Министерство образования и науки Российской Федерации

Южно-Российский государственный политехнический
университет (НПИ) имени М.И. Платова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

**Методические указания
к лабораторным занятиям
и самостоятельной работе по курсу**

Новочеркасск
ЮРГПУ (НПИ)
2017

УДК 311(076.5)

Рецензент – доктор экон. наук, проф. М.А. Комиссарова

Дулин А.Н., Романенко Е.В.

«Информационная безопасность»: Методические указания к выполнению лабораторных занятий и самостоятельной работы / Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова – Новочеркасск: ЮРГПУ, 2016. – 12 с.

Представлены методические указания к выполнению лабораторных занятий и самостоятельной работы, предназначенных для студентов бакалавриата очной и заочной форм обучения по направлениям 38.03.03 «Управление персоналом», направленности «Экономика труда».

1. ЛАБОРАТОРНЫЕ ЗАНЯТИЯ, ИХ НАИМЕНОВАНИЕ И ОБЪЕМ В ЧАСАХ

№	Наименование тем занятий	Кол-во часов	Кол-во часов (ЗФО)	Форма контроля	Литература
1	Основные виды каналов утечки информации.	3	1	Защита отчета лабораторной работы	7 [3]
2	Классификация угроз безопасности информационных систем.	4	1*		7 [3,4]
3	Виды нарушений информационной безопасности.	3	1		7 [3,4]
4	Правовое регулирование открытых информационных ресурсов.	4	1	Защита отчета лабораторной работы	7 [3,4]
5	Правовая защита информационных ресурсов ограниченного доступа:	4	1		7 [1-4]
6	Классификация угроз информационной безопасности компьютерных систем.	4*	1*	Защита отчета лабораторной работы	7 [3,4,5]
7	Зашита от вирусов: а) основные виды компьютерных вирусов; б) профилактика вирусного заражения; в) антивирусные программы.	4*			7 [1-5]
8	Защита от несанкционированного доступа с помощью стандартных и специализированных программно-технических средств.	4*			7 [3,4,5]

* - Занятия, проводимые в интерактивной форме

ТЕМА ЗАНЯТИЯ №1.
ОСНОВНЫЕ ВИДЫ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Современные информационные технологии разделили судьбу всех прогрессивных технологий XX в. Бесспорно, что широкое внедрение средств компьютерной техники (СКТ) и телекоммуникаций в производственную, хозяйственную, финансовую деятельность предприятий, учреждений, организаций значительно повышает эффективность их работы.

На локальном уровне угроз компьютерной безопасности (например, для помещений, занимаемых учреждением, организацией, предприятием, и раз-

мещенных в них СКТ) выделяют каналы утечки информации, под которыми понимают совокупность источников информации, материальных носителей или среды распространения несущих эту информацию сигналов и средств выделения информации из сигналов или носителей.

Факторы информационных угроз следует рассматривать как потенциальную возможность использования каналов утечки информации. Объективное существование данных каналов утечки предполагает их возможное использование злоумышленниками для несанкционированного доступа к информации, ее модификации, блокированию и иных неправомерных манипуляций, т. е. наличие каналов утечки информации влияет на избрание способа совершения преступления.

Каналы утечки информации непосредственного из СКТ и технические устройства съема такой информации стали использоваться злоумышленниками сравнительно недавно.

Задание: подробно описать все известные каналы утечки информации

ТЕМА ЗАНЯТИЯ №2
КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Все множество потенциальных угроз информационной безопасности по природе их возникновения можно разделить на два класса: естественные (объективные) и искусственные (субъективные).

