ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА (РОСАВИАЦИЯ)

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

УТВЕРЖДАЮ

Ректор

_____ / Ю.Ю. Михальчевский

«21» октября 2021 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Обеспечение информационной безопасности

Направление подготовки
25.03.03 Аэронавигация

Направленность программы (профиль)
Техническая эксплуатация автоматизированных систем управления воздушным движением

Квалификация выпускника
бакалавр

Форма обучения
очная

Санкт-Петербург
2021

1 Цели освоения дисциплины

Цель освоения дисциплины «Обеспечение информационной безопасности»: формирование компетенций для успешной профессиональной деятельности выпускника в области построения и эксплуатации сложных организационных и технических систем автоматизированного управления.

Задачами освоения дисциплины являются:

− знакомство с принципами построения и практической реализации информационно-управляющих систем;

− изучение организации совместного решения задач Приложений, планирования и управления вычислительными процессами под управлением операционной системы, планирования и управления вычислительными процессами на уровне компьютерной сети;

− формирование умения исследования функциональной, логической и технической организации информационно-управляющих систем;

− формирование навыка использования математических методов и алгоритмов исследования информационно-управляющих систем. автоматизированных систем управления воздушным движением.

Дисциплина обеспечивает подготовку выпускника к решению задач профессиональной деятельности эксплуатационно-технологического типа.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Обеспечение информационной безопасности» представляет собой дисциплину, относящуюся к обязательной части Блока 1 «Дисциплины (модули)» ОПОП ВО по направлению подготовки 25.03.03 «Аэронавигация» (бакалавриат), профиль «Техническая эксплуатация автоматизированных систем управления воздушным движением».

Дисциплина «Обеспечение информационной безопасности» базируется на результатах обучения, полученных при изучении дисциплин: Информатика, Электротехника и электроника, Операционные системы и сети электронно-вычислительных машин.

Дисциплина «Обеспечение информационной безопасности» является обеспечивающей для дисциплин: Микропроцессорные системы автоматизированных систем управления воздушным движением, Средства передачи информации.

Дисциплина изучается в 6 семестре.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс освоения дисциплины «Обеспечение информационной безопасности» направлен на формирование следующих компетенций:

Код компетенции/ индикатора	Результат обучения: наименование компетенции, индикатора компетенции

Код компетенции/ индикатора	Результат обучения: наименование компетенции, индикатора компетенции
ОПК-1	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
$ИД^{1}_{ОПК-1}$	Ориентируется в пакетах прикладных программ, работает со стандартными программными средствами.
$ИД^{2}_{ОПК-1}$	Выбирает и использует стандартные программные средства для решения поставленных задач, в том числе 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
$ИД^{1}_{ОПК-2}$	Применяет современные библиотечно-информационные технологии для поиска, сбора и анализа информации, необходимой для решения типовых задач, в том числе в профессиональной сфере
$ИД^{2}_{ОПК-2}$	Соблюдает требования информационной безопасности при сборе и интерпретации данных с применением информационно-коммуникационных технологий в процессе решения типовых задач, в том числе в профессиональной сфере
ОПК-4	Способен использовать нормативные правовые акты в профессиональной деятельности
$ИД^{1}_{ОПК-4}$	Ориентируется в условиях постоянного изменения правовой базы, содержащей нормативные правовые документы в сфере профессиональной деятельности
$ИД^{2}_{ОПК-4}$	Соблюдает требования нормативных правовых документов при осуществлении профессиональной деятельности

Планируемые результаты изучения дисциплины:

Знать:

– основные техносферные опасности, их свойства и характеристики;

– основные нормативные и правовые акты в области ИБ;

– основные определения и составляющие ИБ;

– методы сбора, хранения и обработки информации, применяемые в профессиональной деятельности;

– основные методы защиты процессов получения, хранения и переработки информации;

– государственные и международные стандарты, иные нормативные документы, касающиеся обеспечения информационной безопасности в своей профессиональной деятельности;

