ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Кафедра МСИБ

М.А. Буранова, В.В. Пугин

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕДУЩИХ ЗАРУБЕЖНЫХ СТРАНАХ

Учебное пособие к практическим занятиям

Самара

2017

Авторы: М.А. Буранова, В.В. Пугин

УДК 621

Рекомендовано к изданию методическим советом ПГУТИ, протокол № 84 , от 13.07. 2017 г.

Буранова М.А., Пугин В.В.

Б Системы защиты информации в ведущих зарубежных странах: учебное пособие к проведению практических занятий/ М.А. Буранова, В.В. Пугин. – Самара: ПГУТИ, 2017. – 14 с.

Учебное пособие разработано в соответствии с ФГОС ВО по направлениям подготовки 10.05.02, 10.03.01. Предназначено для проведения практических занятий по дисциплине «Системы защиты информации в ведущих зарубежных странах».

ТЕМЫ ЗАНЯТИЙ

1. **Изучение зарубежных технических средств защиты информации**
2. **Изучение зарубежной практики применения алгоритмов криптографической защиты данных**
3. **Государственные органы обеспечения информационной безопасности США**
4. **Государственные органы обеспечения информационной безопасности стран Евросоюза**
5. **Государственные органы обеспечения информационной безопасности в Китайской народной республике**
6. **Изучение информационно-психологической войны и типов информационного оружия**
7. **Изучение международной нормативно-правовой базы по сотрудничеству в области обеспечения информационной безопасности**
8. **Изучение системы международных стандартов информационной безопасности (TCSEC)**
9. **Системы ЗИ в ведущих мировых компаниях**

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1

Изучение зарубежных технических средств защиты информации

Цель работы: изучение зарубежных аналогов российских технических средств, применяемых для защиты информации в государственных учреждениях РФ.

Продолжительность работы – 4 часа.

1. Порядок выполнения работы

Занятие проводится в игровой форме. Группа делится на четыре подгруппы по числу типов технических средств:

1. Средства выявления каналов утечки информации.
2. Средства активной защиты от утечки по техническим каналам.
3. Аппаратные криптографические средства.
4. Досмотровая техника, устройства радиоподавления.

По каждому типу технических средств закрепляется подгруппа студентов. Данная подгруппа проводит сравнительный анализ и выбор наиболее предпочтительного устройства или аппаратно-программного комплекса в зависимости от конкретного задания.

Каждая подгруппа выполняет следующее задание: изучает отечественные и зарубежные средства технической защиты информации по предложенной теме.

Подгруппа делится на три бригады. Первая бригада проводит детальный анализ рынка и выбор технического средства из Российского сегмента. Вторая – из зарубежных аналогов. Третья – осуществляет выбор оптимального решения. На первом занятии первая и вторая бригады должны представить лучшие варианты из своего сегмента и привести доказательства преимуществ своего выбора. Каждая бригада имеет право представления своего решения в любой форме – доклад, презентация и т.д. На следующем занятии третья сторона должна сделать выбор в пользу одного из предложенных решений, предварительно изучив представленные варианты.

Пользуясь электронными и бумажными каталогами технических средств защиты информации в ходе практических занятий, студенту необходимо выбрать наиболее близкие аналоги (зарубежные и отечественные) следующих устройств:

1. Средства выявления каналов утечки информации.
   Примеры отечественных устройств:
   - Многофункциональный поисковый прибор ST-031 «Пиранья».
   - Нелинейный локатор SEL SP-61 «Катран».
2. Средства активной защиты от утечки по техническим каналам.
   Примеры отечественных устройств:
   - Универсальный шумогенератор ГРОМ-ЗИ-4.

- Комплекс виброакустической защиты «Барон».

3. Средства аппаратной криптографии.

   Примеры отечественных устройств:

   - Электронный замок «Соболь-PCI».
   - Межсетевой экран и шифратор IP-потоков «ФПСУ-IP».

4. Досмотровая техника, устройства радиоподавления.

   Примеры отечественных устройств:

   - Подавитель сотовых телефонов «Завеса».
   - Досмотровые металлоискатели ВМ-311, ВМ-611(ПРО).

Следует провести сравнительный анализ технических характеристик, функциональных возможностей и стоимости российских и зарубежных устройств.

