МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ГРАЖДАНСКОЙ АВИАЦИИ

М.А. Родионов

ОРГАНИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ АВИАПРЕДПРИЯТИЯМИ

Учебно-методическое пособие
по изучению дисциплины
и проведению практических занятий

для студентов
направления 25.03.03
очной формы обучения

Москва
2019

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ (МГТУ ГА)»

Кафедра экономики и управления на воздушном транспорте

М.А. Родионов

ОРГАНИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ АВИАПРЕДПРИЯТИЯМИ

Учебно-методическое пособие
по изучению дисциплины
и проведению практических занятий

для студентов
направления 25.03.03
очной формы обучения

Москва
2019

ББК 338:05
Р-60

Рецензент:
Сухоруков А.И. – д-р техн. наук

Родионов М.А.
Р-60 Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями: учебно-методическое пособие по изучению дисциплины и проведению практических занятий. / М.А. Родионов. – Воронеж: ООО «МИР», 2019. – 36с.

Данное учебно-методическое пособие издается в соответствии с рабочей программой учебной дисциплины «Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями» по учебному плану для студентов направления 25.03.03 очной формы обучения.

Рассмотрено и одобрено на заседании кафедры 14.05.2019 г. и методического совета 23.05.2019 г.

В авторской редакции.

Подписано в печать 08.07.2019 г.
Формат 60х84/16 Печ.л. 2,25 Усл. печ. л. 2,09
Заказ 501/8479 Тираж 80 экз.

Московский государственный технический университет ГА
125993 Москва, Кронштадтский бульвар, д.20

Отпечатано ООО «МИР»
394033, г. Воронеж, Ленинский пр-т 119А, лит. Я, оф. 215
Тел.: 8 (958) 649-53-31 Email: 89586495331@mail.ru

Содержание

1 ЦЕЛЬ, ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ И ЕЕ МЕСТО В УЧЕБНОМ ПРОЦЕССЕ

Целью освоения дисциплины **«Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями»** является формирование у студентов основы знаний в области теоретических основ организационно-управленческой деятельности, обеспечивающей эффективное построение процессов обеспечения информационной безопасности управления авиапредприятиями.

Для достижения цели ставятся следующие **задачи**:

- получение студентами основных теоретических знаний по вопросам организации бизнес-процессов обеспечения информационной безопасности;
- раскрытие сущности, целей, основ организации бизнес процессов обеспечения информационной безопасности управления авиапредприятиями;
- информационно-аналитическое сопровождение управленческой деятельности по обеспечению информационной безопасности;
- осуществление информационного аудита в организации бизнес-процессов информационной безопасности управления авиапредприятиями.

Дисциплина «Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями» относится к учебным дисциплинам вариативной части образовательной программы (далее - ООП) направления подготовки 25.03.03 (161000) – Аэронавигация, квалификация (степень) – бакалавр. Дисциплина изучается в седьмом семестре. Форма итоговой отчетности - экзамен.

Потребность в дисциплине определяется тем, что студент нуждается в получении определенных теоретических представлений о роли и задачах организации бизнес-процессов обеспечения информационной безопасности управления в условиях конкурентной борьбы и применения технологий бизнес

– разведки, а также нестабильности среды, знаний об основах обеспечения информационной безопасности управления, а также о возможностях применения современных методов обеспечения информационной безопасности в деятельности авиапредприятий.

Для успешного освоения дисциплины «Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями» студент должен владеть знаниями, умениями и навыками, сформированными дисциплинами ОП бакалавриата: “Авиатранспортный менеджмент”, “Теория процессного управления”, “Информационный менеджмент авиапредприятий”, “Архитектура авиапредприятий”, “Бизнес-анализ”, “Процессный проектный консалтинг на авиапредприятиях”, “Реинжиниринг бизнес-процессов авиапредприятий”, “Системы менеджмента качества авиапредприятий”, “Организация операционных бизнес-процессов авиапредприятий” и др,

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс изучения дисциплины «Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями» направлен на формирование у студентов профессиональных компетенций (ПК) производственно-технологической деятельности:

способность к экономическому, управленческому и математическому образу мышления при решении задач управления бизнес-процессами (ПК-1В);

способность выполнять моделирование бизнес-процессов с использованием прикладного программного обеспечения (ПК-2В);

способность применять методы системного и структурного анализа существующих бизнес-процессов (ПК-3В);

способность разрабатывать регламенты процессов и административные регламенты подразделений (должностей) на основе использования прикладного программного обеспечения (ПК-4В).

