Введение

Пособие разработано в соответствии с рабочей программой дисциплины “Информационная безопасность” и включает в себя: методические рекомендации по изучению дисциплины, список рекомендуемой учебной литературы, тематику практических занятий, тесты для текущего контроля усвоения материала студентами, примерные вопросы для подготовки к зачету и глоссарий.

1. Учебный план дисциплины

Дисциплина “Информационная безопасность” изучается на 2 курсе.

Формы контроля: 2 курс – итоговый зачет по дисциплине.

Объем аудиторных занятий:

лекционные занятия – 32 часа; практические занятия – 32 часа.

Самостоятельная работа студентов: 80 часов.

2. Основные сведения о дисциплине

Дисциплина “Информационная безопасность” является одной из важных для обучения по направлению подготовки “Менеджмент”, профилю подготовки “Менеджмент организации”.

Цель освоения дисциплины:

Целью освоения дисциплины “Информационная безопасность” является формирование у студентов основы знаний в области теоретических основ информационной безопасности, обучение студентов диагностике информационных угроз и опасностей, возникающих при управлении предприятием, методологии предотвращения и нейтрализации последствий реализации информационных угроз и опасностей, комплексному обеспечению информационной безопасности.

Знание материалов курса позволит специалисту более эффективно решать основные задачи управления на основе комплексного подхода в условиях потенциально возможных или реально существующих информационных угроз в экономике, ориентируясь на повышение эффективности и интенсификации производства по всем направлениям деятельности. Дисциплина играет профессионально-ориентирующую роль, предполагающую получение практических навыков, связанных с реализацией функций обеспечения информационной безопасности организации.

Задачи изучения дисциплины (необходимый комплекс знаний и умений):

В результате изучения дисциплины студенты должны:

Иметь представление:

- о сущности и социальной значимости вопросов обеспечения информационной безопасности организации;
- о причинах возникновения информационных угроз и опасностей и их значении в социально-экономическом развитии;
- о специфике обеспечения информационной безопасности предприятия в условиях современного российского рынка;

- роли соответствующих должностных лиц в обеспечении информационной безопасности организации.

Знать:

- основные понятия и определения теории информационной безопасности;
- основы российского законодательства и международного законодательства в области информационной безопасности;
- принципы и методы анализа информационных угроз и опасностей в организациях;
- современные подходы российских и зарубежных специалистов по обеспечению информационной безопасности организации;
- направления работы государственных органов в области обеспечения информационной безопасности.

Уметь:

- выявлять основные факторы, влияющие на процессы обеспечения информационной безопасности предприятия;
- осуществлять анализ состояния информационной безопасности предприятия;
- принимать рациональные управленческие решения по обеспечению информационной безопасности предприятия в различных условиях обстановки.

Иметь опыт:

- практического применения принципов и методов анализа угроз и опасностей, разработки и принятия управленческих решений в области информационной безопасности.
- организации работы подразделения информационной безопасности на основе современной концепции менеджмента.

3. Рекомендуемая литература

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

2. Стратегия национальной безопасности Российской Федерации до 2020 года: Указ Президента РФ от 12 мая 2009 г. № 537.

3. Доктрина информационной безопасности Российской Федерации: Указ Президента РФ от 9 сентября 2000 г. № 1895.

4. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. - СПб., 2003.

5. Кутузов В.И., Раимова А.Т. Основы информационного законодательства. - М., 2004.

6. Панкратов В.Н. Защита от психологического манипулирования. - М., 2004.

7. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. - М., 2004.

8. Родионов М.А. Методологические аспекты информационного аудита в менеджменте предприятия //Научный вестник МГТУ ГА. - 2010. - № 156.

9. Садердинов А.А. и др. Информационная безопасность предприятия. - М., 2004.

10. Семкин С.Н. и др. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие. - М., 2005.

11. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - СПб., 2004.

12. Ярочкин В.И. Информационная безопасность. - М., 2004.

4. Электронный адрес кафедры для консультаций

kafmen@ mstuca.aero - по этому адресу можно задать вопрос и, оставив свой электронный адрес, получить письменный ответ.

5. Структура дисциплины

Дисциплина изучается на 2 курсе. При этом прорабатываются 16 тем, сдается итоговый зачет по курсу. Распределение часов осуществляется согласно таблице.