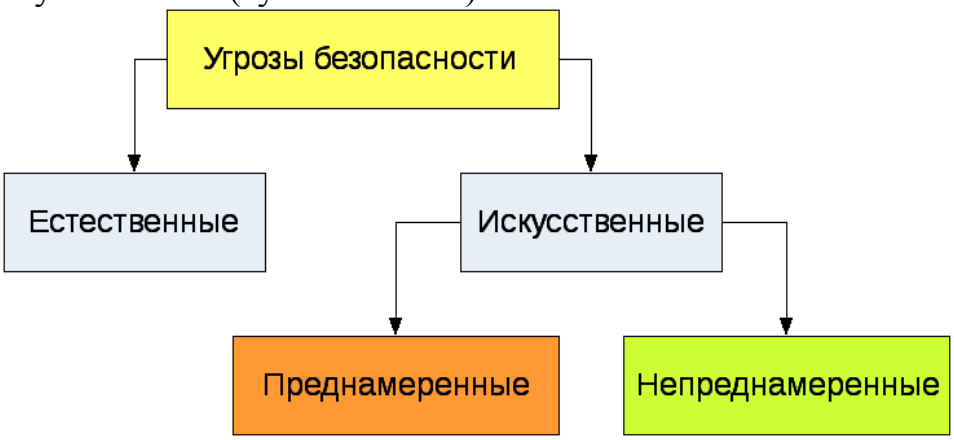

Рисунок - Угрозы безопасности

Естественные угрозы – это угрозы, вызванные воздействиями на автоматизированную систему и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы – это угрозы информационной безопасности, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

1. Непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании автоматизированной системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала.

2. Преднамеренные (умышленные) угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Источники угроз по отношению к автоматизированной системе могут быть внешними или внутренними. Внутренние угрозы реализуются компонентами самой информационной системы – аппаратно-программным обеспечением или персоналом.

Задание: Раскрыть все угрозы безопасности информационных систем

ТЕМА ЗАНЯТИЯ №3
ВИДЫ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организационно-правовые виды нарушений – это нарушения, связанные отсутствием единой согласованной политики компании в сфере защиты информации, невыполнением требований нормативных документов, нарушением режима доступа, хранением и уничтожения информации.

Информационные виды нарушений включают несанкционированное получение полномочий доступа к базам и массивам данных, несанкционированный доступ к активному сетевому оборудованию, серверам доступа, некорректное применение средств защиты и ошибки в управлении ими, нарушения в адресности рассылки информации при ведении информационного обмена.

Физические виды нарушений включают физическое повреждение аппаратных средств автоматизированных систем, линий связи и коммуникационного оборудования, кражи или несанкционированное ознакомление с содержимым носителей информации, хранящихся в неположенных местах, хищение носителей информации, отказы аппаратных средств и др.

К радиоэлектронным видам нарушений относятся такие нарушения, как внедрение электронных устройств перехвата информации, получение информации путем перехвата и дешифрования информационных потоков, дистанционная видеозапись (фотографирование) мониторов, компьютерных распечаток, клавиатуры, навязывание ложной информации в локальных вычислительных сетях, сетях передачи данных и линиях связи.

QA – Несанкционированный доступ и перехват

QD – Изменение компьютерных данных

QF – Компьютерное мошенничество

QR – Незаконное копирование

QS – Компьютерный саботаж

QZ – Прочие компьютерные преступления

QZZ – Иные компьютерные преступления

Данная классификация применяется при отправлении запросов или сообщений о компьютерных преступлениях по телекоммуникационной сети Интерпола. Одним из ее достоинств является введение литеры «Z», отражающей

прочие виды преступлений и позволяющей совершенствовать и дополнять используемую классификацию.

Задание: Раскрыть классификацию, предложенную В.А. Мещеряковым.

ТЕМА ЗАНЯТИЯ №4
ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Задание: Рассмотреть и обсудить следующие вопросы:

1. Понятие и виды открытых информационных ресурсов;
2. Порядок формирования открытых информационных ресурсов и предоставления открытых информационных услуг;
3. Государственное регулирование библиотечного дела;
4. Государственное регулирование архивного дела;
5. Особенности государственного регулирования с банками данных

ТЕМА ЗАНЯТИЯ №5
ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ ОГРАНИЧЕННОГО ДОСТУПА

Задание: Рассмотреть и обсудить следующие вопросы:

1. Понятие и виды информационных ресурсов ограниченного доступа;
2. Порядок формирования информационных ресурсов ограниченного доступа и предоставления информационных услуг ограниченного доступа;

ТЕМА ЗАНЯТИЯ №6 КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Для того чтобы обеспечить эффективную защиту информации, необходимо в первую очередь рассмотреть и проанализировать все факторы, представляющие угрозу информационной безопасности.