В результате изучения дисциплины «Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями» студент должен:

- по компетенции ПК-1В:

знать:

методы и технологии обеспечения информационной безопасности управления авиапредприятиями (ПК-1В.1.24);

основные риски обеспечения информационной безопасности управления авиапредприятиями и организационных мероприятий по их минимизации (ПК-1В.1.25);

уметь:

принимать эффективные экономические решения при организации бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями на основе использования организационных и математических методов (ПК-1В.2.17);

владеть:

навыками восприятия, обобщения и анализа информации при организации бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-1В.3.12);

- по компетенции ПК-2В:

знать:

функциональные возможности современного прикладного программного обеспечения моделирования бизнес-процессов (ПК-2В.1.6);

базовые процедуры исполнения бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-2В.1.21);

методы систематизации и системного анализа бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями, методы и средства их оценки (ПК-2В.1.22);

уметь:

проводить анализ и обосновывать предложения по проектированию и реинжинирингу бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-2В.2.22);

применять методы и средства регламентации, систематизации и оценки бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-2В.2.23);

владеть:

навыками разработки процессной модели авиапредприятия в интересах обеспечения информационной безопасности управления авиапредприятиями (ПК-2В.3.15);

- по компетенции ПК-3В:

знать:

внутренние взаимосвязи в системе бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-3В.1.34);

системы структурных элементов, обеспечивающих реализацию бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-3В.1.35);

входные и выходные материальные и информационные потоки, используемые и формируемые в ходе выполнения функций обеспечения информационной безопасности управления авиапредприятиями (ПК-3В.1.36);

уметь:

выделять объекты процессной модели, оказывающие существенное влияние на деятельность структурных элементов системы бизнес-процессов оперативного контроллинга авиапредприятий. Анализировать структуру

бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-3В.2.23);

выделять объекты процессной модели, оказывающие существенное влияние на деятельность структурных элементов системы бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-3В.2.24);

владеть:

навыками разработки предложений по преобразованию системы бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями (ПК-3В.3.12);

- по компетенции ПК-4В:

знать:

технологии формирования регламентов процессов и административных регламентов подразделений (должностей) на основе использования прикладного программного обеспечения (ПК-4В.1.2);

номенклатуру административных регламентов в сфере обеспечения информационной безопасности управления авиапредприятиями (ПК-4В.1.11);

особенности современных стандартов и методик, принципов разработки регламентов в сфере организации и обеспечения информационной безопасности управления авиапредприятиями (ПК-4В.1.12);

уметь:

разрабатывать процедуры контроля выполнения регламентов процесса, подразделения (должности) или административного регламента подразделения в сфере обеспечения информационной безопасности управления авиапредприятиями (ПК-4В.2.9);

использовать современные стандарты, методики, программное обеспечение при разработке регламентов процессов и административных регламентов подразделений в сфере обеспечения информационной безопасности управления авиапредприятиями (ПК-4В.2.10);

владеть:

навыками разработки регламентов процессов и административных регламентов подразделений в сфере обеспечения информационной безопасности управления авиапредприятиями на основе использования прикладного программного обеспечения (ПК-4В.3.9).

По дисциплине предусмотрены 36 часов лекционных занятий и 32 часов практических занятий (семинаров).

Промежуточный контроль проводится в виде экзамена.

3 МЕТОДИЧЕСКИЕ УКАЗАНИЮ ПО ИЗУЧЕНИЮ ТЕМ ДИСЦИПЛИНЫ

РАЗДЕЛ I. ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ ОРГАНИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ АВИАПРЕДПРИЯТИЯМИ

Тема 1. Информационная безопасность как составная часть комплексной безопасности авиапредприятия и необходимое условие эффективного менеджмента организации.

Понятие информационной безопасности. Информация как стратегический ресурс государства и общества. Актуальность, цели, задачи и порядок изучения курса. Исторические аспекты вопроса. Роль и место информационной безопасности в системе комплексной безопасности организации. Информационная безопасность как составная часть “стратегии непрямых действий” в бизнесе.

Изучая тему, необходимо акцентировать внимание на следующих положениях: основные понятия и определения информационной безопасности,

роль и место информационной безопасности в системе комплексной безопасности организации.

Контрольные вопросы:

1. Роль информационной безопасности в системе комплексной безопасности организации.
2. Перечислите и раскройте содержание основных принципов обеспечения информационной безопасности.
3. Перечислите и раскройте составные части и направления обеспечения информационной безопасности.
4. Основные понятия и определения теории информационной безопасности организации?
5. Роль и место информационной безопасности в системе комплексной безопасности организации и безопасности управления?
6. Особенности обеспечения информационной безопасности аэропорта.
7. Особенности обеспечения информационной безопасности авиакомпании.

Тема 2. Основные понятия и подходы к обеспечению информационной безопасности управления авиапредприятиями.

Основные понятия и определения теории информационной безопасности в соответствии с действующими нормативными правовыми документами Российской Федерации и международным правом, а также современными концепциями. Цели, задачи, направления, составные части, закономерности и принципы обеспечения информационной безопасности управления авиапредприятием. Информационная безопасность управления авиапредприятием. Основные субъекты информационной безопасности управления.

Изучая тему, необходимо акцентировать внимание на следующих положениях: содержание основных понятий и определений теории информационной безопасности в соответствии с действующими нормативными правовыми документами Российской Федерации.