Распределение часов курса

№ п.п.	Наименование тем и разделов	Количество аудиторных часов	В том числе	
			Лекции	ПЗ
1	**2**	**3**	**4**	**5**
1	**Раздел 1. Теоретические положения информационной безопасности**	28	14	14
	Тема 1. Информационная безопасность как составная часть комплексной безопасности и необходимое условие эффективного менеджмента организации	4	2	2
	Тема 2. Основные понятия и определения, сущность и содержание информационной безопасности	4	2	2
	Тема 3. Угрозы информационной безопасности предприятия в условиях современной рыночной экономики	4	2	2
	Тема 4. Нормативное правовое обеспечение информационной безопасности организации	4	2	2
	Тема 5. Особенности обеспечения информационной безопасности в различных сферах жизнедеятельности	4	2	2
	Тема 6. Применение методов системных исследований при анализе процессов обеспечения информационной безопасности	4	2	2
	Тема 7. Риски и эффективность обеспечения информационной безопасности	4	2	2

2	**Раздел 2. Подготовка и проведение мероприятий по обеспечению информационной безопасности предприятия**	36	18	18
	Тема 8. Основы обеспечения информационной безопасности предприятия	2	2	-
	Тема 9. Концепция информационной безопасности организации	6	2	4
	Тема 10. Организация обеспечения информационной безопасности предприятия	6	2	4
	Тема 11. Информационно-аналитическое обеспечения управленческой деятельности по обеспечению информационной безопасности организации	4	2	2
	Тема 12. Информационный аудит организации	2	2	-
	Тема 13. Информационно-техническая безопасность организации	2	2	-
	Тема 14. Методы, способы и средства защиты информации в современных автоматизированных информационных системах	6	2	4
	Тема 15. Информационно-психологическая безопасность организации	2	2	-
	Тема 16. Методы, способы и приемы информационно-психологической защиты должностных лиц организации	6	2	4
3	**Всего часов на освоение учебного материала**	**64**	**32**	**32**

6. Учебная программа дисциплины

Раздел 1. Теоретические положения информационной безопасности

Тема 1. Информационная безопасность как составная часть комплексной безопасности и необходимое условие эффективного менеджмента организации (лекция - 2 часа, практическое занятие - 2 часа)

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.

Литература: [1,2,3,4,9,12]

Центральные вопросы: информация, информационное общество, комплексная безопасность, “стратегия непрямых действий”.

Вопросы:

1. Дайте определение понятию информация.
2. Каковы особенности информационного этапа развития современной цивилизации?
3. В чем суть информационной безопасности с позиций современного менеджмента?
4. Раскройте историю возникновения и основные положения “стратегии непрямых действий в бизнесе”.

Тема 2. Основные понятия и определения, сущность и содержание информационной безопасности (лекция - 2 часа, практическое занятие - 2 часа)

Основные понятия и определения теории информационной безопасности в соответствии с действующими нормативными правовыми документами Российской Федерации и международным правом, а также современными научными взглядами. Цели, задачи, направления, составные части, закономерности и принципы обеспечения информационной безопасности.

Литература: [1,2,3,4,9,11,12]

Центральные вопросы: информационная безопасность, обеспечение информационной безопасности, закономерность, принципы, нормативная правовая база, цель, задачи.

Вопросы:

1. Дайте определение и раскройте содержание понятий «информационная безопасность» и «информационный ресурс».
2. Раскройте цели и задачи информационной безопасности.

3. Перечислите и раскройте содержание основных принципов обеспечения информационной безопасности.

4. Перечислите и раскройте составные части и направления обеспечения информационной безопасности.

Тема 3. Угрозы информационной безопасности предприятия в условиях современной рыночной экономики (лекция - 2 часа, практическое занятие - 2 часа)

Существующие подходы к построению классификации угроз информационной безопасности на различных уровнях управления. Сравнительный анализ возможностей по нейтрализации угроз информационной безопасности для современных предприятий России и развитых зарубежных стран. Модели прогнозирования и нейтрализации угроз информационной безопасности и их применение.

Литература: [2,3,4,6,7,11,12]

Центральные вопросы: угрозы, опасности, прогнозирование, предотвращение, нейтрализация информационных угроз.

Вопросы:

1. Классифицируйте основные угрозы информационной безопасности.

2. Раскройте содержание основных угроз информационной безопасности для современных российских предприятий.

3. Дайте сравнительную характеристику состояния вопросов обеспечения информационной безопасности в экономической области в Российской Федерации и в наиболее развитых странах.

4. Раскройте основные подходы к прогнозированию и нейтрализации угроз информационной безопасности предприятия.

Тема 4. Нормативное правовое обеспечение информационной безопасности организации (лекция - 2 часа, практическое занятие - 2 часа)

Структура нормативного правового обеспечения Российской Федерации в области информационной безопасности. Международная нормативная правовая база по вопросам информационной безопасности. Международные стандарты обеспечения информационного обмена. Структура внутреннего нормативного правового обеспечения информационной безопасности в организации. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке.

Литература: [1,2,3,5,12]

Центральные вопросы: Окинавская хартия глобального информационного общества, доктрина информационной безопасности Российской Федерации, стандарты информационной безопасности, внутреннее и внешнее нормативное правовое поле организации.