– основные результаты при выполнении технико-технологических, организационных и управленческих мероприятий и решений в области ИБ;

– структуру локальных и глобальных компьютерных сетей;

– основные виды атак на компьютерные системы;

– основные средства и методы защиты компьютерных сетей;

– основные программные средства защиты информации при работе на ПК и в сети интернет и их характеристики;

Уметь:

– соблюдать основные требования ИБ, в том числе защиты государственной тайны;

– использовать внешние носители информации для обмена данными между машинами;

– создавать резервные копии, архивы данных и программ;

– выполнять постановку задач, связанных с обеспечением информационной безопасности в своей профессиональной деятельности;

– оценивать эффективность основных результатов при выполнении технико-технологических, организационных и управленческих мероприятий и решений в области ИБ;

– использовать средства защиты информации при работе в сети интернет;

– использовать средства анализа защищенности ПК и способы устранения уязвимостей;

– соблюдать основные требования ИБ, в том числе защиты государственной тайны;

– использовать внешние носители информации для обмена данными между машинами;

– создавать резервные копии, архивы данных и программ;

– выполнять постановку задач, связанных с обеспечением информационной безопасности в своей профессиональной деятельности;

– оценивать эффективность основных результатов при выполнении технико-технологических, организационных и управленческих мероприятий и решений в области ИБ;

– использовать средства защиты информации при работе в сети интернет;

– использовать средства анализа защищенности ПК и способы устранения уязвимостей;

Владеть:

– техническими и программными средствами защиты информации при работе с компьютерными системами, включая приемы антивирусной защиты;

– средствами криптографической защиты информации;

– методами исследования и решения типовых задач информационной безопасности;

– основными навыками анализа эффективности принимаемых решений в области ИБ;

– методами поиска и обмена информацией в глобальных и локальных компьютерных сетях;

– навыками поиска уязвимостей ПК с помощью специальных программных средств и их устранения;

4 Объем дисциплины и виды учебной работы

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

Наименование	Всего часов	Семестр
		6
Общая трудоемкость дисциплины	144	144
Контактная работа:	56,5	56,5
лекции	18	18
практические занятия	32	32
семинары	–	–
лабораторные работы	–	–
курсовой проект (работа)	4	4
Самостоятельная работа студента	54	54
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

Темы дисциплины	Количество часов	Компетенции			Образовательные технологии	Оценочные средства
		ОПК-1	ОПК-2	ОПК-4		
Тема 1 Информационная безопасность деятельности общества. Организационное и правовое обеспечение информационной безопасности.	22	+	+	+	ВК, Л, ПЗ, СРС	У, Т, ПрЗ, Пр
Тема 2 Основы обеспечения информационной безопасности жизнедеятельности общества и авиационных структур.	26	+	+	+	Л, ПЗ, СРС	У, Т, ПрЗ, Пр

Темы дисциплины	Количество часов	Компетенции			Образовательные технологии	Оценочные средства
		ОПК-1	ОПК-2	ОПК-4		
Тема 3 Основы технического обеспечения информационной безопасности в АСУВД.	32	+	+	+	Л, ПЗ, СРС	У, Т, ПрЗ, Пр
Тема 4 Программно-аппаратные средства обеспечения информационной безопасности в АСУВД.	28	+	+	+	Л, ПЗ, СРС	У, Т, ПрЗ, Пр
Итого за 6 семестр	108					
Промежуточная аттестация	36					
Итого по дисциплине	144					

Сокращения: Л – лекция, ПЗ – практическое занятие, ПрЗ – практическое задание; СРС – самостоятельная работа студента, ВК – входной контроль, Пр – проект, У − устный опрос, Т – тест.