Задание: Раскрыть все понятия и закончить предложения

Угроза информационной безопасности КС — это…

По природе возникновения различают: …

По степени преднамеренности проявления угрозы различают: …

По степени воздействия на КС различают: …

По расположению источника угроз: …

По текущему месту расположения информации в КС: …

По непосредственному источнику угроз. Источниками угроз могут быть: …

По цели воздействия на КС: …

По способам реализации угрозы могут осуществляться: …

ТЕМА ЗАНЯТИЯ №7 ЗАЩИТА ОТ ВИРУСОВ:

Задание: Рассмотреть и обсудить следующие вопросы:

1) основные виды компьютерных вирусов;
2) профилактика вирусного заражения;
3) антивирусные программы

ТЕМА ЗАНЯТИЯ №8 ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА С ПОМОЩЬЮ СТАНДАРТНЫХ И СПЕЦИАЛИЗИРОВАННЫХ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ

Задание: Рассмотреть и обсудить следующие вопросы:

1. Признаки компьютерных преступлений.
2. Технические, организационные и программные средства обеспечения сохранности и защиты от несанкционированного доступа
3. Защита носителей информации (исходных документов, лент, картриджей, дисков, распечаток).
4. Выбор надежного оборудования.
5. Разработка адекватных планов обеспечения непрерывной работы и восстановления.
6. Дублирование, мультиплексирование и резервирование офисов.
7. Защита данных от перехвата.

3. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ (СРС)

СРС– темы и разделы тем для самостоятельного изучения, в том числе конспектирование – 33,1 ч. (ЗФО – 86,7 ч.)

№	Наименование тем	Кол-во часов	Кол-во часов (ЗФО)	Литература
1	**Тема 10.** Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации	6,1	15,7	7 [1-3]
2	**Тема 11.** Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обес-	6	15	7 [1-3]

№	Наименование тем	Кол-во часов	Кол-во часов (ЗФО)	Литература
	печения. Правовое двуединство документированных информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации			
3	**Тема 12.** Правомерные методы получения предпринимательской информации, их состав. Законодательные акты, охраняющие вещную собственность на документированную информацию.	5	14	7 [1-3]
4	**Тема 13.** Правовая защита субъектов в области массовой информации, обеспечение гарантий свободы массовой информации. Производственная тайна. Служебная тайна. Профессиональная тайна. Банковская тайна. Тайны личная и семейная.	5	14	7 [1-3]
5	**Тема 14.** Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией. Принципы и формы морального и материального стимулирования ответственного отношения сотрудников к работе с конфиденциальной информацией.	6	14	7 [1-3]
6	**Тема 15.** Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования	5	14	7 [1-3]

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОГО ИЗУЧЕНИЯ И КОНСПЕКТИРОВАНИЯ

Тема 10. Рассмотреть следующие вопросы:

1. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу создания и распространения информации.
2. Правовые механизмы защиты в нормах законов, регулирующих отношения в области формирования информационных ресурсов, продуктов и услуг.
3. Правовые механизмы защиты в нормах законов, регулирующих отношения по поводу права на потребление информации.

Тема 11. Рассмотреть следующие вопросы:

1. Правовые механизмы защиты в нормах законов, регулирующих отношения в области создания и применения информационных систем, информационных технологий и средств их обеспечения.
2. Правовое двуединство документированных информационных ресурсов.
3. Правовые и экономические предпосылки выделения ценной информации.

Тема 12. Рассмотреть следующие вопросы:

1. Правомерные методы получения предпринимательской информации, их состав.
2. Законодательные акты, охраняющие вещную собственность на документированную информацию.