Контрольные вопросы:

1. Сущность информационной безопасности.
2. Объекты информационной безопасности управления авиапредприятием.
3. Характеристика современных тенденций изменения процессов организации и процессов обеспечения информационной безопасности.
4. Субъекты информационной безопасности управления.
5. Обеспечение информационной безопасности управления – это?
6. Интересы организации в информационной сфере?
7. Цели, задачи, направления, обеспечения информационной безопасности управления авиапредприятием.
8. Составные части, закономерности и принципы обеспечения информационной безопасности управления авиапредприятием.

Тема 3. Угрозы бизнес-процессам обеспечения информационной безопасности управления современными авиапредприятиями.

Существующие подходы к построению классификации угроз информационной безопасности на различных уровнях управления бизнес-процессами. Риск-ориентированная оценка информационной безопасности управления. Модели прогнозирования и нейтрализации угроз информационной безопасности и их применение.

Изучая тему, необходимо акцентировать внимание на следующих положениях: Существующие подходы к построению классификации угроз информационной безопасности на различных уровнях управления бизнес-

процессами. Модели прогнозирования и нейтрализации угроз информационной безопасности и их применение.

Контрольные вопросы:

1. Сущность угроз бизнес-процессам обеспечения информационной безопасности управления.
2. Угрозы жизненно-важным интересам организации в информационной сфере.
3. Модели прогнозирования и нейтрализации угроз информационной безопасности.
4. Основные типы политики безопасности обеспечения информационной безопасности управления авиапредприятиями.
5. Система информационной безопасности управления авиапредприятия.
6. Методы и средства защиты информации.
7. Алгоритмы информационно-психологической защиты.

Практическое занятие №1.

«Угрозы бизнес-процессам обеспечения информационной безопасности управления современными авиапредприятиями»

Перечень контрольных вопросов по теме:

1. Угрозы бизнес-процессам информационной безопасности управления.
2. Классификация угроз информационной безопасности.
3. Анализ угроз бизнес-процессам информационной безопасности управления и их последствий.
4. Модели прогнозирования и нейтрализации угроз информационной безопасности и их применение.
5. Угрозы информационной безопасности на авиапредприятии.
6. Проблемы практической реализации модели информационной безопасности управления авиапредприятием.

Тема 4. Нормативное правовое обеспечение и стандартизация процессов обеспечения информационной безопасности управления авиапредприятиями.

Структура нормативного правового обеспечения Российской Федерации в области информационной безопасности. Международная нормативная правовая база по вопросам информационной безопасности. Структура внутреннего нормативного правового обеспечения информационной безопасности управления на авиапредприятии. Понятие персональных данных. Законодательство о персональных данных. Субъекты и операторы персональных данных. Международные стандарты обеспечения информационного обмена. Специфика информационных угроз, особенности решения вопросов обеспечения информационной безопасности в различных сферах жизнедеятельности общества, а также бизнес - процессах. Субъекты, объекты, цели и задачи, механизмы обеспечения информационной безопасности управления. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Роль и место вопросов обеспечения информационной безопасности управления при организации бизнес-процессов авиапредприятия.

Изучая тему, необходимо акцентировать внимание на следующих положениях: Структура нормативного правового обеспечения Российской Федерации в области информационной безопасности, структура внутреннего нормативного правового обеспечения информационной безопасности управления на авиапредприятии.

Контрольные вопросы:

1. Нормативная правовая база российского законодательства в области информационной безопасности (в части, касающейся предприятий).
2. Международные нормативно-правовые документы по вопросам информационной безопасности (в части, касающейся предприятий).

3. Состояние и перспективы борьбы с компьютерной преступностью в России. Анализ положений Уголовного кодекса Российской Федерации.

4. Основные положения законодательства в сфере обеспечения информационной безопасности управления авиапредприятиями.

5. Государственные стандарты, регламентирующие терминологию в области защиты информации.

6. Основные нормативные правовые и руководящие документы, касающиеся вопросов соблюдения государственной тайны и их содержание.

7. Определение и содержание процессов лицензирования и сертификации.

Тема 5. Применение методов системных исследований при анализе процессов обеспечения информационной безопасности управления авиапредприятиями.

Основные положения современной теории системных исследований. Методология применения системного подхода при анализе процессов обеспечения информационной безопасности, соотношение гуманитарных, естественнонаучных и технических аспектов. Системный и процессный подходы к управлению информационной безопасностью. Влияние структурных и функциональных особенностей системы управления авиапредприятием на бизнес-процессы обеспечения информационной безопасности.

Изучая тему, необходимо акцентировать внимание на следующих положениях: методология применения системного подхода при анализе процессов обеспечения информационной безопасности, соотношение гуманитарных, естественнонаучных и технических аспектов.

Контрольные вопросы:

1. Перечислите основные направления современных системных исследований, раскройте их содержание.

2. Системный подход к управлению информационной безопасностью.

3. Процессный подход к управлению информационной безопасностью.

4. Перечислите основные факторы, влияющие на процессы обеспечения информационной безопасности организации.

5. Применения методов системных исследований при анализе процессов обеспечения информационной безопасности управления.

6. Моделирование как основной метод, используемый при разработке и принятии управленческих решений по информационной безопасности организации.