5.2 Темы (разделы) дисциплины и виды занятий

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
Тема 1 Информационная безопасность деятельности общества. Организационное и правовое обеспечение информационной безопасности.	4	8			10		22
Тема 2 Основы обеспечения информационной безопасности жизнедеятельности общества и авиационных структур.	4	8			14		26
Тема 3 Основы технического обеспечения информационной безопасности в АСУВД.	6	8			14	4	32
Тема 4 Программно-аппаратные средства обеспечения информационной безопасности в АСУВД.	4	8			16		28
Итого за … семестр	18	32	–	–	54	4	108

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
Промежуточная аттестация							36
Итого по дисциплине							144

Сокращения: Л – лекции, ПЗ – практические занятия, С – семинары, ЛР – лабораторные работы, СРС – самостоятельная работа студента, КР – курсовая 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 информационной безопасности жизнедеятельности общества и авиационных структур.

Информационное противоборство. Ее психологическая и техническая составляющие. Угрозы информационной безопасности на предприятиях авиационного транспорта. 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 информационной безопасности в АСУВД.

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

Тема 4 Программно-аппаратные средства обеспечения информационной безопасности в АСУВД.

Обеспечение сохранности данных и защита ПЭВМ в АС. Информационная безопасность систем управления базами данных. Политика безопасности в АСУВД. 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.

5.4 Практические занятия

Номер темы дисциплины	Тематика практических занятий	Трудоемкость (часы)
1	ПЗ 1. (Тема 1). Устный опрос. Стандарты информационной безопасности.	2
1	ПЗ 2. (Тема 1). Тест 1. Информационное противоборство.	2
1	ПЗ 3. (Тема 1). Дискуссия. Угрозы информационной безопасности.	2
2	ПЗ 4. (Тема 2). Устный опрос. Построение систем защиты от угроз нарушения информации.	2
2	ПЗ 5. (Тема 2). Устный опрос. Криптографические методы защиты информации.	2
2	ПЗ 6. (Тема 2). Дискуссия. Уязвимости компьютеров и компьютерных сетей.	2
3	ПЗ 7. (Тема 3). Устный опрос. Основные виды атак на компьютерные системы.	2
3	ПЗ 8. (Тема 3). Устный опрос. Сетевые средства экранирования.	2
3	ПЗ 9. (Тема 3). Дискуссия. Системы анализа защищенности	2
4	ПЗ 10. (Тема 4). Устный опрос. Системы обнаружения и предотвращения вторжений.	2
4	ПЗ 11. (Тема 4). Устный опрос. Информационная безопасность систем управления базами данных.	2
4	ПЗ 12. (Тема 4). Устный опрос. Политика безопасности.	4
4	ПЗ 13. (Тема 4). Тест 2. Политика безопасности.	4
4	ПЗ 14. (Тема 4). Практическое задание. СКЗИ Secret Net и Сфера.	2
Итого по дисциплине		32

5.5 Лабораторный практикум

Лабораторный практикум учебным планом не предусмотрен.

5.6 Самостоятельная работа

Номер темы дисци-плины	Виды самостоятельной работы	Трудо-емкость (часы)
1	Изучение теоретического материала и подготовка к практическим занятиям 1-3. Подготовка к устному опросу, дискуссии, практическому заданию [1, 8, 10-12].	12
2	Изучение теоретического материала и подготовка к практическим занятиям 4-6. . Подготовка к устному опросу, дискуссии, практическому заданию [2, 12]	14
3	Изучение теоретического материала и подготовка к практическим занятиям 7-9. . Подготовка к устному опросу, дискуссии, практическому заданию [2, 4, 8, 13]	14
4	Изучение теоретического материала и подготовка к практическим занятиям 10-14. Подготовка к устному опросу, дискуссии, практическому заданию [2, 4, 8, 13]	14
Итого по дисциплине		54

5.7 Курсовые работы

Наименование этапа выполнения курсовой работы (проекта)	Трудоемкость (часы)
Выдача задания на курсовую работу	2
Защита курсовой работы	2
Итого за семестр:	4

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. : Изда-

тельство Юрайт, 2017. — 325 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8 — Режим доступа: https://urait.ru/viewer/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-413158.

