МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНТРАНС РОССИИ)
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)
ФГБОУ ВО «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ»
(ФГБОУ ВО СПбГУ ГА)

УТВЕРЖДАЮ

Первый
проректор-проректор
по учебной работе
_____ Н.Н. Сухих
«15» февраля 2018 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность информационных систем

Направление подготовки
25.04.04. Эксплуатация аэропортов и обеспечение полетов воздушных судов

Направленность (профиль) программы
Управление транспортной безопасностью

Квалификация выпускника
магистр

Форма обучения:
заочная

Санкт-Петербург
2018

1 Цели освоения дисциплины

Целью освоения дисциплины «Безопасность информационных систем» является формирование у студентов системы знаний в области информационной безопасности компьютерных систем и применения на практике 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 (модуля) 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 выпускника к грамотному использованию защитных механизмов обеспечивающих защиту информационных ресурсов в информационных системах.

2. Место дисциплины в структуре ОПОП ВО

Данная учебная дисциплина относится к общенаучным дисциплинам и требует от студентов знаний по дисциплинам математического и естественнонаучного цикла в объёме, определяемом соответствующими программами.

Данная дисциплина позволяет студенту обобщить разнообразные знания, полученные в процессе изучения дисциплин профессионального и естественнонаучного циклов, и использовать их для организации и проведения работ по созданию необходимых условий, направленных на формирование заданной политики информационной безопасности на предприятиях системы воздушного транспорта.

Дисциплина «Безопасность информационных систем» представляет собой дисциплину по выбору вариативной части общенаучного цикла дисциплин (М1.В.ДВ.01.01).

Дисциплина «Безопасность информационных систем» изучается во втором семестре и базируется на знаниях, полученных студентами при изучении соответствующих дисциплин при получении образования в рамках бакалавриата.

Дисциплина «Безопасность информационных систем» является обеспечивающей для преддипломной практики и дипломного проектирования.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля)

Процесс освоения дисциплины (модуля) направлен на формирование следующих компетенций:

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
ОК-7 способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности; ПК-18 способностью и готовностью оценивать основные риски функционирования структурных подразделений авиационного предприятия (аэропортовых служб); ПК-27 способностью и готовностью рассчитывать и оценивать условия и последствия; ПК-53 способностью организовывать и совершенствовать системы учета и документооборота.	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

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
	системы воздушного транспорта; - программными средствами защиты информации при работе с компьютерными системами, включая приёмы антивирусной защиты.

4 Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины (модуля) составляет 2 зачетных единицы 72 академических часа.

Наименование	Всего часов	Курс 1
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 (зачёту, экзамену) *необходимо указать конкретный вид промежуточной аттестации*	8,7 Зачет	8,7 Зачет

5 Содержание дисциплины (модуля)

5.1 Соотнесения тем (разделов) дисциплины (модуля) и формируемых компетенций

Темы, разделы дисциплины	Количество часов	ОК-7	ПК-18	ПК-27	ПК-53	Образовательные технологии	Оценочные средства
Тема 1. Задачи по обеспечению информационной безопасности компьютерных систем	6	+	+			ВК, СРС	У
Тема 2. Уровни обеспечения Информационной безопасности	7		+		+	ИЛ, СРС	
Тема 3. Анализ угроз информационной безопасности.	7	+		+		СРС	
Тема .4. Таксономия критериев информационной безопасности.	14		+			Л, ПЗ, СРС	У
Тема 5. Защита информационных систем от вредоносного программного обеспечения	15		+	+	+	Л, ПЗ, ИПЗ, СРС	У
Тема 6. Межсетевое экранирование	14		+	+		ИЛ, ИПЗ, СРС	У
Промежуточная аттестация	9						
Итого по дисциплине	**72**						**Зачет**

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

5.2 Темы (разделы) дисциплины и виды занятий

Наименование раздела дисциплины	Л	ИЛ	ПЗ	ИПЗ	СРС	Всего часов
Тема 1. Задачи по обеспечению информационной безопасности компьютерных систем					6	6
Тема 2. Уровни обеспечения Информационной безопасности		1			6	7
Тема 3. Анализ угроз информационной безопасности.					7	7
Тема .4. Таксономия критериев информационной безопасности.	1		1		12	14
Тема 5. Защита информационных систем от вредоносного программного обеспечения	1		1	1	12	15
Тема 6. Межсетевое экранирование		1		1	12	14
Итого:	**2**	**2**	**2**	**2**	**55**	**63**
Промежуточная аттестация:						**9**
Всего по дисциплине:						**72**

5.3 Содержание дисциплины

Тема 1. Задачи по обеспечению информационной безопасности компьютерных систем

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

Тема 2. Тема 2. Уровни обеспечения Информационной безопасности

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

Тема 3. Анализ угроз информационной безопасности.

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

Тема 4. Таксономия критериев информационной безопасности

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

Тема 5. Защита информационных систем от вредоносного программного обеспечения

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

Тема 6. Межсетевое экранирование

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

5.4 Практические занятия

Номер темы дисциплины (модуля)	Тематика практических занятий (семинаров)	Трудо-емкость (часы)
4	Таксономия критериев информационной безопасности	1
5	Защита информационных систем от вредоносного программного обеспечения	2
6	Межсетевое экранирование	1
Итого по дисциплине		**4**

5.5 Лабораторный практикум

Лабораторный практикум учебным планом не предусмотрен.

