации по техническим каналам [1 - 17].	8
Итого по дисциплине		102

5.7 Курсовые проекты

Курсовые проекты 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, 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 (дата обращения 16.01.2021).

3 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 (дата обращения 16.01.2021).

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, 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 (дата обращения 16.01.2021).

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, 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 (дата обращения 16.01.2021).

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

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

7 **Фирма «НИТА»** [Электронный ресурс]: официальный сайт ООО «Фирма «НИТА». — Режим доступа : <http://www.nita.ru>, свободный (дата обращения: 01.02.2017).

8 **Система поиска Google**[Электронный ресурс]. – Режим доступа:www.google.com, свободный (дата обращения: 01.02.2021).

9 **Электронная библиотека** [Электронный ресурс]. – Режим доступа: www.wikipedia.org, свободный (дата обращения: 01.02.2021).

10 **Онлайн переводчик** [Электронный ресурс]. – Режим доступа: www.lingvo.ru, свободный (дата обращения: 01.02.2021).

11 **InformationSecurity/Информационная безопасность** [Электронный ресурс]: официальный сайт журнала «InformationSecurity/Информационная безопасность» – Режим доступа: www.itsec.ru, свободный (дата обращения: 01.12.2021).

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: 01.12.2021).

13 **Федеральная служба по техническому и экспортному контролю (ФСТЭК России)** [Электронный ресурс]: официальный сайт ФСТЭК РФ.– Режим доступа <https://fstec.ru/> свободный (дата обращения: 01.12.2021).

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

14 **Электронная библиотека научных публикаций «eLIBRARY.RU»** [Электронный ресурс] — Режим доступа: <http://elibrary.ru/>, свободный (дата обращения: 21.01.2021 г.);

15 **Электронно-библиотечная система издательства «Юрайт»** [Электронный ресурс] — Режим доступа: <https://biblio-online.ru>, свободный (дата обращения: 21.01.2021 г.);

16 **Scilab** [Программное обеспечение] — Режим доступа: <https://www.scilab.org/> - свободный (дата обращения: 21.01.2021).

17 **Электронно-библиотечная система издательства «Лань»** [Электронный ресурс]. Режим доступа: www.e.lanbook.com свободный

7 Материально-техническое обеспечение дисциплины

Наименование дисциплины	Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Информационная безопасность	Ауд. 800 «Компьютерный класс № 1»	Компьютерные столы - 12 шт., стулья - 12 шт., 12 персональных компьютеров, с доступом в сеть Интернет, учебная доска, экран для	Qt Creator ((L)GPL v3) PascalABC.NET((L)GPL v3) VisualStudioCommunity (бесплатное лицензионное соглашение) Kaspersky Anti-Virus Suite (лицензия № 1D0A170720092603110550) Notepad++ (GPL v2) Microsoft Windows Office Professional Plus 2007 (лицензия № 43471843)