Практическое занятие №2.

«Системный и процессный подходы к управлению информационной безопасностью»

1. Состав и структура системы комплексного обеспечения информационной безопасности.
2. Особенности методов системных исследований при анализе процессов обеспечения информационной безопасности управления.
3. Процессный подход к управлению информационной безопасностью.
4. Системный подход к управлению информационной безопасностью.

Задачи по теме

Задача 1.

Авиакомпания «Дельта» в результате интенсивного развития расширения зоны полетов открыла 30 филиалов и 70 представительств по России, занимая одно из первых мест по перевозкам в России с перспективами стать лидером сегмента услуг.

Сложность заключаются в отсутствии постоянства и планирования периодичности заявок и время заказа, выделить постоянные маршруты.

В данной ситуации значение надежного и бесперебойного функционирования информационной системы «Дельта» становится стратегически важным. Информационные сбои могут привести к неоказанию услуг, нарушению сроков доставки грузов.

Открытия новых представительств вызвало усложнение информационной структуры компании и спровоцировало определенные проблемы в управлении информационными потоками.

В представительствах устанавливалось разное программное обеспечение без контроля со стороны руководства, целесообразность инсталляции программного продукта определялась специалистами самостоятельно.

В итоге в разных представительствах были установлены различные версии операционных систем и офисных продуктов, что привело к проблемам совместимости форматов данных и стало препятствием для оперативного информационного обмена.

Отсутствие четкой информационной политики компании послужило причиной неконтролируемых и нецелесообразных затрат на закупку программного обеспечения.

Проблема: руководство «Дельта» поставило задачу оптимизации информационного обмена в компании и обеспечения защиты информации.

Определите:

- перечень необходимых мер?

- возможность и целесообразность использования стандартизации?

- варианты процесса стандартизации программного обеспечения в компании?

- последствия стандартизации программного обеспечения в компании?

На основании полученных данных разработайте рациональный вариант плана оптимизации информационной системы авиапредприятия.

Тема 6. Риски и эффективность обеспечения бизнес-процессов информационной безопасности управления авиапредприятиями.

Риски при обеспечении бизнес-процессов информационной безопасности управления авиапредприятиями. Модель оценки информационной безопасности на основе оценки процессов. Оценка информационной безопасности на основе зрелости процессов менеджмента. Риск-ориентированная оценка обеспечения информационной безопасности управления. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке.

Изучая тему, необходимо акцентировать внимание на следующих положениях: Риски при обеспечении бизнес-процессов информационной безопасности управления, модель оценки информационной безопасности на основе оценки процессов.

Контрольные вопросы:

1. Риски при обеспечении бизнес-процессов информационной безопасности управления.
2. Анализ информационных рисков и управление ими.
3. Перечислите основные этапы анализа и оценки информационных рисков, раскройте их содержание.
4. Виды рисков обеспечения информационной безопасности авиапредприятия.
5. Модель оценки информационной безопасности на основе оценки процессов
6. Типовые модели оценки рисков информационной безопасности управления.
7. Риск-ориентированная оценка обеспечения информационной безопасности управления.

Практическое занятие №3.

«Риски и эффективность обеспечения бизнес-процессов информационной безопасности управления авиапредприятиями».

1. Риски при обеспечении бизнес-процессов информационной безопасности управления авиапредприятиями.
2. Управление рисками информационной безопасности управления.
3. Нейтрализация негативных последствий рисков информационной безопасности управления и контрмеры.
4. Риск-ориентированная оценка информационной безопасности управления авиапредприятием.

РАЗДЕЛ II. ПРАКТИКА ОРГАНИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ АВИАПРЕДПРИЯТИЯМИ

Тема 7. Основы организации бизнес-процессов информационной безопасности управления. Политика информационной безопасности управления авиапредприятиями.

Роль и место системы обеспечения информационной безопасности управления в работе авиапредприятия. Деятельность по обеспечению информационной безопасностью управления авиапредприятия как процесс. Бизнес-процессы управления информационной безопасностью на уровне авиапредприятия. Анализ результатов и затрат различных видов ресурсов на обеспечение информационной безопасности управления. Основные этапы процесса обеспечения информационной безопасности предприятия и их содержание. Роль и место Концепции информационной безопасности в процессе разработки, создания и функционирования системы информационной безопасности организации, основные требования к ней. Основные разделы Концепции и Политики информационной безопасности управления

предприятия и их содержание. Документы, практически реализующие Концепцию информационной безопасности. Содержание руководства по обеспечению информационной безопасности в организации. Создание защищенного документооборота на авиапредприятии. Модели управление доступом. Основные этапы процесса организации мероприятий по обеспечению информационной безопасности управления авиапредприятиями. Субъекты обеспечения информационной безопасности авиапредприятия: состав, структура и функции. Модель управления процессами обеспечения информационной безопасности авиапредприятия. Порядок и особенности действий должностных лиц по вопросам обеспечения информационной безопасности в различных условиях обстановки. Электронно-цифровая подпись.