3 Суворова, Г. М. **Информационная безопасность** [Электронный ресурс]: учебное пособие для вузов / Суворова, Г. М. — М. : Издательство Юрайт, 2021. — 253 с. — (Серия : Высшее образование). — ISBN 978-5-534-13960-0 — Режим доступа: https://urait.ru/viewer/informacionnaya-bezopasnost-467370.

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://urait.ru/viewer/zaschita-informacii-osnovy-teorii-413854.

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://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-413316.

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: 15.05.2021).

8 **Система поиска Google**[Электронный ресурс]. – Режим доступа:www.google.com, свободный (дата обращения: 15.05.2021).

9 **Электронная библиотека** [Электронный ресурс]. – Режим доступа:www.wikipedia.org, свободный (дата обращения: 15.05.2021).

10 **Онлайн переводчик** [Электронный ресурс]. – Режим доступа:www.lingvo.ru. , свободный (дата обращения15.05.2021).

11 **InformationSecurity/Информационная безопасность** [Электронный ресурс]: официальный сайтжурнала «InformationSecurity/Информационная безопасность» – Режим доступа:www.itsec.ru, свободный (дата обращения: 15.05.2021).

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: 15.05.2021).

13 **Федеральная служба по техническому и экспортному контролю (ФСТЭК России)** [Электронный ресурс]: официальный сайтФСТЭК РФ.– Режим доступаhttps://fstec.ru/свободный (дата обращения: 15.05.2021).

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: 15.05.2021);

15 **Электронно-библиотечная система издательства «Юрайт»** [Электронный ресурс] — Режим доступа: https://urait.ru/;

16 **Scilab** [Программное обеспечение] — Режим доступа: https://www.scilab.org/- свободный (дата обращения: 15.05.2021).

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

7 Материально-техническое обеспечение дисциплины

Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3
Обеспечение информационной безопасности	Лабораторная аудитория №804 Компьютерные столы - 10 шт., стулья - 10 шт., 10 персональных компьютеров, с доступом в сеть Интернет, учебная доска. Комплект презентационных материалов. Microsoft Windows, Microsoft Office, Oracle VirtualBox, Scilab.	196210, г. Санкт-Петербург, ул. Пилотов, дом 38, лит. А

8 Образовательные и информационные технологии

В рамках изучения дисциплины предполагается использовать следующие образовательные технологии.

Входной контроль проводится преподавателем в начале изучения дисциплины с целью коррекции процесса усвоения обучающимися дидактических единиц при изучении базовых дисциплин.

Лекция составляет основу теоретического обучения в рамках дисциплины и направлена на систематизированное изложение накопленных и актуальных научных знаний. Лекция предназначена для раскрытия состояния и перспектив развития экономических знаний в современных условиях. На лекции концентрируется внимание обучающихся на наиболее сложных и узловых вопросах, стимулируется их активная познавательная деятельность.

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

При изучении дисциплины используются как традиционные лекции, так и интерактивные лекции. Интерактивные лекции проводятся в форме проблемных лекций, главная цель которых – приобретение знаний студентами при непосредственном действенном их участии. На проблемных лекциях процесс познания студентов в сотрудничестве и диалоге с преподавателем и друг с другом приближается к исследовательской деятельности. Содержание проблемы раскрывается путем организации поиска ее решения или суммирования и анализа традиционных и современных точек зрения. Основными этапами познавательной деятельности студентов в процессе проблемной лекции являются:
а) осознание проблемы; б) выдвижение гипотез, предложения по решению проблемы; в) обсуждение вариантов решения проблемы; г) проверка решения.

Цель практических занятий – закрепить теоретические знания, полученные обучающимися на лекциях и в результате самостоятельного изучения соответствующих тем, а также приобрести начальные практические навыки. Рассматриваемые в рамках практического занятия задачи, ситуации, примеры и проблемы имеют профессиональную направленность и содержат элементы, необходимые для формирования компетенций в рамках подготовки обучающихся. Практические занятия предусматривают участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практические занятия проводятся в аудиторной и интерактивной форме.