Вопросы:

1. Раскройте наиболее важные положения основных нормативных правовых документов в области информационной безопасности в Российской Федерации.

2. Дайте краткую характеристику основных международных нормативных правовых документов в области информационной безопасности.

3. Перечислите и охарактеризуйте наиболее часто используемые отечественные и зарубежные стандарты информационной безопасности.

4. Раскройте содержание основных разрабатываемых в организации документов по вопросам информационной безопасности.

Тема 5. Особенности обеспечения информационной безопасности в различных сферах жизнедеятельности (лекция - 2 часа, практическое занятие - 2 часа)

Специфика информационных угроз, особенности решения вопросов обеспечения информационной безопасности в различных сферах жизнедеятельности, а также бизнес-процессах. Субъекты, объекты, цели и задачи, механизмы обеспечения информационной безопасности. Защита интеллектуальной собственности. Роль и место вопросов обеспечения информационной безопасности в ходе реализации Федеральных целевых программ в области информационных технологий.

Литература: [2,3,4,12]

Центральные вопросы: механизмы обеспечения информационной безопасности, защита интеллектуальной собственности, защита персональных данных, Федеральные целевые программы в области информационных технологий.

Вопросы:

1. Раскройте особенности информационных угроз в различных сферах жизнедеятельности.

2. Охарактеризуйте специфику информационных угроз в сфере бизнеса.

3. Перечислите основные механизмы обеспечения информационной безопасности, раскройте их содержание.

4. Раскройте состояние вопроса защиты интеллектуальной собственности в Российской Федерации.

Тема 6. Применение методов системных исследований при анализе процессов обеспечения информационной безопасности (лекция - 2 часа, практическое занятие - 2 часа)

Основные положения современной теории системных исследований. Методология применения системного подхода при анализе процессов обеспечения информационной безопасности, соотношение гуманитарных, естественнонаучных и технических аспектов.

Влияние структурных и функциональных особенностей системы управления организации на процессы обеспечения ее информационной безопасности.

Литература: [4,8,12]

Центральные вопросы: информационная система, системный поход, структура, функции, процессы обеспечения информационной безопасности.

Вопросы:

1. Перечислите основные направления современных системных исследований, раскройте их содержание.
2. Изложите содержание системного подхода применительно к процессам обеспечения информационной безопасности.
3. Перечислите основные факторы, влияющие на процессы обеспечения информационной безопасности организации (предприятия, фирмы).

Тема 7. Риски и эффективность обеспечения информационной безопасности (лекция - 2 часа, практическое занятие - 2 часа)

Этапы алгоритма анализа и оценки информационных рисков. Основные направления управления информационными рисками. Оценка эффективности мероприятий по обеспечению информационной безопасности. Система показателей и критериев оценки эффективности. Анализ возможностей использования различных методов математического моделирования при исследовании проблем обеспечения информационной безопасности.

Литература: [7,10,12]

Центральные вопросы: содержание понятия риска, виды финансово-экономических рисков, информационные риски, методы уменьшения потерь от рисков при обеспечении информационной безопасности.

Вопросы:

1. Перечислите основные этапы анализа и оценки информационных рисков, раскройте их содержание.
2. Раскройте методы снижения рисков в антикризисном менеджменте.
3. Дайте определение понятию “эффективность мероприятий по обеспечению информационной безопасности”. Как оно соотносится с понятием риска?

Раздел 2. Подготовка и проведение мероприятий по обеспечению информационной безопасности предприятия

Тема 8. Основы обеспечения информационной безопасности предприятия (лекция - 2 часа)

Роль и место системы обеспечения информационной безопасности в работе организации (предприятия, фирмы). Анализ результатов и затрат различных видов ресурсов на обеспечение информа-

ционной безопасности. Основные этапы процесса обеспечения информационной безопасности предприятия и их содержание.

Литература: [8,10,12]

Центральные вопросы: комплексная безопасность предприятия, информационная безопасность предприятия, модель системы управления, информационная модель предприятия, система информационной безопасности предприятия.

Вопросы:

1. Перечислите и кратко охарактеризуйте основные этапы процесса обеспечения информационной безопасности предприятия.
2. Изложите содержание этапа разработки информационной модели предприятия.
3. Какими методами осуществляется анализ результатов и затрат различных видов ресурсов на обеспечение информационной безопасности.

Тема 9. Концепция информационной безопасности организации (лекция - 2 часа, практическое занятие - 4 часа)

Роль и место Концепции информационной безопасности в процессе разработки, создания и функционирования системы информационной безопасности организации, основные требования к ней. Основные разделы Концепции информационной безопасности предприятия и их содержание. Документы, практически реализующие Концепцию информационной безопасности на предприятии. Содержание руководства по обеспечению информационной безопасности в организации. Создание защищенного документооборота в организации.

