ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА (РОСАВИАЦИЯ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕУЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА»

УТВЕРЖДАЮ

Ректор

_____ Ю.Ю. Михальчевский

«___» _____ 2023 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки
25.04.03 Аэронавигация

Направленность программы (профиль)
Государственное регулирование деятельности в области гражданской авиации

Квалификация выпускника
магистр

Форма обучения
заочная

Санкт-Петербург
2023

1 Цели освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Повышение безопасности в транспортных системах всегда было одной из важнейших задач. Актуально это и для системы воздушного транспорта, что подтверждается развитием событий в последнее время.

Направления, по которым проводится планомерная работа по повышению уровня авиационной безопасности, охватывают огромный круг вопросов – от совершенствования правовой и нормативной базы, до конкретных мер, в том числе совершенствование информационной поддержки системы и внедрения современных технических средств.

В задачу дисциплины входит познакомить студентов с современным состоянием обеспечения различных направлений информационной безопасности.

Задачами освоения дисциплины являются:

– освоение базовой терминологии, использующейся в сфере обеспечения информационной безопасности;

– освоение нормативно-правовой базы по обеспечению информационной безопасности;

– формирование знаний о структуре и основных требованиях стандартов, в сфере информационной безопасности;

– формирование представлений о механизмах формирования политики информационной безопасности.

Дисциплина обеспечивает подготовку обучающегося к решению задач профессиональной деятельности организационно-управленческого, научно-исследовательского типа.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность» представляет собой дисциплину, относящуюся к обязательной части Блока 1 Дисциплины (модули).

Дисциплина «Информационная безопасность» базируется на результатах обучения, полученных при изучении дисциплины: «Управление транспортной безопасностью».

Дисциплина «Информационная безопасность» является обеспечивающей для дисциплины «Управление безопасностью полетов», а также для Подготовки к процедуре защиты и защиты выпускной квалификационной работы.

Дисциплина изучается во 2 семестре.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс освоения дисциплины направлен на формирование следующих компетенций:

Код компетенции/ индикатора	Результат обучения: наименование компетенции, индикатора компетенции
ОПК-10	Способен к выявлению и анализу опасностей и угроз, возникающих в процессе развития современного информационного общества
ОПК-10.1	Прогнозирует эффективность функционирования систем обеспечения безопасности, оценивая затраты и риски
ОПК-10.2	Анализирует угрозы обеспечения безопасности объектов и разрабатывает методы противодействия им
ОПК-10.3	Осуществляет построение как отдельных процессов управления информационной безопасностью, так и системы процессов в целом
ОПК-11	Способен организовывать и обеспечивать соблюдение основных требований информационной безопасности, в том числе защиту охраняемой законом тайны
ОПК-11.1	Анализирует направления развития информационно-коммуникационных технологий объекта защит
ОПК-11.2	Анализирует текущее состояние информационной безопасности на предприятии с целью разработки требований к разрабатываемым процессам управления информационной безопасностью
ОПК-11.3	Применяет процессный подход к управлению информационной безопасностью в сферах деятельности области аэронавигации

Планируемые результаты изучения дисциплины:

Знать:

– основные пути и методы решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта;

– требования нормативно-правовой базы в области обеспечения информационной безопасности на предприятиях гражданской авиации;

– основные возможности и характеристики программных средств обеспечения защиты информации.

Уметь:

– определять «узкие» места в системе обеспечения информационной безопасности, и предлагать пути их устранения;

– грамотно эксплуатировать программные средства информационной безопасности.

Владеть:

– методикой разработки и внедрения систем информационной безопасности в структурных подразделениях системы воздушного транспорта;

– программными средствами защиты информации при работе с компьютерными системами, включая приёмы антивирусной защиты.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетных единицы 72 академических часа.