Изучая тему, необходимо акцентировать внимание на следующих положениях: роль и место системы обеспечения информационной безопасности управления в работе авиапредприятия, бизнес-процессы управления информационной безопасностью.

Контрольные вопросы:

1. Роль и место системы обеспечения информационной безопасности управления.
2. Бизнес-процессы управления информационной безопасностью на уровне авиапредприятия.
3. Основные этапы обеспечения информационной безопасности авиапредприятия.
4. Модель управления процессами обеспечения информационной безопасности авиапредприятия.
5. Субъекты обеспечения информационной безопасности авиапредприятия и объекты: состав, структура, функции.
6. Перечислите и кратко охарактеризуйте основные разделы Концепции информационной безопасности авиапредприятия.

7. Перечислите и кратко охарактеризуйте основные этапы процесса организации мероприятий по обеспечению информационной безопасности авиапредприятия.

Практическое занятие №4.

«Разработка Политики / Концепции информационной безопасности управления авиапредприятия»

1. Роль и место Политики / Концепции информационной безопасности управления в обеспечении информационной безопасности.

2 Что является основой для разработки Политики / Концепции информационной безопасности управления предприятием?

3. Какие этапы по созданию системы информационной безопасности организации выполняются после разработки Политики / Концепции информационной безопасности.

4. Основные разделы Политики / Концепции информационной безопасности управления авиапредприятия и их содержание.

Задачи по теме

Задача 1.

На основе положений действующих нормативно-правовых документов, разработать проект концепции информационной безопасности авиакомпании, содержащую следующие основные положения:

1. Общие положения Концепции по обеспечению информационной безопасности.

2. Цели системы информационной безопасности.

3. Задачи системы информационной безопасности.

4. Проблемная ситуация в сфере информационной безопасности:

- объекты информационной безопасности;

- определение модели действий вероятного нарушителя.

- описание особенностей (профиля) каждой из групп вероятных нарушителей;

- основные виды угроз информационной безопасности авиакомпании;

- классификации угроз;

- основные непреднамеренные и преднамеренные искусственные угрозы.

5. Статистическая информация по искусственным нарушениям информационной безопасности.

6. Оценка потенциального ущерба от реализации угрозы.

Тема 8. Информационно-аналитическое сопровождение управленческой деятельности по обеспечению информационной безопасности авиапредприятиями.

Мониторинг управляемых процессов, прогнозирование их развития, моделирование информационных опасностей и угроз, а также мероприятий по их нейтрализации, как необходимые условия адекватной диагностики управляемых процессов, повышения эффективности планируемых и предпринимаемых мер по обеспечению информационной безопасности управления авиапредприятия. Модель принятия управленческого решения по безопасности управления авиапредприятием. Анализ процесса принятия управленческого решения с точки зрения обеспечения его информационной безопасности. Использование “стратегии непрямых действий” в бизнесе.

Изучая тему, необходимо акцентировать внимание на следующих положениях: модель принятия управленческого решения по безопасности управления авиапредприятием, анализ процесса принятия управленческого решения с точки зрения обеспечения его информационной безопасности.

Контрольные вопросы:

1. Информационно-аналитические средства, используемые при разработке и принятии решения по информационной безопасности организации.

2. Перечислите и охарактеризуйте основные этапы процесса принятия управленческого решения по информационной безопасности.

3. Информационный аудит организации авиапредприятия.

4. Основные этапы разработки управленческого решения по информационной безопасности организации.

5. Информационная безопасность процесса принятия управленческого решения в организации.

6. Модель принятия управленческого решения по безопасности управления авиапредприятием.

Практическое занятие №5.

«Анализ процесса принятия управленческого решения с точки зрения обеспечения его информационной безопасности управления»

1. Процесс принятия управленческого решения с позиции обеспечения информационной безопасности управления.

2. Использование “стратегии непрямых действий” в бизнесе.

3. Модель принятия управленческого решения по безопасности управления.

4. Функционал менеджмента авиапредприятия, обеспечивающего информационную безопасность управления.

Задачи по теме

Задача 1.

На основе положений действующих нормативно-правовых документов, разработать проект раздела Концепции информационной безопасности авиакомпании, содержащий следующие положения:

1. Механизмы обеспечения информационной безопасности авиакомпании.

2. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3. Основные направления политики в сфере информационной безопасности.

4. Планирование мероприятий по обеспечению информационной безопасности.

5. Критерии и показатели информационной безопасности.

Задача 2.

На основе положений действующих нормативно-правовых документов, разработать проект раздела Концепции информационной безопасности авиакомпании, содержащий следующие положения:

1. Мероприятия по реализации мер информационной безопасности
2. Организационное обеспечение информационной безопасности.
3. Техническое обеспечение информационной безопасности.
4. Правовое обеспечение информационной безопасности.
5. Оценивание эффективности системы информационной безопасности.

Тема 9. Роль и место информационного аудита в организации бизнес-процессов информационной безопасности управления авиапредприятиями.