5.6. Самостоятельная работа

№ раздела, темы дисциплины	Виды самостоятельной работы	**Трудоемкость (часы)**
1	самостоятельное овладение студентами материала темы. [4]	6
2	самостоятельное овладение студентами материала темы [2, 5]	6
3	самостоятельное овладение студентами материала темы [1,2,3,6]	7
4	самостоятельное овладение студентами материала темы [3] выполнение задания в соответствии с	12

	инструкциями и методическими указаниями преподавателя	
5	самостоятельное овладение студентами материала темы [2,4] выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя	12
6	самостоятельное овладение студентами материала темы [1,3] выполнение задания в соответствии с инструкциями и методическими указаниями преподавателя	12
	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

-**проблемная 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 (модуля)

9.1. Оценка текущего контроля успеваемости и знаний студентов

Оценка

При изучении дисциплины использование бально-рейтинговой системы не предусмотрено.

Оценка студенту за семестр без сдачи зачета - не предусмотрена.

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.

9.2. Типовые контрольные задания для проведения текущего контроля и промежуточной аттестации по итогам обучения по дисциплине (модулю)

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 зачета:

1. Общие понятие информационной безопасности компьютерных систем (ИБКС). Практические аспекты ИБКС, уровни обеспечения ИБКС. (ОК-1, ОК-8)
2. Законодательный уровень обеспечения ИБКС. Основные законодательные акты и нормативные документы. (ОК-8, ОК-22, ПК-1, ПК-18, ПК-39, ПК-51)
3. Административный уровень обеспечения ИБКС. Его назначение и содержание. (ОК-8, ОК-22, ПК-1, ПК-18, ПК-39, ПК-51)
4. Процедурный уровень обеспечения ИБКС. Его назначение и содержание. (ОК-8, ОК-22, ПК-1, ПК-18, ПК-39, ПК-51)
5. Программно-технический уровень обеспечения ИБКС. Его назначение и содержание. (ОК-8, ОК-22, ПК-1, ПК-18, ПК-39, ПК-51)
6. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «ПОЛИТИКА БЕЗОПАСНОСТИ», и механизмы ее реализации. (ОК-8, ПК-18, ПК-45)
7. Таксономия критериев информационной безопасности по «Оранжевой книге». Механизмы «ПРОИЗВОЛЬНОЕ УПРАВЛЕНИЕ ДОСТУПОМ», и «ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ОБЪЕКТОВ». (ОК-8, ПК-18, ПК-45
8. Таксономия критериев информационной безопасности по «Оранжевой книге». Механизмы «МЕТКИ БЕЗОПАСНОСТИ», и «НОРМАТИВНОЕ УПРАВЛЕНИЕ ДОСТУПОМ». (ОК-8, ПК-18, ПК-45
9. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «АУДИТ», и механизмы его реализации. (ОК-8, ПК-18, ПК-45
10. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «КОРРЕКТНОСТЬ», и механизмы его реализации. (ОК-8, ПК-18, ПК-45
11. Таксономия критериев информационной безопасности по «Оранжевой книге». Содержание понятия «ДОКУМЕНТАЦИЯ». (ОК-8, ПК-18, ПК-45
12. Анализ угроз информационным компьютерным системам. Виды потенциальных угроз. (ОК-1, ОК-11, ПК-1, ПК-39, ПК-51)
13. Противодействие межсетевому несанкционированному доступу. Эталонная модель взаимодействия открытых систем. Назначение, принцип функционирования. (ОК-8, ОК-11, ОК-22, ПК-39, ПК-41, ПК-45)

14. Противодействие межсетевому несанкционированному доступу. Комплексный межсетевой экран. Состав, назначение. (ОК-8, ОК-11, ОК-22, ПК-39, ПК-41, ПК-45)

15. Противодействие межсетевому несанкционированному доступу. Экранирующий маршрутизатор. Назначение, выполняемые функции, достоинства и недостатки. (ОК-8, ОК-11, ОК-22, ПК-39, ПК-41, ПК-45)

16. Противодействие межсетевому несанкционированному доступу. Шлюз сеансового уровня. Назначение, выполняемые функции, достоинства и недостатки. (ОК-8, ОК-11, ОК-22, ПК-39, ПК-41, ПК-45)

17. Противодействие межсетевому несанкционированному доступу. Прикладной шлюз. Назначение, выполняемые функции, достоинства и недостатки. (ОК-8, ОК-11, ОК-22, ПК-39, ПК-41, ПК-45)

18. Вредоносное программное обеспечение; виды, отличительные особенности. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

19. Компьютерные вирусы. Механизм распространения. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

20. Компьютерные вирусы. Файловый нерезидентный вирус. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

21. Компьютерные вирусы. Файловый резидентный вирус. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

22. Компьютерные вирусы. Бутовый вирус. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

23. Компьютерные вирусы. Особенности макровирусов. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

24. Троянские программы. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

25. Сетевые черви. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

26. Другое вредоносное программное обеспечение. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

27. Средства борьбы с вредоносным программным обеспечением. Классификация. (ОК-8, ОК-11, ПК-18, ПК-39, ПК-45)

10. Методические рекомендации для обучающихся по освоению дисциплины (модуля)

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 инженерных 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 ВПО по направлению подготовки 162700 Эксплуатация аэропортов и обеспечение полетов воздушных судов (квалификация (степень) «магистр»).

Разработчик:

Ст. преподаватель Шестаков С.А.

Программа согласована:

Руководитель ОПОП

д.т.н., профессор Балясников В.В.

Директор Высшей школы аэронавигации

к.т.н. Богданов В.Г.

Программа рассмотрена и одобрена на заседании Учебно-методического совета Университета 14 февраля 2018 года, протокол № 5.