Самостоятельная работа обучающихся является составной частью учебной работы. Ее основной целью является формирование навыка самостоятельного приобретения знаний по некоторым вопросам теоретического курса, закрепление и углубление полученных знаний, самостоятельная работа со справочниками, периодическими изданиями и научно-популярной литературой. Самостоятельная работа включает выполнение учебных заданий, в том числе и индивидуальных, а также работу над курсовым проектом.

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

Уровень и качество знаний обучающихся оцениваются по результатам текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины.

Устный опрос проводится на практических занятиях с целью контроля усвоения теоретического материала, излагаемого на лекциях.

Тест проводится по темам в соответствии с данной программой и предназначен для проверки обучающихся на предмет освоения материала лекций.

Дискуссия, являясь одной из наиболее эффективных технологий группового взаимодействия, усиливает развивающие и воспитательные эффекты обучения, создает условия для открытого выражения участниками своих мыслей, позиций, обладает возможностью воздействия на установки ее участников. Принципами организации дискуссии являются содействие возникновению альтернативных мнений, путей решения проблемы, конструктивность критики, обеспечение психологической защищенности участников.

Практические задания выдаются студентам на практических занятиях и предназначены для закрепления теоретических знаний, а также для отработки умений и навыков. Как правило, они подразумевают проработку теоретического материала предыдущих лекций и последующее выполнение определенной последовательности действий на компьютере. При проверке преподавателем правильности выполнения задания студент также должен показать знание соответствующего теоретического материала.

Защита лабораторных работ подразумевает устный опрос студента по основным теоретическим сведениям, необходимым для выполнения работы, методике ее выполнения, полученным при этом результатам и их интерпретации

Промежуточная аттестация по итогам освоения дисциплины проводится в виде экзамена в 6 семестре. К моменту сдачи экзамена должны быть успешно пройдены предыдущие формы контроля.

Экзамен позволяют оценить уровень освоения компетенций за весь период изучения дисциплины. Билет включает два теоретических вопроса и задачу.

9.1 Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов по дисциплине

Не применяется.

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

Решение практических заданий оценивается:

«зачтено»: обучающийся самостоятельно правильно решает задачу, дает обоснованную оценку по итогу решения;

«не зачтено»: обучающийся отказывается от выполнения задачи или не способен ее решить самостоятельно, а также с помощью преподавателя.

Устный опрос:

«зачтено»: зачитывается в том случае, если получены достаточно полные и аргументированные ответы на вопросы преподавателя;

«не зачтено»: не зачитывается в том случае, если обучающийся не смог ответить на вопросы или ответил правильно менее чем на 61% вопросов.

Тест оценивается на «отлично», если количество правильных ответов 90% и более; «хорошо» – от 76% до 89%; «удовлетворительно» – от 61% лр 75%; «неудовлетворительно» – менее 61%.

9.3 Темы курсовых работ (проектов) по дисциплине

1. Обзор и сравнительный анализ стандартов информационной безопасности.
2. Антивирусная защита в АС.
3. Электронная цифровая подпись.
4. Алгоритмические основы криптографических систем.
5. Сетевые средства экранирования в АС.
6. Комплексные системы защиты от вторжений.
7. Информационная безопасность систем управления базами данных.
8. Политика безопасности в АС.
9. Защита информации от утечки по техническим каналам.
10. Аудит информационной безопасности.

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

11. Состав и типы компьютеров. Программное и аппаратное обеспечение персонального компьютера. Системы счисления.
12. Процессор. Память. Устройства ввода/вывода.
13. Локальные и глобальные компьютерные сети.
14. Операционная система MS Windows. Управление системой файлов.
15. Состав и назначение пакета MS Offis. Подготовка документов в MS Word.Обработка данных в MS Excel.
16. Виды программ, алгоритмы. Свойства алгоритма. Способы записи алгоритма.
17. Интегрированная среда Visual Basic. Формы, элементы управления, меню. Алфавит языка. Константы, переменные. Стандартные типы данных. Стандартные функции. Линейная структура программы: ввод, вычисление, вывод. Операторы.
18. Условный оператор if. Логические выражения. Операторы цикла. Вложенные циклы.