Организация и проведение анализа информационной уязвимости авиапредприятия. Роль и место информационного аудита в ходе комплексного аудита организации (авиапредприятия), в процессе информационной санации. Виды информационного аудита, условия их проведения, содержание и взаимосвязь.

Изучая тему, необходимо акцентировать внимание на следующих положениях: организация и проведение анализа информационной уязвимости авиапредприятия, роль и место информационного аудита в ходе комплексного аудита организации.

Контрольные вопросы:

1. Информационный аудит авиапредприятия.

2. Анализ информационных рисков и управление ими.
3. В чем состоит необходимость осуществления информационного аудита на авиапредприятии?
4. Организация и проведение анализа информационной уязвимости авиапредприятия.
5. Виды информационного аудита, их содержание и взаимосвязь.

Практическое занятие № 6.

«Виды информационного аудита, условия их проведения, содержание и взаимосвязь»

1. Роль аудита системы информационной безопасности.
2. Цели аудита информационной безопасности управления.
3. Виды аудита информационной безопасности управления.
4. Этапы информационного аудита безопасности управления.
5. Содержание информационного аудита безопасности управления.

Тема 10. Организация бизнес-процессов информационно-технической безопасности современных автоматизированных информационных систем.

Управление информационно-технической безопасностью предприятия. Демаскирующие признаки информационных объектов. Технические каналы утечки информации. Способы и средства предотвращения утечки информации. Угрозы и объекты обеспечения информационно-технической безопасности, принципы, методы и способы ее обеспечения. Технология процесса обеспечения информационно-технической безопасности организации. Контроль состояния технической защиты информации. Анализ способов нарушений информационной безопасности в современных автоматизированных информационных системах и их таксономия. Способы и средства защиты информации авиапредприятия от утечки по техническим каналам. Средства программно-математического и программно-технического воздействия. Виды

“вирусов” и защита от них. Использование защищенных компьютерных систем. Системы обнаружения и предотвращения атак. Методы и средства защиты данных, применяемые в сетях. Методы криптографии. Электронная цифровая подпись, виды.

Изучая тему, необходимо акцентировать внимание на следующих положениях: управление информационно-технической безопасностью авиапредприятия, органы, принципы, методы, способы и средства защиты и добывания информации.

Контрольные вопросы:

1. Управление информационно-технической безопасностью авиапредприятия.
2. Угрозы и объекты обеспечения информационно-технической безопасности.
3. Технические каналы утечки информации.
4. Способы и средства предотвращения утечки информации.
5. Методы и способы защиты информации в современных автоматизированных информационных системах.
6. Средства защиты информации в современных автоматизированных информационных системах.
7. Средства программно-математического и программно-технического воздействия.
8. Методы и средства защиты данных, применяемые в сетях.
9. Виды “вирусов” и защита от них.

Практическое занятие №7.

«Методы, способы и средства защиты информации в современных автоматизированных информационных системах»

1. Угрозы безопасности информации в современных автоматизированных информационных системах.

2. Методы, средства и способы защиты информации в современных автоматизированных информационных системах.

3. Алгоритмы криптозащиты информации.

4. Анализ средств программно-математического и программно-технического воздействия.

Задачи по теме

Задача 1.

Определите из ниже предложенных вариантов физические средства защиты информации:

1) средства, которые реализуются в виде автономных устройств и систем;

2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;

3) это программы, предназначенные для выполнения функций, связанных с защитой информации

4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств.

Задача 2.

Подготовить краткий отчет по вопросу “Системы защиты информации в ведущих зарубежных странах (США, Великобритания, Франция, Германия, Китай, Япония)”. Определить материалы, описывающие механизмы, способы защиты и преимущественно используемое программное обеспечение.

<u>Тема 11.</u> Организация бизнес-процессов информационно-психологической безопасности. Методы, способы и приемы информационно-психологической защиты должностных лиц авиапредприятия.

Теоретические скрытного информационно-психологического управления. Методы и приемы информационно-психологического воздействия на должностных лиц: продуктивного общения, приемы ведения дискуссии, методы и приемы “мягкого” и “жесткого” информационно-психологического воздействия. Психологический анализ учебных видеофрагментов, демонстрирующих различные приемы информационно-психологического воздействия. Содержание типовых алгоритмов информационно-психологической защиты. Методы, способы и приемы информационно-психологической защиты должностных лиц организации.

Изучая тему, необходимо акцентировать внимание на следующих положениях: методы и приемы информационно-психологического воздействия на должностных лиц, содержание типовых алгоритмов информационно-психологической защиты.

Контрольные вопросы:

1. Методы, способы информационно-психологической защиты должностных лиц авиапредприятия.
2. Приемы информационно-психологической защиты должностных лиц авиапредприятия.
3. Содержание типовых алгоритмов информационно-психологической защиты.
4. Приемы НЛП в информационно-психологической защите должностных лиц авиапредприятия.

Практическое занятие №8.

«Методы, способы и приемы информационно-психологической защиты должностных лиц авиапредприятия»

1. Методы информационно-психологического воздействия на должностных лиц.

2. Способы и приемы информационно-психологического воздействия на должностных лиц.