2. Форма и содержание докладов

Доклад (в любой форме, можно в виде презентации) должен содержать:

1. Титульный лист.
2. Техническое описания российских или зарубежных средств, представленное в табличном виде. Сравнительный анализ рассмотренных средств.
3. Перечень использованных информационных источников.

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2

Изучение зарубежной практики применения алгоритмов криптографической защиты данных

Цель работы: ознакомление с практикой применения и реализации современных криптографических алгоритмов в ведущих зарубежных странах.

Продолжительность работы - 2 часа.

1. Порядок выполнения работы

В ходе выполнения задания следует оценить уровень обеспечения и реализации современных криптографических алгоритмов в национальных системах защиты информации ведущих зарубежных стран и сравнить с российской практикой. Рассмотреть:

1) алгоритмы симметричного шифрования;
2) алгоритмы асимметричного шифрования;
3) алгоритмы электронной подписи и хэширования.

2. Форма и содержание отчета

Отчет (в любой форме, можно в виде презентации) должен содержать:

1. Титульный лист.
2. Характеристику нормативного обеспечения (законов, стандартов) криптографической защиты в зарубежных странах, аналогов в РФ.
3. Описание наиболее широко используемых криптографических алгоритмов и их программных реализаций в зарубежных странах.
4. Характеристику практики применения криптографических средств в зарубежных странах.
5. Перечень использованных информационных источников.

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №3

Государственные органы обеспечения информационной безопасности США

Цель работы: ознакомление со структурой и функциями государственного аппарата обеспечения информационной безопасности США, правовым регулированием ИБ в США, подготовкой кадров в области защиты информации.

Продолжительность работы - 2 часа.

1. Порядок выполнения работы

За две недели до занятия студентам выдается задание в виде подготовки докладов.

Темы докладов:

1. Современная концепция информационной войны в США.
2. Правовое регулирование информационной безопасности в США.
3. Государственные органы обеспечения национальной безопасности США.
4. Особенности подготовки кадров в области информационной безопасности в США.

2. Форма и содержание докладов

Отчет (в любой форме, можно в виде презентации) должен содержать:

Доклад должен содержать:

1. Титульный лист.
2. Правовые аспекты регулирования деятельности в области информационной безопасности.
3. Подготовка кадров в области информационной безопасности.
4. Характеристики спецслужб, охватывающие основные аспекты их деятельности:
   - актуальные цели и задачи службы;
   - структура и функции службы;
   - реализуемые сейчас и в ближайшем прошлом проекты и достигнутые результаты;
   - взаимодействие с другими спецслужбами и организациями.
5. Перечень использованных информационных источников

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №4

Государственные органы обеспечения информационной безопасности стран Евросоюза

Цель работы: ознакомление со структурой и функциями государственного аппарата обеспечения информационной безопасности стран Евросоюза, правовым регулированием ИБ в странах: Соединённом королевстве Великобритании и Северной Ирландии, в Федеративной республике Германия, во Французской республике, в Швеции, подготовкой кадров в области защиты информации в рассматриваемых странах.

Продолжительность работы - 4 часа.

1. Порядок выполнения работы

За две недели до занятия студентам выдается задание в виде подготовки докладов.

Темы докладов:

1. Состояние проблемы информационной безопасности в странах Евросоюза.
2. Системы защиты информации в Соединённом королевстве Великобритании и Северной Ирландии.
3. Системы защиты информации в Федеративной республике Германия.
4. Системы защиты информации во Французской республике.
5. Системы защиты информации в Швеции.

2. Форма и содержание докладов

Доклад должен содержать:

1. Титульный лист.
2. Характеристики иностранных спецслужб, охватывающие основные аспекты их деятельности:
   - актуальные цели и задачи службы;
   - структура и функции службы;
   - реализуемые сейчас и в ближайшем прошлом проекты и достигнутые результаты;
   - взаимодействие с другими спецслужбами и организациями.
3. Правовые аспекты регулирования деятельности в области информационной безопасности.
4. Подготовка кадров в области информационной безопасности.
5. Перечень использованных информационных источников

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №5

Государственные органы обеспечения информационной безопасности в Китайской народной республике

Цель работы: ознакомление со структурой и функциями государственного аппарата обеспечения информационной безопасности Китайской народной республики (КНР), правовым регулированием ИБ в КНР, подготовкой кадров в области защиты информации.