19. Понятие массива. Объявление массивов. Динамические массивы. Элементы массива, индексы. Методы инициализации массивов.
20. 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: - основные техносферные опасности, их свойства и характеристики; - основные нормативные и правовые акты в области ИБ; - основные определения и составляющие ИБ; Уметь: – соблюдать основные требования ИБ, в том числе защиты государственной тайны;
	$ИД^{2}_{ОПК-1}$	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;
ОПК-2	$ИД^{1}_{ОПК-2}$	*Знать*: – Государственные и международные стандарты, иные нормативные документы, касающиеся обеспечения информационной безопасности в своей профессиональной деятельности; *Уметь*: – Выполнять постановку задач, связанных с обеспечением информационной безопасности в своей профессиональной деятельности;

Компетенции	Показатели оценивания (индикаторы достижения) компетенций	Критерии оценивания
	$ИД^{2}_{ОПК-2}$	Знать: - основные результаты при выполнении технико-технологических, организационных и управленческих мероприятий и решений в области ИБ; Уметь: - оценивать эффективность основных результатов при выполнении технико-технологических, организационных и управленческих мероприятий и решений в области ИБ;
ОПК-4	$ИД^{1}_{ОПК-4}$	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;
	$ИД^{2}_{ОПК-4}$	Знать: - основные программные средства защиты информации при работе на ПК и в сети интернет и их характеристики. Уметь: - использовать средства анализа защищенности ПК и способы устранения уязвимостей.
II этап		
ОПК-1	$ИД^{1}_{ОПК-1}$	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.

Компетенции	Показатели оценивания (индикаторы достижения) компетенций	Критерии оценивания
	$ИД^{2}_{ОПК-1}$	Уметь: - использовать внешние носители информации для обмена данными между машинами; - создавать резервные копии, архивы данных и программ; Владеть: - средствами криптографической защиты информации.
ОПК-2	$ИД^{1}_{ОПК-2}$	*Уметь*: – Выполнять постановку задач, связанных с обеспечением информационной безопасности в своей профессиональной деятельности; *Владеть*: – Методами исследования и решения типовых задач информационной безопасности
	$ИД^{2}_{ОПК-2}$	Уметь: - оценивать эффективность основных результатов при выполнении технико-технологических, организационных и управленческих мероприятий и решений в области ИБ; Владеть: - основными навыками анализа эффективности принимаемых решений в области ИБ.
ОПК-4	$ИД^{1}_{ОПК-4}$	Уметь: - использовать средства защиты информации при работе в сети интернет; Владеть: - методами поиска и обмена информацией в глобальных и локальных компьютерных сетях.
	$ИД^{2}_{ОПК-4}$	Уметь: - использовать средства анализа защищенности ПК и способы устранения уязвимостей. Владеть: - навыками поиска уязвимостей ПК с помощью специальных программных средств и их устранения.

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» в*ыставляется 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

9.6.1 Примерные контрольные задания для проведения текущего контроля успеваемости

Типовые вопросы для 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.
10. Способы определения программных закладок.

Типовые тестовые задания

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
* Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Основными источниками угроз информационной безопасности являются
- Хищение жестких дисков, подключение к сети, инсайдерство
* Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. Виды информационной безопасности:
* Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4. Цели информационной безопасности – своевременное обнаружение, предупреждение:
* несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5. Основные объекты информационной безопасности:
* Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6. Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
* Потеря, искажение, утечка информации

9.6.2 Контрольные вопросы промежуточной аттестации по итогам освоения дисциплины

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

Типовые практические задания для промежуточной аттестации в форме экзамена

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 пакетаили 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

Методика преподавания дисциплины характеризуется совокупностью методов, приемов и средств обучения, обеспечивающих реализацию содержания и учебно-воспитательных целей дисциплины, которая может быть представлена как некоторая методическая система, включающая методы, приемы и средства обучения. Такой подход позволяет более качественно подойти к вопросу освоения дисциплины обучающимися.