3. Основные способы и средства обеспечения информационно-психологической безопасности.

4. Содержание алгоритма информационно-психологической защиты личности.

5. Манипулятивные техники информационно-психологического воздействия.

4 ВОПРОСЫ ДЛЯ ПРОВЕДЕНИЯ ЗАКЛЮЧИТЕЛЬНОГО КОНТРОЛЯ

1. Основные понятия и определения теории информационной безопасности организации.

2. Роль и место информационной безопасности в системе комплексной безопасности организации.

3. Основные положения Доктрины информационной безопасности Российской Федерации (в части, касающейся предприятий).

4. Сущность и содержание информационно-технической безопасности авиапредприятия.

5. Сущность и содержание информационно-психологической безопасности авиапредприятия.

6. Информационно-аналитическое обеспечение в системе информационной безопасности управления.

7. Нормативная правовая база российского законодательства в области информационной безопасности (в части, касающейся предприятий).

8. Международные нормативно-правовые документы по вопросам информационной безопасности (в части, касающейся предприятий).

9. Состояние и перспективы борьбы с компьютерной преступностью в России. Анализ положений Уголовного кодекса Российской Федерации.

10. Основные положения законодательства в сфере обеспечения информационной безопасности управления авиапредприятиями.

11. Интересы организации (предприятия, фирмы) в информационной сфере (конкретная организация – по выбору студента).

12. Угрозы жизненно-важным интересам организации (предприятия, фирмы) в информационной сфере (конкретная организация – по выбору студента).

13. Основные подходы к политике обеспечения информационной безопасности управления авиапредприятиями.

14. Система информационной безопасности управления авиапредприятия.

15. Концепция информационной безопасности организации (предприятия).

16. Международные стандарты информационного обмена.

17. Виды “нарушителей” режима защиты информации, модели их действий.

18. Основные нормативные правовые и руководящие документы, касающиеся вопросов соблюдения государственной тайны и их содержание.

19. Основные нормативные правовые и руководящие документы, касающиеся вопросов соблюдения коммерческой тайны и их содержание.

20. Определение и содержание процессов лицензирования и сертификации.

20. Система информационной безопасности организации (предприятия).

21. Органы обеспечения информационной безопасности организации (предприятия): состав, структура и функции в различных условиях обстановки.

22. Организация мероприятий по обеспечению информационной безопасности предприятия (фирмы).

23. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке.

24. Создание и обеспечение защищенного документооборота в организации.

24. Информационный аудит организации авиапредприятия.

25. Анализ информационных рисков и управление ими.

26. Органы, методы, способы и средства добывания информации по техническим каналам.

27. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах.

28. Средства программно-математического и программно-технического воздействия и защита от них.

29. Виды компьютерных “вирусов” и защита от них.

30. Методы и средства защиты данных, применяемые в сетях.

31. Понятие и содержание криптографии, основные методы.

32. Электронная цифровая подпись (понятие, содержание процесса использования электронной цифровой подписи, проблемы).

33. Методы и приемы информационно-психологического воздействия на должностных лиц.

34. Алгоритмы информационно-психологической защиты.

35. Использование интернет-технологий и обеспечение информационной безопасности.

36. Основные технологии построения защищенных информационных систем.

37. Формы контроля состояния технической защиты информации.

38. Государственные стандарты, регламентирующие терминологию в области защиты информации.

39. Средства защиты информации от утечки по техническим каналам.

40. Защита интеллектуальной собственности (определение, содержание процесса защиты, проблемы).

41. Моделирование как основной метод, используемый при разработке и принятии управленческих решений по информационной безопасности организации (предприятия, фирмы).

42. Информационно-аналитические средства, используемые при разработке и принятии решения по информационной безопасности организации (предприятия, фирмы).

43. Основные этапы разработки управленческого решения по информационной безопасности организации.

44. Информационная безопасность процесса принятия управленческого решения в организации.

45. Особенности обеспечения информационной безопасности аэропорта.

46. Особенности обеспечения информационной безопасности полета воздушного судна.

47. Перечислите и раскройте основные принципы обеспечения информационной безопасности предприятия (организации).

48. Информационная безопасность и защита интеллектуальной собственности.

49. Сущность и содержание мероприятий по комплексной специальной проверке помещений.

50. Сущность и содержание основных методов криптографического преобразования информации.

51. Особенности обеспечения информационной безопасности полета воздушного судна.

52. Особенности обеспечения информационной безопасности аэропорта.

53. Стандарт ISO/IEC 15408, ISO/IEC 27000.

54. Стандарты серии BS 7799, Cobit 5.

55. Стандарт BSI 100-1, BSI 100-3.

56. Стандарт BS 1199-1 Code of Practice for Information Security Management (Свод правил по управлению ИБ).

5 РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА И ИНТЕРНЕТ-РЕСУРСЫ

а) основная литература

1. Родионов М.А. Организация бизнес-процессов обеспечения информационной безопасности управления авиапредприятиями. М., МГТУ ГА, 2018.