Литература: [4,9,12]

Центральные вопросы: Концепция информационной безопасности предприятия, способы и средства обеспечения информационной безопасности, защищенный документооборот в организации.

Вопросы:

1. Что такое Концепция информационной безопасности организации.
2. Перечислите и кратко охарактеризуйте основные разделы Концепции информационной безопасности предприятия.
3. Изложите содержание одного из разделов Концепции информационной безопасности предприятия (конкретное предприятие и этап - по выбору студента, при согласовании с преподавателем).

Тема 10. Организация обеспечения информационной безопасности предприятия (лекция - 2 часа, практическое занятие - 4 часа)

Основные этапы процесса организации мероприятий по обеспечению информационной безопасности на предприятии. Органы обес-

печения информационной безопасности организации: состав, структура и функции. Порядок и особенности действий должностных лиц по вопросам обеспечения информационной безопасности в различных условиях обстановки.

Литература: [10,11,12]

Центральные вопросы: функции органов управления предприятием по обеспечению информационной безопасности, служба информационной безопасности, функциональные обязанности должностных лиц по обеспечению информационной безопасности.

Вопросы:

1. Раскройте роль и место процесса организации в общем процессе управления информационной безопасностью предприятия.
2. Перечислите и кратко охарактеризуйте основные этапы процесса организации мероприятий по обеспечению информационной безопасности предприятия.
3. Изложите состав, структуру и функции органов обеспечения информационной безопасности предприятия (на конкретном примере - по выбору студента, по согласованию с преподавателем).
4. Расскажите порядок и особенности действий должностных лиц по вопросам обеспечения информационной безопасности в различных условиях обстановки на выбранном предприятии.

Тема 11. Информационно-аналитическое обеспечение управленческой деятельности по обеспечению информационной безопасности организации (лекция - 2 часа, практическое занятие - 2 часа)

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

Литература: [7,10,12]

Центральные вопросы: процесс принятия управленческих решений по обеспечению информационной безопасности, информационно-аналитическая деятельность менеджеров по безопасности, инструментарий для информационно-аналитического обеспечения процессов принятия управленческих решений по обеспечению информационной безопасности предприятия.

Вопросы:

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

2. Почему для современной информационно-аналитической деятельности по обеспечению информационной безопасности необходима инструментальная поддержка?

3. Какие существуют средства инструментальной поддержки процесса принятия управленческих решений по обеспечению информационной безопасности? Охарактеризуйте основные особенности используемых при этом моделей и задач.

Тема 12. Информационный аудит организации (лекция - 2 часа)

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

Литература: [7,8,9,11]

Центральные вопросы: информационный аудит, информационные риски, информационная санация.

Вопросы:

1. В чем состоит необходимость осуществления информационного аудита на предприятии?

2. Дайте краткую характеристику нормативной правовой базы информационного аудита для российских предприятий.

3. Перечислите и раскройте содержание основных видов информационного аудита.

Тема 13. Информационно-техническая безопасность организации (лекция - 2 часа)

Демаскирующие признаки информационных объектов. Органы, принципы, методы, способы и средства добывания информации. Технические каналы утечки информации. Способы и средства предотвращения утечки информации. Угрозы и объекты обеспечения информационно-технической безопасности, принципы ее обеспечения. Технология процесса обеспечения информационно-технической безопасности организации. Контроль состояния технической защиты информации.

Литература: [9,11,12]

Центральные вопросы: технические каналы утечки информации, демаскирующие признаки, комплексная техническая проверка помещений.

Вопросы:

1. Раскройте роль и место информационно-технической безопасности в работе предприятия.

2. Перечислите и дайте краткую характеристику техническим каналам уточки информации.

3. Расскажите об основных угрозах и объектах обеспечения информационно-технической безопасности на предприятии.

4. Раскройте основные принципы информационно-технической защиты.

Тема 14. Методы, способы и средства защиты информации в современных автоматизированных информационных системах (лекция - 2 часа, практическое занятие - 4 часа)

Анализ способов нарушений информационной безопасности в современных автоматизированных информационных системах и их таксономия. Способы и средства. 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.

Литература: [8,9,10,11,12]

Центральные вопросы: автоматизированная информационная система, защиты информации от утечки по техническим каналам, компьютерные вирусы, криптография, электронная цифровая подпись.

Вопросы:

1. Перечислите и дайте краткую характеристику основных способов и средств информационно-технической защиты на современных предприятиях.

2. Проведите сравнительный анализ средств программно-математического и программно-технического воздействия.

3. Перечислите основные виды вирусов и способы защиты от них.

4. Раскройте основные методы криптографической защиты.

Тема 15. Информационно-психологическая безопасность организации (лекция - 2 часа)

Теоретические основы межличностной коммуникации, 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.