Наименование	Всего часов	Семестр
		2
Общая трудоемкость дисциплины	72	72
Контактная работа	8,3	8,3
лекции,	4	4
практические занятия,	4	4
семинары,		
лабораторные работы,		
курсовой проект (работа)		
другие виды аудиторных занятий.		
Самостоятельная работа студента	55	55
Контрольные работы		
в том числе контактная работа		
Промежуточная аттестация	9	9
контактная работа	0,3	0,3
самостоятельная работа по подготовке к зачету	8,7 Зачет	8,7 Зачет

5 Содержание дисциплины

5.1 Соотнесения тем (разделов) дисциплины и формируемых компетенций

Темы, разделы дисциплины	Количество часов	ОПК-10.1	ОПК-10.2	ОПК-10.3	ОПК-11.1	ОПК-11.2	ОПК-11.3	Образовательные технологии	Оценочные средства
Тема 1. Общие понятия об информационной безопасности.	11.5	+	+					ВК, Л, СРС	У
Тема 2. Уровни обеспечения Информационной безопасности	10,5		+		+	+	+	ПЗ, СРС	У
Тема 3. Угрозы информационной безопасности.	11,5	+		+		+		Л, СРС	У
Тема .4. Таксономия критериев информационной безопасности.	9,5		+				+	СРС	У
Тема 5. Противодействие несанкционированному межсетевому доступу.	9,5		+	+	+			СРС	У
Тема 6. Вредоносное программное обеспечение. Средства борьбы с вредоносным ПО	10,5		+	+			+	ПЗ, СРС	У
Промежуточная аттестация	9	+	+	+	+	+	+	СРС	Зачет
Итого по дисциплине	72								

Сокращения: Л − лекция, ПЗ – практические занятия, СРС − самостоятельная работа студента, ВК − входной контроль, У − устный опрос.

5.2 Темы (разделы) дисциплины и виды занятий

Наименование раздела дисциплины	Л	ПЗ	СРС	Всего часов
Тема 1. Общие понятия об информационной безопасности.	2		9,5	11.5
Тема 2. Уровни обеспечения Информационной безопасности		2	8,5	10,5
Тема 3. Угрозы информационной безопасности.	2		9,5	11,5
Тема .4. Таксономия критериев информационной безопасности.			9,5	9,5
Тема 5. Противодействие несанкционированному межсетевому доступу.			9,5	9,5
Тема 6. Вредоносное программное обеспечение. Средства борьбы с вредоносным ПО		2	8,5	10,5
ИТОГО :	4	4	55	63
ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ:				9
ВСЕГО ПО ДИСЦИПЛИНЕ:				72

5.3 Содержание дисциплины

Тема 1. Общие понятия об информационной безопасности.

Значение информационной безопасности компьютерных систем для стабильного функционирования предприятий и организаций системы воздушного транспорта. Определение понятия «информационная безопасность», практические аспекты информационной безопасности.

Тема 2. Уровни обеспечения Информационной безопасности

Законодательный, административный, процедурный и программно-технический уровни обеспечения информационной безопасности. Политика информационной безопасности предприятия.

Тема 3. Угрозы информационной безопасности

Классификация и анализ угроз информационной безопасности компьютерных систем. Оценка угроз информационной безопасности.

Тема 4. Таксономия критериев информационной безопасности

«Оранжевая книга», её значение и содержание. Механизмы создания и поддержания надежной вычислительной базы.

Тема 5. Противодействие несанкционированному межсетевому доступу

Эталонная модель взаимодействия открытых систем: её назначение и функционирование. Комплексный межсетевой экран, состав, назначение составляющих элементов.

Тема 6. Вредоносное программное обеспечение. Средства борьбы с вредоносным программным обеспечением

Классификация вредоносного программного обеспечения. Компьютерные вирусы, троянские программы, сетевые компьютерные черви, и другое вредоносное программное обеспечение. Классификация средств борьбы с вредоносным программным обеспечением.

5.4 Практические занятия (семинары)

Номер темы дисциплины	Тематика практических занятий (семинаров)	Трудо-емкость (часы)
2	Уровни обеспечения Информационной безопасности	2
6	Вредоносное программное обеспечение. Средства борьбы с вредоносным ПО	2
Итого по дисциплине		4

5.5 Лабораторный практикум

Лабораторный практикум учебным планом не предусмотрен.

5.6 Самостоятельная работа

Номер темы дисциплины	Виды самостоятельной работы	Трудо-емкость (часы)
1	Самостоятельное овладение студентами материала темы. [4]	9,5
2	Самостоятельное овладение студентами материала темы [2, 5] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя	8,5
3	Самостоятельное овладение студентами материала темы [1,2,3] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя	9,5
4	Самостоятельное овладение студентами материала темы [3]	9,5

Номер темы дисциплины	Виды самостоятельной работы	Трудо-емкость (часы)
	Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя	
5	Самостоятельное овладение студентами материала темы [2,4] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя	9,5
6	Самостоятельное овладение студентами материала темы [1,3] Выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя	8,5
Всего:		55

6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) основная литература:

1. Ерохин В.В. Безопасность информационных систем [Электронный ресурс] : учебное пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. — Электрон. дан. — Москва : ФЛИНТА, 2015. — 182 с. — Режим доступа: https://e.lanbook.com/book/62972

2. Заляжных В.А. Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем [Электронный ресурс] : учебно-методическое пособие / В.А. Заляжных, А.В. Гирик. — Электрон. дан. — Санкт-Петербург : НИУ ИТМО, 2014. — 136 с. — Режим доступа: https://e.lanbook.com/book/71193.