		проектора.	
Информационная безопасность	Ауд. 801 «Компьютерный класс № 2»	Компьютерные столы - 16 шт., круглый стол – 2 шт., стулья - 28 шт., 28 персональных компьютеров, с доступом в сеть Интернет, учебная доска, экран для проектора.	PascalABC.NET ((L)GPL v3) VisualStudioCommunity (бесплатное лицензионное соглашение) Kaspersky Anti-Virus Suite (лицензия № 1D0A170720092603110550) Photoshop CS3 (госконтракт № SBR1010080401-00001346-01) VirtualBox(GPL v2) Scilab (CeCILL) Microsoft Windows Office Professional Plus 2007 (лицензия № 43471843)
Информационная безопасность	Ауд. 802 «Лаборатория информатики»	Компьютерные столы - 40 шт., стулья - 40 шт., 40 персональных компьютеров, с доступом в сеть Интернет, учебная доска, проектор (переносной), экран для проектора (переносной).	Anaconda3 (BSD license) Photoshop CS3 (госконтракт № SBR1010080401-00001346-01) Kaspersky Anti-Virus Suite (лицензия № 1D0A170720092603110550) K-Lite Codec Pack (freeware) VirtualBox (GPL v2) Scilab (CeCILL) Microsoft Windows Office Professional Plus 2007 (лицензия № 43471843) VBoxPro 9.0 (госконтракт № SBR1010080401-00001346-01) LogiSim (GNU GPL) VisualStudioCommunity (Бесплатное лицензионное соглашение)
Информационная безопасность	Ауд. 803 «Компьютерный класс № 3»	Компьютерные столы - 11 шт., стулья - 11 шт., 11 персональных компьютеров, с доступом в сеть Интернет, учебная доска.	Kaspersky Anti-Virus Suite (лицензия № 1D0A170720092603110550) Photoshop CS3 (госконтракт № SBR1010080401-00001346-01) K-Lite Codec Pack (freeware) Microsoft Windows Office Professional Plus 2007 (лицензия № 43471843) VirtualBox (GPL v2) PascalABC.NET ((L)GPL v3) Anaconda3 (BSD license) Scilab (CeCILL) LogiSim (GNU GPL) Visual Studio Community (Бесплатное лицензионное соглашение)

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». Перечень вопросов представлен в п. 9.4.

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 интерактивных лекций (48 часов, п.5.1.) в виде проблемных лекций. Проблемные 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, проработ-

ку на этой основе учебного материала, подготовку к устному опросу, а также подготовку к промежуточной аттестации.

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. 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. 9.6.

Промежуточная аттестация по итогам освоения дисциплины проводится в виде экзамена в 5 и экзамена 6 семестрах. Этот вид промежуточной аттестации позволяет оценить уровень освоения студентом компетенций за весь период изучения дисциплины. Экзамен предполагает устные ответы на 3 вопроса из перечня вопросов, вынесенных на промежуточную аттестацию.

9.1 Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов

Балльно-рейтинговая система оценивания не предусмотрена.

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

Выполнение практического задания и устный опрос оцениваются в 5 семестре от 1,6 до 2,5 баллов, в 6 семестре от 1,7 до 2,6 баллов в зависимости от правильности, оптимальности и полноты решения, а также от ответов на дополнительные вопросы преподавателя.

Максимальный балл выставляется, если студент продемонстрировал полные знания теоретического материала и выполнил все пункты задания; мини-

мальное количество – если студент выполнил все пункты задания, но показал слабые знания теоретического материала.

По итогам освоения дисциплины проводится промежуточная аттестация обучающихся в форме экзамена и предполагает устный ответ студента по билетам на два теоретических вопроса и решение одного практического задания.

Экзамен является заключительным этапом изучения дисциплины и имеет целью проверить и оценить учебную работу студентов, уровень полученных ими знаний, умение применять их к решению практических задач, овладение практическими навыками в объеме требований образовательной программы на этапе формирования компетенций. Экзамен по дисциплине проводится в 5 и 6 семестрах. К экзамену допускаются студенты, выполнившие все требования учебной программы и успешно прошедшие промежуточные контрольные точки, предусмотренные настоящей программой.

9.3 Темы курсовых работ (проектов) по дисциплине

1. Использование сетевых средств экранирования в АС.
2. Использование системы анализа защищенности
3. Использование системы обнаружения и предотвращения вторжений.
4. Использование системного реестра ОС Windows в целях защиты ПК.
5. Настройка параметров информационной безопасности в ОС Windows.
6. Разработка и использование политик безопасности в операционной системе.
7. Разработка и использование политик безопасности в АС.
8. Программно-аппаратные средства защиты при работе в глобальной и локальной сети.
9. Технические средства хранения и защиты конфиденциальной информации.
10. Технические средства обеспечения защищенного документооборота.