Литература: [6,12]

Центральные вопросы: информационно-психологическое воздействие, убеждение, внушение, психотронное и психотропное воздействие, компьютерные средства информационно-психологического воздействия.

Вопросы:

1. Перечислите основные методы и приемы информационно-психологического воздействия и раскройте их содержание.

2. Перечислите и дайте краткую характеристику основных способов и средств обеспечения информационно-психологической безопасности на современных предприятиях.

3. Раскройте содержание алгоритма информационно-психологической защиты личности.

<u>Тема 16.</u> Методы, способы и приемы информационно-психологической защиты должностных лиц организации (лекция - 2 часа, практическое занятие - 4 часа)

Содержание типовых алгоритмов информационно-психологической защиты: активная защита, пассивная защита. Трансактный анализ и прогноз общения. Методы, способы и приемы информационно-психологической защиты должностных лиц организации в различных условиях обстановки.

Литература: [6,9,12]

Центральные вопросы: алгоритм информационно-психологической защиты, тактика и стратегия информационно-психологической защиты должностных лиц предприятия.

Вопросы:

1. Выберите должностное лицо на предприятии (конкретное предприятие - по выбору студента, по согласованию с преподавателем) и охарактеризуйте основные способы и средства информационно-психологического воздействия на него).

2. Перечислите основные способы и приемы информационно-психологической защиты выбранного должностного лица.

3. Проведите сравнительный анализ способов и приемов информационно-психологической защиты должностных лиц предприятия в различных условиях обстановки.

7. Терминология (понятийный аппарат) дисциплины

Блокирование компьютерной информации - закрытие информации, характеризующееся недоступностью её использования по прямому назначению со стороны законного пользователя, собственника или владельца.

Доступ к информации – ознакомление с информацией, её обработка (в частности, копирование), модификация, уничтожение.

Идентификатор доступа – уникальный признак объекта или субъекта доступа.

Идентификация – присвоение объектам и субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность организации – состояние защищённости информационной среды организации, обеспечивающее её формирование, использование и развитие.

Информационная система - комплекс, включающий вычислительное и коммуникационное оборудование, программное обеспечение, лингвистические средства и информационные ресурсы, а также системный персонал и обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей.

Информационно-управляющая система - формальная система обеспечения руководителей информацией, необходимой для принятия решений.

Информация - сведения о лицах, предметах, фактах, событиях, явлениях или процессах, независимо от формы их представления. Информация необходима каждому как условие и как средство существования человека в обществе. И поэтому также нуждается в защите, как среда обитания, пища и все остальные элементы жизнедеятельности. Под охраняемой законом информацией следует понимать информацию, изъятую из открытого оборота на основании закона, иного нормативного правового акта, а также правил внутреннего распорядка, основанных на указанных правовых актах.

Контроль - процесс, обеспечивающий достижение организацией поставленных целей.

Конфиденциальная информация – информация, которая требует защиты.

Конфиденциальность – свойство информации, состоящее в том, что информация не может быть получена неавторизованным пользователем во время ее хранения, обработки и передачи.

Копирование компьютерной информации – это воспроизводство информации в любой материальной форме.

Косвенные факторы окружающей среды - факторы окружающей среды, которые могут не оказывать немедленного и непосредственного воздействия на деятельность организации, но, тем не менее, влияют на ее деятельность.

Кризис – крайнее обострение противоречий в системе (организации), угрожающее ее жизнестойкости в окружающей среде.

Кризис экономический (от греч. krisis) – резкое ухудшение экономического состояния страны, проявляющееся в значительном спаде производства, нарушении сложившихся производственных связей, банкротстве предприятий, росте безработицы и в итоге – в снижении жизненного уровня, благосостояния населения.

Логическая бомба – резидентная компьютерная программа, которая запускает несанкционированную операцию, когда происходит определенное событие (например, наступает нужная дата).

Многоуровневая защита – защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Модификация информации - внесение в нее любых несанкционированных собственником изменений, обуславливающих ее отличие от той, которую включил в систему и которой владеет собственник информационного ресурса.

Нарушение работы ЭВМ, системы ЭВМ или их сети – это временное или устойчивое создание помех для их функционирования в соответствии с назначением. Оно может быть следствием: поражения компьютерной информации в собственном смысле этого термина; выхода из строя программного обеспечения; нарушения целостности техники, на которой реализовано (установлено) программное обеспечение; повреждение систем связи.

При этом речь идёт не только о затруднениях, непосредственно связанных с манипуляциями в памяти компьютера, но и о помехах, проявляющихся на экране дисплея, при распечатывании и копировании компьютерной информации, а также всякого рода периферийных устройствах и управляющихся датчиках оборудования.