Учебные занятия начинаются и заканчиваются по времени в соответствии с утвержденным режимом СПб ГУГА в аудиториях согласно семестровым расписаниям теоретических занятий. На занятиях, предусмотренных расписанием, обязаны присутствовать все обучающиеся.

Лекции являются одним из важнейших видов учебных занятий и составляют основу теоретической подготовки обучающихся по дисциплинам. Лекция имеет целью дать систематизированные основы научных знаний по дисциплине, раскрыть состояние и перспективы прогресса конкретной области науки и экономики, сконцентрировать внимание на наиболее сложных и узловых вопросах. Эта цель определяет дидактическое назначение лекции, которое заключается в том, чтобы ознакомить обучающихся с основным содержанием, категориями, принципами и закономерностями изучаемой темы и предмета обучения в целом, его главными идеями и направлениями развития. Именно на лекции формируется научное мировоззрение обучающегося, закладываются теоретические основы фундаментальных знаний будущего управленца, стимулируется его активная познавательная деятельность, решается целый ряд вопросов воспитательного характера.

Каждая лекция должна представлять собой устное изложение лектором основных теоретических положений изучаемой дисциплины или отдельной темы как логически законченное целое и иметь конкретную целевую установку. Особое место в лекционном курсе по дисциплине занимают вводная и заключительная лекции.

Вводная лекция должна давать общую характеристику изучаемой дисциплины, подчеркивать новизну проблем, указывать ее роль и место в системе изучения других дисциплин, раскрывать учебные и воспитательные цели и кратко знакомить обучающихся с содержанием и структурой курса, а также с организацией учебной работы по нему. Заключительная лекция должна давать научно-практическое обобщение изученной дисциплины, показывать перспективы развития изучаемой области знаний, навыков и практических умений.

Практические занятия проводятся в целях выработки практических умений и приобретения навыков при решении управленческих задач. Основным содержанием этих занятий является практическая работа каждого обучающегося. Назначение практических занятий – закрепление, углубление и

комплексное применение на практике теоретических знаний, выработка умений и навыков обучающихся в решении практических задач. Вместе с тем, на этих занятиях, осуществляется активное формирование и развитие навыков и качеств, необходимых для последующей профессиональной деятельности. Практические занятия проводятся по наиболее сложным вопросам дисциплины и имеют целью углубленно изучить ее содержание, привить обучающимся навыки самостоятельного поиска и анализа информации, умение делать обоснованные выводы, аргументировано излагать и отстаивать свое мнение. Каждое практическое занятие заканчивается, как правило, кратким подведением итогов, указаниями преподавателя о последующей самостоятельной работе.

Промежуточная аттестация по итогам освоения дисциплины проводится в виде экзамена в 6 семестре. К моменту сдачи экзамена должны быть успешно пройдены предыдущие формы контроля. Экзамен позволяют оценить уровень освоения компетенций за весь период изучения дисциплины.

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

Программа рассмотрена и утверждена на заседании кафедры № 8 «Прикладной математики и информатики»
«15» сентября 2021 года, протокол № 2 .

Разработчик:

к.т.н. Земсков Ю.В.

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

Заведующий кафедрой № 8 «Прикладной математики и информатики»

д.т.н., доцент Костин Г.А.

(ученая степень, ученое звание, фамилия и инициалы заведующего кафедрой)

Программа согласована:
Руководитель ОПОП ВО
д.т.н., доцент Костин Г.А.

(ученая степень, ученое звание, фамилия и инициалы руководителя ОПОП)

Программа рассмотрена и одобрена на заседании Учебно-методического совета Университета «20» октября 2021 года, протокол № 2.