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

Перечень вопросов по дисциплине «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 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

Компетенции	Показатели оценивания (индикаторы достижения компетенций)	Критерии оценивания
I этап		
ОПК-1	ИД ¹ _{ОПК-1}	Знать: – Принципы работы в пакетах прикладных программ, Уметь: – работать со стандартными программными средствами.
	ИД ² _{ОПК-1}	Знать: – Принципы использования стандартных программных средства для решения поставленных задач, в том числе в сфере профессиональной деятельности Уметь: – использовать стандартные программные средства для решения поставленных задач
ОПК-2	ИД ¹ _{ОПК-2}	Знать: – способы применения современных библиотечно-информационных технологий для поиска, сбора и анализа информации, необходимой для решения типовых задач, в том числе в профессиональной сфере. Уметь: – использовать современные библиотечно-информационные технологии для поиска, сбора и

Компетенции	Показатели оценивания (индикаторы достижения) компетенций	Критерии оценивания
		анализа информации,
ОПК-6	ИД ¹ _{ОПК-6}	Знать: – требования информационной безопасности при сборе и интерпретации данных с применением информационно-коммуникационных технологий в процессе решения типовых задач, в том числе в профессиональной сфере. Уметь: – соблюдать требования информационной безопасности при сборе и интерпретации данных с применением информационно-коммуникационных технологий в процессе решения типовых задач,
	ИД ² _{ОПК-6}	Знать: – основные законы математики и естественных наук и важность их использования в профессиональной деятельности. Уметь: – использовать основные законы математики и естественных наук
ПК-1	ИД ¹ _{ПК-1} ИД ² _{ПК-1}	Знать: – основные законы математики и естественных наук для решения профессиональных задач, Уметь: – применять стандартные программные средства
ПК-6	ИД ¹ _{ПК-6}	
II этап		
ОПК-1	ИД ¹ _{ОПК-1}	Уметь: – ориентироваться в пакетах прикладных программ, Владеть: – навыками работы со стандартными программными средствами.
	ИД ² _{ОПК-1}	Уметь: – выбирать и использовать стандартные программные средства для решения поставленных задач, в том числе в сфере профессиональной деятельности Владеть:

Компетенции	Показатели оценивания (индикаторы достижения) компетенций	Критерии оценивания
		– навыками использования стандартных программных средств для решения поставленных задач, в том числе в сфере профессиональной деятельности
ОПК-2	ИД ¹ _{ОПК-2}	Уметь: – применять современные библиотечно-информационные технологии для поиска, сбора и анализа информации, необходимой для решения типовых задач, в том числе в профессиональной сфере. Владеть: – навыками использования современных библиотечно-информационных технологий для поиска, сбора и анализа информации, необходимой для решения типовых задач, в том числе в профессиональной сфере.
	ИД ² _{ОПК-2}	Уметь: – соблюдать требования информационной безопасности при сборе и интерпретации данных с применением информационно-коммуникационных технологий в процессе решения типовых задач, в том числе в профессиональной сфере. Владеть: – навыками сбора и интерпретации данных с применением информационно-коммуникационных технологий в процессе решения типовых задач, в том числе в профессиональной сфере
ОПК-6	ИД ¹ _{ОПК-6}	Уметь: – использовать основные законы математики и естественных наук в профессиональной деятельности. Владеть: – навыками использования основных законов математики и естественных наук в профессиональной деятельности.
	ИД ² _{ОПК-6}	Уметь: – Использовать основные законы математики и естественных наук для решения профессиональных задач, Владеть:

Компетенции	Показатели оценивания (индикаторы достижения) компетенций	Критерии оценивания
		– правилами работы в стандартных программных средствах
ПК-1 ПК-6	ИД ¹ _{ПК-1} ИД ² _{ПК-1} ИД ¹ _{ПК-6}	Умеет: -свободно работать в офисных приложениях, -выделять базовые информационные технологии для применения в профессиональной деятельности; Владеет: - навыками грамотного проведения и разработки организационно - технической документации установленной отчетности по утвержденным формам; - навыками работы с основными офисными программами; -навыками поиска, обработки информации и сохранения информации;

Шкала оценивания при проведении промежуточной аттестации

«Отлично» выставляется обучающемуся, показавшему всесторонние, систематизированные, глубокие знания по рассматриваемой компетенции и умение уверенно применять их на практике при решении задач, свободное и правильное обоснование принятых решений. Отвечая на вопрос, может быстро и безошибочно проиллюстрировать ответ собственными примерами. Обучающийся самостоятельно правильно решает задачу, дает обоснованную оценку итогам решения.