б) дополнительная литература:

3. Бондарев В.В. Введение в информационную безопасность автоматизированных систем [Электронный ресурс] : методические указания / В.В. Бондарев. — Электрон. дан. — Москва: МГТУ им. Н.Э. Баумана, 2016. — 250 с. — Режим доступа: https://e.lanbook.com/book/103554.

4. Мельников Д.А. Информационная безопасность открытых систем [Электронный ресурс] : учебник / Д.А. Мельников. — Электрон. дан. — Москва : ФЛИНТА, 2014. — 448 с. — Режим доступа: https://e.lanbook.com/book/48368.

5. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]: учебно-методическое пособие / П.Н. Девянин. — Электрон. дан. — Москва: Горячая линия-Телеком, 2012. — 320 с. — Режим доступа: https://e.lanbook.com/book/5150.

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

https://www.intuit.ru/studies/courses/10/10/lecture/296?page=1
https://www.intuit.ru/studies/courses/10/10/lecture/302
https://www.intuit.ru/studies/courses/3649/891/lecture/32336?page=1
https://www.intuit.ru/studies/courses/10/10/lecture/306
https://www.intuit.ru/studies/courses/10/10/lecture/310
https://www.intuit.ru/studies/courses/10/10/lecture/312
https://www.intuit.ru/studies/courses/10/10/lecture/300
https://studref.com/325272/informatika/klassifikatsiya_ugroz_informatsionnoy_bezopasnosti#846
http://protect.htmlweb.ru/orange1.htm
https://studfiles.net/preview/3103252/page:8/
https://www.kazedu.kz/referat/84974/4
https://www.kazedu.kz/referat/84974/5
https://www.kazedu.kz/referat/84974/8
https://ocompah.ru/razlichie-mezhdu-kompyuternyj-virus-cherv-troyanskij-kon.html
http://old.intuit.ru/department/security/antiviruskasp/2/
http://old.intuit.ru/department/security/antiviruskasp/2/2.html#sect3
http://old.intuit.ru/department/security/antiviruskasp/5/
http://old.intuit.ru/department/security/antiviruskasp/6/
http://old.intuit.ru/department/security/antiviruskasp/7/
https://www.itweek.ru/security/article/detail.php?ID=104405
https://studfiles.net/preview/5282711/
http://routeworld.ru/80-model-vzaimodeystviya-otkrytyh-sistem-osi.html
http://citforum.ru/nets/protocols/1_01_02.shtml
https://studfiles.net/preview/5970826/page:56/
https://studfiles.net/preview/5970826/page:57/
https://studfiles.net/preview/5970826/page:58/
https://studfiles.net/preview/5970826/page:59/
http://ypn.ru/322/osi-depended-firewall-functioning-features/
https://vuzlit.ru/986869/protivodeystvie_nesanktsionirovannomu_mezhsetevomu_dostupu

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

1. Сканер уязвимостей XSpider фирмы Positive Technologies ;
2. Комплексная система контроля защищённости MaxPatrol 8 фирмы Positive Technologies;
3. Антивирусный пакет Kaspersky Endpoint Security Standard for Windows.

7 Материально-техническое обеспечение дисциплины (модуля)

Для успешного освоения дисциплины необходимо иметь аудиторию, оборудованную:

- мультимедийными средствами;
- плакатами, стендами по тематики дисциплины (или презентации с информацией по тематики дисциплины);
- видео библиотекой (видеозаписи учений и тренировок, видеофильмы по тематике дисциплины);
- наглядные пособия, необходимые для проведения занятий по дисциплине.

8 Образовательные и информационные технологии

Входной контроль проводится в форме устных опросов с целью оценивания остаточных знаний по ранее изученным дисциплинам или разделам изучаемой дисциплины.