Нарушитель правил разграничения доступа – субъект доступа, который осуществляет несанкционированный доступ к информации.

Незапрограммированное решение - выбор, который приходится делать в новой или неопределенной ситуации с неизвестными факторами воздействия.

Неопределенность внешней среды - функция количества информации по конкретному фактору внешней среды и относительной уверенности в точности такой информации.

Несанкционированный доступ – доступ к информации, который нарушает правила разграничения доступа с использованием штатных средств, предостав-

ляемых средствами вычислительной техники или автоматизированными системами.

Нестабильная внешняя среда - внешнее окружение с высоким уровнем взаимосвязанности факторов, что влечет за собою сложность, подвижность и неопределенность среды.

Обратная связь - реакция на сообщение, которая помогает отправителю, источнику информации определять, воспринята ли им отправленная информация.

Объект доступа – единица информации, доступ к которой регламентируется правилами разграничения доступа. Объектами доступа и контроля является практически всё, что содержит конечную информацию: таблицы, базовые или виртуальные, а также более мелкие элементы данных: столбцы и строки таблиц и даже поля строк, значения. Таблицы базы данных имеют владельца или создателя. Их объединяет ещё и то, что все они для конечного пользователя представляются как таблицы, то есть как нечто именованное, содержащее информацию в виде множества строк и записей одинаковой структуры. Строки таблиц разбиты на поля именованными столбцами.

Организационная структура - логическое соотношение уровней управления и функциональных областей, организованное таким образом, чтобы обеспечить эффективное достижение целей.

Планирование - процесс выбора целей и решений, необходимых для их достижений.

Подразделение - формальная группа в организации, отвечающая за выполнение конкретного набора задач для организации в целом.

Подсистема обеспечения - подразделение организации, которое выполняет функции, необходимые для работы производственной подсистемы.

Полномочия - ограниченное право использовать ресурсы организации и направлять усилия ее сотрудников на выполнение заданий.

Правила разграничения доступа – совокупность правил, регламентирующих права субъектов доступа к объектам доступа.

Преступления в сфере компьютерной информации - умышленно совершенные общественно опасные деяния, запрещённые Уголовным законом под угрозой наказания, в которых объектом преступного посягательства являются общественные отношения по правомерному и безопасному использованию компьютерной информации. В данном случае в качестве предмета преступления будет выступать компьютерная информация или информационные ресурсы, содержащиеся на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети.

Прогнозирование - метод планирования, в котором предсказание будущего опирается на накопленный опыт, текущие предположения относительно будущего и научные методы прогноза.

Программа-вирус - это специально созданная программа, способная размножаться, присоединяться к другим программам (т.е. “заражать” их) и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов, искажение результатов вычислений, засорение или стирание памяти, создание помех в работе ЭВМ, выводить на экран монитора посторонние сообщения, символы и т.д.

Санкционированный доступ – доступ к информации, который не нарушает правил разграничения доступа.

Система обратной связи (в управлении) - любой механизм, обеспечивающий получение данных о результатах, которые могут быть использованы руководителями для корректировки отклонений от намеченного плана.

Троянские кони – это программы, позволяющие выполнять определенные действия без ведома хозяина (пользователя) зараженной системы (в настоящее время получила распространение разновидность «троянцев» которая отсылает своему «хозяину» через Internet различную информацию с зараженного компьютера, включая пароли зарегистрированных пользователей).

Угроза безопасности информационной системы – под ней обычно понимают потенциально возможное событие, действие, процесс или явление, которое может оказать нежелательное воздействие на систему и информацию, которая в ней хранится и обрабатывается. Такие угрозы, воздействуя на информацию через компоненты системы, могут привести к уничтожению, искажению, копированию, несанкционированному распространению информации, к ограничению или блокированию доступа к ней.

Уничтожение компьютерной информации - полная физическая ликвидация информации или ликвидацию таких её элементов, которые влияют на изменение существенных, идентифицирующих информацию признаков.

Физическая безопасность – обеспечение сохранности самого оборудования, предназначенного для функционирования информационной среды, контроль доступа людей к этому оборудованию. Дополнительно сюда может быть включено понятие защиты самих пользователей информационной среды от физического воздействия злоумышленников, а также защиты информации не виртуального характера (твердых копий – распечаток, служебных телефонных справочников, домашних адресов сотрудников, испорченных внешних носителей).

Червь – вредоносная программа, создающая свои многочисленные копии в памяти компьютера и распространяющая их по всей системе, приводя ее в нерабочее состояние. Иногда написанный как отдельный сегмент, такой червь тайно внедряют в главную систему для «забавы» или с целью повреждения или разрушения информации. Термин постепенно уступает понятию «вирус».