«Хорошо» выставляется обучающемуся, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задачи некоторые неточности, хорошо владеет всем содержанием, видит взаимосвязи, но не всегда делает это самостоятельно без помощи преподавателя. Обучающийся решает задачу верно, но при помощи преподавателя.

«Удовлетворительно» выставляется обучающемуся, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он владеет основными разделами учебной программы в рамках заданной компетенции, необходимыми для дальнейшего обучения и может применять полученные знания по образцу в стандартной ситуации. Отвечает только на конкретный вопрос, соединяет знания из разных разделов курса только при наводящих вопросах

преподавателя. Ситуационная задача решена не полностью, или содержатся незначительные ошибки в расчетах.

«Неудовлетворительно» выставляется обучающемуся, который не знает большей части основного содержания учебной программы дисциплины в рамках компетенций, допускает грубые ошибки в формулировках основных понятий дисциплины и не умеет использовать полученные знания при решении типовых практических задач. Не раскрыты глубина и полнота при ответах. Задача не решена даже при помощи преподавателя.

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

Контрольные задания для проведения текущего контроля 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 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 вопросов к экзамену для проведения промежуточного контроля по дисциплине в 5 семестре

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.

Примерный перечень заданий для проведения промежуточного контроля по дисциплине в 6 семестре

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.

8. Установка и настройка незнакомого антивирусного программного пакета или известного за ограниченное время.

9. Нахождение зашифрованных файлов с помощью программы PGP и их расшифровка.

10. Расшифровка сообщения путем подбора ручных симметричных способов шифрования.

11. Разработка и настройка параметров парольной защиты для повышения защищенности от попыток его дискредитации в условной организации.

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.

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 проблемные вопросы.

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. 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.

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 5-6 семестров). 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 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. Экза-

мен предполагает ответы на 3 вопроса из перечня вопросов, вынесенных на промежуточную аттестацию (п. 9.6).

Рабочая программа дисциплины разработана в соответствии с требованиями
ФГОС ВО по направлению подготовки 25.03.03 «Аэронавигация».

Программа рассмотрена и утверждена на заседании кафедры № 27
«Безопасность жизнедеятельности» 20 04 2021 года, протокол № 5.

Разработчики:

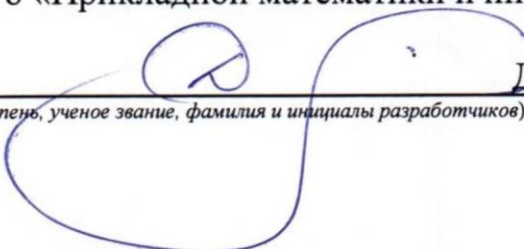
к.н., доцент


(ученая степень, ученое звание, фамилия и инициалы разработчиков)

Самойлов В. А.

Заведующий кафедрой № 8 «Прикладной математики и информатики»

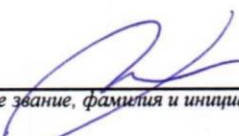
к.н., доцент


(ученая степень, ученое звание, фамилия и инициалы разработчиков)

Далингер Я. М.

Программа согласована:
Руководитель ОПОП

д.т.н., профессор


(ученая степень, ученое звание, фамилия и инициалы разработчиков)

Балясников В.В.

Программа одобрена на заседании Учебно-методического совета
Университета «16» 06 2021 года, протокол № 7.