При изучении дисциплины используются как традиционные **лекции**, так и интерактивные лекции.

Интерактивные лекции проводятся в нескольких вариантах

-п**роблемная лекция** начинается с постановки проблемы, которую необходимо решить в процессе изложения материала.

-лекция-визуализация учит студентов преобразовывать устную и письменную информацию в визуальную форму, что формирует у них профессиональное мышление за счет систематизации и выделения наиболее значимых, существенных элементов содержания обучения.

- лекция-беседа предполагает непосредственный контакт преподавателя с аудиторией, позволяет привлечь внимание студентов к наиболее важным вопросам темы, вовлечь в двусторонний обмен мнениями, выяснить уровень их осведомленности по рассматриваемой теме, степени их готовности к восприятию последующего материала, позволяет адресовать вопрос к конкретному студенту, спросить его мнение по обсуждаемой проблеме.

-лекция-дискуссия. Преподаватель при изложении лекционного материала не только использует ответы студентов на свои вопросы, но и организует свободный обмен мнениями в интервалах между логическими разделами.

Практические занятия проводятся с использованием специальных компьютерных программ и предназначены для закрепления полученных знаний, а также выработки необходимых умений и навыков.

Интерактивное практическое занятие проводится с использование средств вычислительной техники и специального программного обеспечения, и предполагает выполнение выданных конкретных заданий.

Самостоятельная работа студента проводится с целью закрепления и совершенствования осваиваемых компетенций, предполагает сочетание самостоятельных теоретических занятий и самостоятельное выполнение практических заданий, описанных в рекомендованной литературе [1,2].

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

9.1 Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов

Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов учебным планом не предусмотрена.

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

В процессе преподавания дисциплины для текущего контроля обучающихся используются следующие формы:

- тестирование по темам;
- решение типовых ситуационных задач на практических занятиях;
- выполнение письменной аудиторной работы.

Тестирование:

Тест считается зачтенным при наличии более 60% правильных ответов. Тест считается не зачтенным при наличии менее 60% правильных ответов.

Решение ситуационных задач (критерии):

обучающийся самостоятельно правильно решает задачу, дает обоснованную оценку по итогу решения;

обучающийся отказывается от выполнения задачи, или не способен ее решить самостоятельно, а также с помощью преподавателя (в случае неподготовленности по изученным темам, имеющим отношение к решению данной задачи).

Письменная аудиторная работа (критерии):

обучающийся правильно решает задачу, сдает ее вовремя по окончании занятия преподавателю, дает обоснованную оценку по итогу решения;

обучающийся отказывается от выполнения задачи, или не способен ее решить самостоятельно, а также с помощью преподавателя (в случае неподготовленности по изученным темам, имеющим отношение к решению данной задачи).

По итогам освоения дисциплины проводится промежуточная аттестация.

Основными документами, регламентирующими порядок организации и проведения текущего контроля успеваемости и промежуточной аттестации

студентов, обучающихся в ГУГА являются: устав СПбГУ ГА, учебная программа по соответствующему направлению подготовки магистров, Положение о балльно-рейтинговой системе оценки знаний и обеспечения качества учебного процесса в ГУГА.

На первом занятии преподаватель доводит до сведения обучающихся график текущего контроля освоения дисциплины и критерии оценки знаний при текущем контроле успеваемости, а также сроки и условия промежуточной аттестации.

Экзамен является заключительным этапом изучения дисциплины и имеет целью проверить и оценить уровень полученных студентами знаний, умение применять их к решению практических задач, овладение практическими навыками в объеме требований образовательной программы на промежуточном этапе формирования компетенций.

Зачет принимается лектором, ведущим занятия в данной группе по данной дисциплине.

9.3Темы курсовых работ (проектов) по дисциплине

Курсовые проекты не предусмотрены

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

По дисциплине «Управление транспортной безопасностью»:

1. Общее понятие безопасности.
2. Основные причины, вызывающие возрастание значения безопасности РФ в современных условиях.
3. Основные документы, определяющие понятия «безопасность РФ» и «национальная безопасность РФ».
4. Основные термины и определения, связанные с понятием безопасности на транспорте.
5. Понятие комплексной системы обеспечения безопасности.
6. Основные направления нормативно-правовой деятельности в области обеспечения безопасности на транспорте и их характеристика.
7. Основные направления организационной деятельности по обеспечению безопасности на транспорте и их характеристика.
8. Основные организационные задачи субъектов транспортной инфраструктуры по обеспечению безопасности на транспорте и их характеристика.
9. Понятие моделей объектов, процессов и систем их классификация и требования к ним.
10. Назначение моделей.