8. Темы практических занятий и их объем в часах

№ темы	Наименование практического занятия	Объем в часах
1.	Роль и место информационной безопасности в деятельности организации (предприятия, фирмы)	2
2.	Категориальный аппарат информационной безопасности	2
3.	Классификация угроз информационной безопасности авиа-предприятия	2
4.	Сравнительный анализ отечественной и международной нормативной правовой базы в области информационной безопасности	2
5.	Особенности обеспечения информационной безопасности в социально-политической, экономической, финансовой и экологической сферах	2
6.	Системный подход к обеспечению информационной без-опасности организации (предприятия, фирмы)	2
7.	Анализ существующих подходов к оценке эффективности мероприятий по обеспечению информационной безопасно-сти предприятия	2
9.	Деловая игра “Разработка концепции информационной без-опасности авиапредприятия”	4
10.	Деловая игра “Особенности действий основных должност-ных лиц авиапредприятия по вопросам обеспечения инфор-мационной безопасности в различных условиях обстановки”	4
11.	Особенности информационно-аналитической деятельности на различных этапах принятия управленческого решения по информационной безопасности организации	2
14.	Деловая игра “Обеспечение информационно-технической безопасности предприятия в конкретной ситуации”	4
16.	Деловая игра “Обеспечение информационно-психологической безопасности предприятия в конкретной ситуации”	4
	ИТОГО	32

9. Тесты для проведения рубежного контроля знаний

Выберите один или несколько верных вариантов ответа:

1. Какой стандарт определяет требования к управлению информационной безопасностью?

а) ГОСТ Р 15408;

б) ГОСТ ИСО/МЭК 27001;

в) ГОСТ ИСО/МЭК 17799.

2. Три основных требования к обеспечению безопасности информации:

а) неприкосновенность, целостность, устойчивость;

б) публичность, доступность, защищенность;

в) тайна, охрана, зашифрованность;

г) доступность, целостность, конфиденциальность;

д) охрана, устойчивость, защищенность.

3. Укажите юридически корректный синоним термина “компьютер”:

а) сервер;

б) процессор;

в) системный блок;

г) ЭВМ;

д) вычислитель.

4. В каком режиме авторское право охраняет права на программу для ЭВМ?

а) как изобретение;

б) как способ вычислений;

в) как коммерческую тайну;

г) а)+в);

д) как аудиовизуальное произведение;

е) как алгоритм;

ж) как права на носитель, на котором программа написана;

з) как научный труд;

и) е)+з);

к) все перечисленные варианты.

5. К методам нейтрализации возможных последствий выявленных рисков относятся:

а) избегание, противодействие, передача, принятие;

б) сокрытие, перекладывание на партнеров;

в) страхование, аутсорсинг, резервирование;

г) ни один из перечисленных вариантов.

6. На каком уровне утверждается Концепция информационной безопасности предприятия?

а) на уровне вышестоящего или надзирающего органа;

б) на уровне начальника службы информационной безопасности;

в) на уровне технического директора;

г) на уровне руководителя функционального подразделения;

д) на уровне высшего руководства предприятия;

е) в зависимости от обстановки;

ж) это не имеет значение.

7. На кого возлагается ответственность за выбор подлежащих защите ресурсов предприятия?

а) на руководителей подразделений, в которых находятся данные ресурсы;

б) на службу информационной безопасности;

в) на конкретных исполнителей, использующих данные ресурсы;

г) на вышестоящие или надзирающие органы;

д) верны все вышеперечисленные варианты ответов;

е) данный вопрос не определен в стандарте по информационной безопасности.

8. Имеет ли право администратор информационной системы предприятия передавать ответственность и полномочия по обеспечению информационной безопасности поставщику услуг?

а) да;

б) нет;

в) данный вопрос не определен в стандарте по информационной безопасности;

г) полномочия – нет, ответственность – да;

д) полномочия – да, ответственность – нет;

е) данный вопрос решается в зависимости от сложившейся ситуации.

9. Если пароль может состоять только из строчных латинских букв (их 26), а также цифр (их 10) и имеет длину 10 символов, то сколько имеется вариантов данного пароля?

а) 26^{10};

б) 10^{26};

в) $26^{10} + 10^{10}$;

г) $26 * 10 + 10 * 10$;

д) $26 * 10$;

е) 36^{2};

ж) $26^{2} + 10^{2}$;

з) ни один из вариантов не является правильным.

10. В какой стране доступ в Интернет полностью запрещен для всех граждан?

а) Узбекистан;

б) Тунис;

в) Сирия;

г) Мьянма;

д) Мальдивы;

е) Куба;

ж) КНДР;

з) Иран;

и) такой страны нет.

11. Каким законным способом может быть ограничено право на тайну переписки в России?

а) по решению оператора связи;

б) по решению владельца средств связи;

в) по добровольному согласию гражданина;

г) по решению следователя;

д) по решению суда;

е) по решению прокурора;

ж) не может быть ограничено ни в каких случаях;

з) ни один из вышеперечисленных ответов не является правильным.