Тема 13. Рассмотреть следующие вопросы:

1. Правовая защита субъектов в области массовой информации, обеспечение гарантий свободы массовой информации.
2. Производственная тайна.
3. Служебная тайна.
4. Профессиональная тайна.
5. Банковская тайна.
6. Тайны личная и семейная

Тема 14. Рассмотреть следующие вопросы:

1. Методы контроля соблюдения персоналом правил работы с конфиденциальной информацией.
2. Принципы и формы морального и материального стимулирования ответственного отношения сотрудников к работе с конфиденциальной информацией

Тема 15. Рассмотреть следующие вопросы:

1. Криптографические средства защиты.
2. Криптографическое преобразование данных.
3. Симметричные и асимметричные методы шифрования.
4. Общая технология шифрования

Экзаменационные вопросы по курсу

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной без-

опасности общества.

4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Охарактеризовать технические каналы несанкционированного доступа к информации.
14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
15. Проанализировать особенности угроз автоматизированным информационным системам.
16. Проанализировать основные направления правовой защиты информации.
17. Определить объекты защиты авторских прав.
18. Назвать основные права автора в отношении его произведения.
19. Дать определение государственной тайны и назвать грифы секретности.
20. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
21. Принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.
22. Основные положения концепции информационной безопасности предприятия.
23. Регламент обеспечения информационной безопасности предприятия.
24. Основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
25. Критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
26. Содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
27. Дать классификацию компьютерных вирусов.
28. Описать основные антивирусные программы.
29. Охарактеризовать основные способы криптографического преобразования

данных.

СРС экз. – самостоятельная работа по подготовке к экзамену - 35,65 ч. (ЗФО – 8,65 ч.)

Контактная внеаудиторная работа

СРС: – групповые консультации в течение семестра – 0,9 ч. (ЗФО – 0,3 ч.)

– групповые консультации перед экзаменом – 2 ч.

СРС экз. – сдача экзамена – 0,35 ч.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Галатенко В. А.Основы информационной безопасности / [Электронный ресурс]. - Интернет-Университет Информационных Технологий - 2006 год - 208 страниц. Режим доступа: http://www.knigofond.ru.
2. Галатенко В. А. Стандарты информационной безопасности / [Электронный ресурс]. - Интернет-Университет Информационных Технологий - 2006 год - 264 страницы. Режим доступа: http://www.knigofond.ru.
3. Анисимов А. А. Менеджмент в сфере информационной безопасности / [Электронный ресурс]. - Интернет-Университет Информационных Технологий - 2009 год - 176 страниц. Режим доступа: http://www.knigofond.ru.
4. Жуков А.Е. Системы блочного шифрования: учебное пособие по курсу «Криптографические методы защиты информации» / [Электронный ресурс]. - Издательство МГТУ им. Н.Э. Баумана - 2013 год - 79 страниц. Режим доступа: http://www.knigofond.ru.
5. Скрипник Д. А. Обеспечение безопасности персональных данных / [Электронный ресурс]. - Интернет-Университет Информационных Технологий - 2011 год - 109 страниц. Режим доступа: http://www.knigofond.ru.
6. – дидактические материалы
7. Слайды и наглядные пособия (расположенные в лабораториях)
8. Комплект вопросов для контроля знаний.
9. http://www.elibrary.ru.

Учебно-методическое издание

Дулин Александр Николаевич
Романенко Елена Валерьевна

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Методические указания
к лабораторным занятиям и самостоятельной работе по курсу

Редактор *Н.А.Юшко*
Подписано в печать
Формат 60х84 $^{1}/_{16}$. Бумага офсетная. Печать цифровая.
Усл. печ. л. Уч.-изд.л. 1,5 . Тираж экз. Заказ .

Южно-Российский государственный политехнический университет
(НПИ) им. М.И. Платова
Редакционно-издательский отдел ЮРГПУ (НПИ)
346428, г. Новочеркасск, ул. Просвещения, 132

Отпечатано в ИД «Политехник»
346428, г. Новочеркасск, ул. Первомайская, 166
idp-npi@mail.ru