2. Баранова Е. Бабаш А. Информационная безопасность и защита. Учебное пособие. РИОР, Инфра-М. 2017. 324 с. URL: https://play.google.com/store/books/.

3. Родичев Ю. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. Питер. 2017. 256 с. URL: https://play.google.com/store/books/.

4. Информационный менеджмент: Учебник / Под ред. Н.М. Абдикеева.- М.: ИНФРА-М, 2014, ЭБС Знаниум.

5. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - М.: Национальный Открытый Университет «ИНТУИТ», 2016. https://play.google.com/store/books/.

б) дополнительная литература

6. И. Л. Бачило. Информационное право: учебник / - 3-е изд., перераб. и доп. - М.: Издательство Юрайт; 2015. https://play.google.com/store/books/.

7. Информационные технологии в менеджменте (управлении): учебник и практикум для академического бакалавриата / под общ. ред. Ю. Д. Романовой. - М.: Издательство Юрайт, 2016. https://play.google.com/store/books/.

8. Куняев Н.Н., Правовое обеспечение национальных интересов Российской Федерации в информационной сфере. М.: Логос. 2015. https://play.google.com/store/books/.

9. Нестеров С. Основы информационной безопасности. Учебное пособие. М. Лань. 2016. 324 с. https://play.google.com/store/books/.

Список нормативных правовых документов

1. Конституция Российской Федерации. // Информационно-правовая система «ГАРАНТ». 2018.

2. Федеральный закон Российской Федерации «О безопасности» № 390-ФЗ от 28 декабря 2010 г. // Российская газета, 2010, № 295.

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ “Об информации, информационных технологиях и о защите информации”. // Информационно-правовая система «ГАРАНТ». 2018.

4. Федеральный закон от 27 июля 2006 г. № 152-ФЗ “О персональных данных”. // Информационно-правовая система «ГАРАНТ». 2018.

5. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи». // Информационно-правовая система «ГАРАНТ». 2018.

6. Федеральный закон “Об участии в международном информационном обмене” от 4 июля 1996 г. № 85-ФЗ. // Информационно-правовая система «ГАРАНТ». 2018.

7. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".// Информационно-правовая система «ГАРАНТ». 2018.

8. Стратегия национальной безопасности Российской Федерации. Указ Президента Российской Федерации от 31.12.2015 г. № 683. // Информационно-правовая система «ГАРАНТ». 2019.

9. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5.12.2016 № 646. // Информационно-правовая система «ГАРАНТ». 2019.

10. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27013-2014 "Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и

ИСО/МЭК 20000-1" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 16 сентября 2014 г. № 1084-ст). // Информационно-правовая система «ГАРАНТ». 2018.

11. ГОСТ 34.201-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем". // Информационно-правовая система «ГАРАНТ». 2018.

12. ГОСТ 34.602-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы" (Information technology. Set of standards for automated systems. Technical directions for automated system making). // Информационно-правовая система «ГАРАНТ». 2018.

13. РД 50-34.698-90 "Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов". // Информационно-правовая система «ГАРАНТ». 2019.

14. ISO/IEC 15408-1:2009 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель" (Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model).

15. ISO/IEC 15408-2:2008 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности" (Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components).

16. ISO/IEC 15408-3:2008 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования к обеспечению защиты".

17. ISO/IEC 27001:2013 "Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (Information technology - Security techniques - Information security management systems - Requirements).

18. ISO/IEC 27002:2013 "Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации" (Information technology - Security techniques - Code of practice for information security controls).

19. ISO/IEC 27003:2010 "Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности" (Information technology - Security techniques - Information security management system implementation guidance).

20. ISO/IEC 27004:2009 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения" (Information technology - Security techniques - Information security management - Measurement).

21. ISO/IEC 27005:2011 "Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности" (Information technology - Security techniques - Information security risk management).

22. ISO/IEC 27033-1:2009 "Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции" (Information technology - Security techniques - Network security - Part 1: Overview and concepts).

23. ISO/IEC 18028-4:2005 "Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 4. Обеспечение безопасности удаленного доступа" (Information technology - Security techniques - IT network security - Part 4: Securing remote access).

24. ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования". // Информационно-правовая система «ГАРАНТ». 2018.

25. ITU-T X.842 "Информационные технологии. Методы защиты. Руководящие указания по применению и управлению службами доверенной третьей стороны" (Information technology - Security techniques - Guidelines for the use and management of trusted third party services).

Интернет-ресурсы:

- www.mstuca.ru - электронные ресурсы Университета - электронные версии пособий, методических разработок по всем видам учебной работы;
- http://www.e-xecutive.ru/ - Сообщество менеджеров;
- http://www.mlgvs.ru/library.html#search - Центральная нормативно-методическая библиотека ГА;
- http://www.favt.ru/ - Федеральное агентство воздушного транспорта;
- http://www.itsec.ru/our_news.php - портал Информационная безопасность;
- http://garant.ru/ - Правовая система ГАРАНТ;
- http://consultant.ru/ - Правовая система Консультант Плюс.