9.5 Показатели, критерии, описание шкалы оценивания

Показатели оценивания	Критерии оценивания
Знать: - основные пути и методы решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта; - требования нормативно-правовой базы в области обеспечения информационной безопасности на предприятиях гражданской авиации; - основные возможности и характеристики программных средств обеспечения защиты информации.	Перечисление, сравнение методов решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта, основных характеристик программных средств обеспечения защиты информации. Анализ, сопоставление требований нормативно-правовой базы в области обеспечения информационной безопасности на предприятиях гражданской авиации, методов решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта.
Уметь: - определять «узкие» места в системе обеспечения информационной безопасности, и предлагать пути их устранения; - грамотно эксплуатировать программные средства информационной безопасности.	Самостоятельность в определении узких места в системе обеспечения информационной безопасности, предложении пути их устранения. Профессиональная грамотность в эксплуатации программных средств информационной безопасности.
Владеть: - методикой разработки и внедрения систем информационной безопасности в структурных подразделениях системы воздушного транспорта**;** - программными средствами защиты информации при работе с компьютерными системами, включая приёмы антивирусной защиты.	Владение методикой разработки и внедрения систем информационной безопасности в структурных подразделениях системы воздушного транспорта**;** - программными средствами защиты информации при работе с компьютерными системами, включая приёмы антивирусной защиты.

Описание шкалы оценивания:

Зачет: сравнивает методы решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта, основных характеристик программных средств обеспечения защиты информации.

Анализирует, сопоставляет требования нормативно-правовой базы в области обеспечения информационной безопасности на предприятиях

гражданской авиации, методы решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта.

Самостоятельно определяет узкие места в системе обеспечения информационной безопасности, предлагает пути их устранения.

Профессионально грамотно эксплуатирует программные средства информационной безопасности.

Владеет методикой разработки и внедрения систем информационной безопасности в структурных подразделениях системы воздушного транспорта**;**

- программными средствами защиты информации при работе с компьютерными системами, включая приёмы антивирусной защиты.

Не зачет: перечисляет методы решения задач в области создания режима информационной безопасности систем автоматизации воздушного транспорта, основные характеристики программных средств обеспечения защиты информации. Самостоятельно не определяет узкие места в системе обеспечения информационной безопасности, не предлагает пути их устранения.

Не владеет методикой разработки и внедрения систем информационной безопасности в структурных подразделениях системы воздушного транспорта**,** программными средствами защиты информации при работе с компьютерными системами, включая приёмы антивирусной защиты.

9.6 Типовые контрольные задания для проведения текущего контроля и промежуточной аттестации по итогам обучения по дисциплине

1. Дать определение понятию «Информационная безопасность»;
2. Объяснить понятие практического аспекта информационной безопасности «Доступность»;
3. Объяснить понятие практического аспекта информационной безопасности «Целостность»;
4. Объяснить понятие практического аспекта информационной безопасности «Конфиденциальность»;
5. Законодательный уровень обеспечения информационной безопасности. Что это такое? Что входит в это понятие? Примеры законодательных актов;
6. Административный уровень обеспечения информационной безопасности. Понятие «Политика безопасности». Уровни детализации административного уровня, их содержание;
7. Программа безопасности. Её синхронизация с жизненным циклом информационных систем;
8. Процедурный уровень обеспечения информационной безопасности. Что это такое? Классы мер процедурного уровня;
9. Процедурный уровень обеспечения информационной безопасности. Управление персоналом;
10. Процедурный уровень обеспечения информационной безопасности. Физическая защита.

11. Процедурный уровень обеспечения информационной безопасности. Поддержание работоспособности;

12. Процедурный уровень обеспечения информационной безопасности. Реагирование на нарушения режима безопасности;

13. Процедурный уровень обеспечения информационной безопасности. Планирование восстановительных работ;

13. Программно-технический уровень обеспечения информационной безопасности. Сервисы программно-технического уровня:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищённости;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

14. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Общие понятия.

15. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Понятие «Политика безопасности» и её механизмы;

16. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Понятие «Аудит» и его механизмы;

17. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Понятие «Корректность» (Гарантированности) и её механизмы;

18. «Критерии безопасности компьютерных систем» (Оранжевая книга). Таксономия требований. Понятие «Документация» и её содержание;

19. Классификация угроз информационной безопасности;

20. Эталонная модель взаимодействия открытых систем. Назначение.

21. Эталонная модель взаимодействия открытых систем. Структура.

22. Эталонная модель взаимодействия открытых систем. Функции уровней.

23. Эталонная модель взаимодействия открытых систем. Прохождение пакетов через ЭМВОС при передаче данных.

24. Комплексный межсетевой экран. Назначение.

25. Комплексный межсетевой экран. Состав.

26. Комплексный межсетевой экран. Экранирующий маршрутизатор. Его назначение.

27. Комплексный межсетевой экран. Экранирующий маршрутизатор. Выполняемые защитные функции.

28. Комплексный межсетевой экран. Экранирующий маршрутизатор. Достоинства и недостатки.

29. Комплексный межсетевой экран. Шлюз сеансового уровня. Назначение.

30. Комплексный межсетевой экран. Шлюз сеансового уровня. Выполняемые защитные функции.

31. Комплексный межсетевой экран. Шлюз сеансового уровня. Функция обеспечения виртуального соединения.

32. Комплексный межсетевой экран. Шлюз сеансового уровня. Процедура квитирования связи по протоколу TCP/IP.

33. Комплексный межсетевой экран. Шлюз сеансового уровня. Трансляция внутренних IP-адресов.

34. Комплексный межсетевой экран. Шлюз сеансового уровня. Достоинства и недостатки.

35. Комплексный межсетевой экран. Шлюз прикладного уровня. Назначение.

36. Комплексный межсетевой экран. Шлюз прикладного уровня. Выполняемые защитные функции.

37. Комплексный межсетевой экран. Шлюз прикладного уровня. Программные посредники.

38. Комплексный межсетевой экран. Шлюз прикладного уровня. Достоинства и недостатки.

39. Вредоносное программное обеспечение. Классификация (виды).

40. Вредоносное программное обеспечение. Компьютерные вирусы. Классификация.

41. Вредоносное программное обеспечение. Компьютерные вирусы. Файловый нерезедентный вирус.

42. Вредоносное программное обеспечение. Компьютерные вирусы. Файловый резедентный вирус.

43. Вредоносное программное обеспечение. Компьютерные вирусы. Бутовый вирус.

44. Вредоносное программное обеспечение. Компьютерные вирусы. Макровирус.

45. Вредоносное программное обеспечение. Троянские программы. Семейства троянских программ.

46. Вредоносное программное обеспечение. Компьютерные вирусы. Компьютерные сетевые черви.

47. Вредоносное программное обеспечение. Компьютерные вирусы. Отличительные признаки компьютерных вирусов, троянских программ, компьютерных сетевых червей.

48. Вредоносное программное обеспечение. Другое вредоносное программное обеспечение. Примеры.

49. Средства борьбы с вредоносным программным обеспечением. Выполняемые функции.

50. Современные антивирусные пакеты.

Примерный перечень вопросов для промежуточной аттестации:

1. Общие понятие информационной безопасности компьютерных систем (ИБКС). Практические аспекты ИБКС, уровни обеспечения ИБКС.
2. Законодательный уровень обеспечения ИБКС. Основные законодательные акты и нормативные документы.
3. Административный уровень обеспечения ИБКС. Его назначение и содержание.
4. Процедурный уровень обеспечения ИБКС. Его назначение и содержание
5. Программно-технический уровень обеспечения ИБКС. Его назначение и содержание.
6. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «ПОЛИТИКА БЕЗОПАСНОСТИ», и механизмы ее реализации.
7. Таксономия критериев информационной безопасности по «Оранжевой книге». Механизмы «ПРОИЗВОЛЬНОЕ УПРАВЛЕНИЕ ДОСТУПОМ», и «ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВ». Таксономия критериев информационной безопасности по «Оранжевой книге». Механизмы «МЕТКИ БЕЗОПАСНОСТИ», и «НОРМАТИВНОЕ УПРАВЛЕНИЕ ДОСТУПОМ».
8. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «АУДИТ», и механизмы его реализации.
9. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «КОРРЕКТНОСТЬ», и механизмы его реализации.
10. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «ДОКУМЕНТАЦИЯ».
11. Анализ угроз информационным компьютерным системам. Виды потенциальных угроз.
12. Противодействие межсетевому несанкционированному доступу. Эталонная модель взаимодействия открытых систем. Назначение, принцип функционирования.
13. Противодействие межсетевому несанкционированному доступу. Комплексный межсетевой экран. Состав, назначение. Противодействие межсетевому несанкционированному доступу. Экранирующий маршрутизатор. Назначение, выполняемые функции, достоинства и недостатки.
14. Противодействие межсетевому несанкционированному доступу. Шлюз сеансового уровня. Назначение, выполняемые функции, достоинства и недостатки.