12. Нужно ли регистрировать инциденты безопасности?

а) не нужно;

б) нужно, кроме внешних инцидентов;

в) нужно, кроме внутренних инцидентов;

г) нужно все инциденты;

д) на усмотрение руководителя службы информационной безопасности предприятия;

е) в зависимости от вида инцидента.

13. Кто должен подписать заявление в правоохранительные органы по поводу инцидента безопасности в информационной системе предприятия?

а) системный администратор;

б) руководитель службы информационной безопасности;

в) руководитель предприятия;

г) исполнитель, который зарегистрировал инцидент;

д) все перечисленные должностные лица;

е) не имеет значения.

14. Законодательство какой страны применяется к действиям пользователя в сети Интернет?

а) страны, на территории которой находится пользователь;

б) страны, на территории которой находится сервер;

в) страны, на территории которой зарегистрирован провайдер пользователя;

г) страны, на территории которой находится истец;

д) США;

е) любой страны, по выбору истца;

ж) страны, обозначенной в договоре между пользователем и провайдером;

з) в соответствии с интернет - законодательством;

и) в зависимости от того, чьи интересы затронуты;

к) не применяется никакое законодательство;

л) применяется только международное законодательство.

15. По какому критерию расставляются приоритеты информационных рисков?

а) по вероятности реализации угроз;

б) по величине возможного ущерба;

в) по стоимости рисков;

г) по времени реализации угроз;

д) по срокам преодоления возможных последствий;

е) по близости к профильной деятельности предприятия.

16. Для эффективной защиты база антивируса должна обновляться:

а) ежедневно;

б) еженедельно;

в) ежемесячно;

г) ежеквартально;

д) после каждого обнаруженного вируса.

17. Решение каких задач информационной безопасности обеспечивает электронная цифровая подпись?

а) конфиденциальность;

б) устойчивость

в) доступность;

г) целостность;

д) а) + б) + в);

е) а) + б) + г);

ж) а) + в) +гв);

е) б) + в) + г).

18. В какой орган субъект персональных данных вправе обратиться для обжалования действий оператора, который обрабатывает его персональные данные с нарушением?

а) в ФСБ;

б) в полицию;

в) в Гостехкомиссию;

г) в ФСТЭК;

д) в Россвязьнадзор;

е) Уполномоченному по правам человека в Российской Федерации;

ж) в Роскомстат;

з) в суд по месту жительства.

19. Следует ли скрывать ход и результаты расследования инцидента безопасности?

а) нет, эта информация должна быть общедоступной;

б) да, это конфиденциальная информация;

в) следует распространить эту информацию как можно шире.

20. Что из перечисленного полезно сделать, если по электронной почте от знакомого получено сообщение, содержащее вирус?

а) переслать сообщение с вирусом системному администратору;

б) переслать сообщение с вирусом в правоохранительные органы;

в) отослать сообщение с вирусом обратно;

г) предупредить отправителя о вирусе.

10. Примерные вопросы для подготовки к зачету

1. Основные понятия и определения теории информационной безопасности организации (предприятия, фирмы).

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

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

4. Сущность и содержание информационно-технической безопасности организации (предприятия, фирмы).

5. Сущность и содержание информационно-психологической безопасности организации (предприятия, фирмы).

6. Информационно-аналитическое обеспечение в системе информационной безопасности.

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

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

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

10. Основные направления реализации Федеральной целевой программы “Электронная Россия” и информационная безопасность (в части, касающейся предприятий, фирм).

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

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

13. Система обеспечения информационной безопасности России.

14. Система информационной безопасности региона, ведомства, муниципального образования.

15. Концепция информационной безопасности организации.

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. Содержание процессов лицензирования и сертификации.

20. Система информационной безопасности организации (предприятия).

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

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

23. Разрабатываемые на предприятии документы по вопросам информационной безопасности и требования по их корректировке.

24. Создание и обеспечение защищенного документооборота в организации.

25. Информационный аудит организации (предприятия).

26. Анализа информационных рисков и управление ими.

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

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

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

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

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

32. Понятие и содержание криптографии, основные методы.

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

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

35. Алгоритмы информационно-психологической защиты.

36. Использование интернет-технологий и обеспечение информационной безопасности.

37. Основные технологии построения защищенных информационных систем.

38. Формы контроля состояния технической защиты информации.

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

40. Средства защиты информации от утечки по техническим каналам.

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

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

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

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

45. Информационная безопасность процесса принятия управленческого решения в организации.

46. Особенности обеспечения информационной безопасности аэропорта.

47. Особенности обеспечения информационной безопасности полета воздушного судна.

СОДЕРЖАНИЕ