15. Противодействие межсетевому несанкционированному доступу. Прикладной шлюз. Назначение, выполняемые функции, достоинства и недостатки.

16. Вредоносное программное обеспечение; виды, отличительные особенности

17. Компьютерные вирусы. Механизм распространения.

18. Компьютерные вирусы. Файловый нерезидентный вирус.

19. Компьютерные вирусы. Файловый резидентный вирус.

20. Компьютерные вирусы. Бутовый вирус.

21. Компьютерные вирусы. Особенности макровирусов.

22. Троянские программы.

23. Сетевые черви.

24. Другое вредоносное программное обеспечение.

25. Средства борьбы с вредоносным программным обеспечением. Классификация.

10 Методические рекомендации для обучающихся по освоению дисциплины

При проведении всех видов занятий основное внимание уделять рассмотрению принципов формирования системы информационной безопасности на предприятиях и в организациях гражданской авиации, работе по анализу потенциальных угроз, а также применению изучаемого материала на практике.

Теоретическая подготовка студентов по дисциплине обеспечивается на лекциях. На лекциях обучаемым даются систематизированные основы знаний по состоянию и основным проблемам информационной безопасности.

Теоретические положения, излагаемые в лекциях должны иллюстрироваться примерами их практической реализации в информационных системах и средствах обеспечения защиты информации. Для облегчения восприятия студентом сложного и разнообразного материала рекомендуется изучение новых разделов курса начинать с краткого введения, в котором устанавливается связь с предыдущими и смежными дисциплинами учебного плана, и рекомендовать конкретную учебную литературу. Чрезвычайно важно научить студента применять получаемые знания к решению практических задач. Для этого могут быть разработаны специальные задания с решениями, по которым и организуется самостоятельная работа студентов в течение семестра. На самостоятельное изучение выносятся наиболее простые вопросы изучаемых тем. Самостоятельное изучение позволяет привить навык поиска интересующих вопросов в источниках, в том числе и дополнительных.

Проведение практических занятий осуществляется после прочтения на лекциях соответствующего теоретического материала, и служит средством закрепления полученных знаний и формирования навыков и умений исследований.

Практические занятия призваны обеспечить получение студентами практических навыков и умений по применению полученных знаний.

Все виды учебных занятий проводятся с активным использованием технических средств обучения и имеющихся в наличии образцов.

Изучение дисциплины построено таким образом, чтобы обеспечивалось наилучшее усвоение материала. Для активизации, индивидуализации и интенсификации изучения дисциплины в течение всего периода обучения предполагается проводить краткосрочные письменные контрольные работы (летучки) перед началом лекций и практических занятий.

Текущий контроль успеваемости студентов необходимо осуществлять систематически: на лекциях, при подготовке и проведении практических занятий. Кроме того, следует проводить рубежный контроль усвоения теоретического материала по наиболее сложным разделам программы дисциплины.

Итоговый контроль знаний студентов по разделам и темам дисциплины проводится в виде зачета.

Преподаватель дисциплины имеет право на некоторые непринципиальные отступления от содержания программы в научных и педагогических целях.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 25.04.03 Аэронавигация, направленность программы (профиль) «Государственное регулирование деятельности в области гражданской авиации» (2021 год набора).

Программа рассмотрена и утверждена на заседании кафедры №21 Летной эксплуатации и безопасности полетов в ГА «17» ___10____2022 года, протокол № 3.

Разработчики:

ст. преподаватель Шестаков С.А.

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

Заведующий кафедрой № 12:

к.п.н., доцент. Федоров А.В.

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

Программа согласована:

Руководитель ОПОП ВО:

к.т.н., доцент Королькова М.А..

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

Программа рассмотрена и одобрена на заседании Учебно-методического совета Университета «23»___11___ 2022 года, протокол № 3.