Продолжительность работы - 2 часа.

1. Порядок выполнения работы

За две недели до занятия студентам выдается задание в виде подготовки докладов.

Темы докладов:

1. Современная концепция информационной войны в КНР.
2. Правовое регулирование информационной безопасности в КНР.
3. Государственные органы обеспечения национальной безопасности КНР.
4. Особенности подготовки кадров в области информационной безопасности в КНР.

2. Форма и содержание докладов

Доклад должен содержать:

1. Титульный лист.
2. Правовые аспекты регулирования деятельности в области информационной безопасности.
3. Подготовка кадров в области информационной безопасности.
4. Характеристики спецслужб, охватывающие основные аспекты их деятельности:
   - актуальные цели и задачи службы;
   - структура и функции службы;
   - реализуемые сейчас и в ближайшем прошлом проекты и достигнутые результаты;
   - взаимодействие с другими спецслужбами и организациями.
5. Перечень использованных информационных источников.

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6

Изучение информационно-психологической войны и типов информационного оружия

Цель работы: ознакомление с современной картиной политических отношений в информационном обществе и сущности информационно-психологической войны как средства достижения политических целей.

Продолжительность работы - 2 часа.

1. Порядок выполнения работы

В ходе выполнения задания следует осмыслить сущность информационно-психологической войны в процессе изучения следующих средств поражения информационной инфраструктуры и массовой психологии.

1. Информационное оружие, предназначенное для негативного воздействия на человека:
   - средства массовой информации.
2. Информационное оружие, предназначенное для вывода из строя средств электронных коммуникаций противника:
   - средства радиоэлектронной борьбы (РЭБ);
   - средства специального программно-технического воздействия (СПТВ).
3. Перечень использованных информационных источников.

2. Форма и содержание докладов

Доклад должен содержать:

1. Титульный лист.
2. Описание механизмов действия средств ведения информационно-психологической войны.
3. Историю развития и применения типов информационного оружия, в частности в локальных вооруженных конфликтах второй половины 20 века.
4. Современный уровень развития типов информационного оружия в России и ведущих зарубежных странах.
5. Перечень использованных информационных источников.

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7

Изучение международной нормативно-правовой базы по сотрудничеству в области обеспечения информационной безопасности

Цель работы: ознакомление с основными международными стандартами, регламентирующими обеспечение защиты конфиденциальной информации.

Продолжительность работы - 2 часов.

1. Порядок выполнения работы

При выполнении задания следует проанализировать содержание следующих документов:

1. Международный стандарт управления информационной безопасностью ISO 17799.
2. Общие критерии безопасности информационных технологий ГОСТ ИСО\МЭК 15408.
3. Критерии оценки надежности компьютерных систем («Оранжевая книга»).
4. Стандарт COBIT («Контрольные объекты для информационных и смежных технологий»).

Необходимо сопоставить эти стандарты с российской нормативной базой в области информационной безопасности и оценить их применимость в России.

2. Форма и содержание отчета

Отчет должен содержать:

1. Титульный лист.
2. Историю создания и развития стандартов и их связь со смежными документами.
3. Назначение и описание стандартов.
4. Практику применения стандартов за рубежом и в России.
5. Перечень использованных информационных источников.

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8

Изучение системы международных стандартов информационной безопасности

Цель работы: ознакомление с основными международными стандартами, регламентирующими обеспечение защиты конфиденциальной информации.

Продолжительность работы - 6 часов.

1. Порядок выполнения работы

При выполнении задания следует проанализировать содержание следующих документов:

1. Международный стандарт управления информационной безопасностью ISO 17799.
2. Общие критерии безопасности информационных технологий ГОСТ ИСО\МЭК 15408.
3. Критерии оценки надежности компьютерных систем («Оранжевая книга»).
4. Стандарт COBIT («Контрольные объекты для информационных и смежных технологий»).

Необходимо сопоставить эти стандарты с российской нормативной базой в области информационной безопасности и оценить их применимость в России.

2. Форма и содержание отчета

Отчет должен содержать:

1. Титульный лист.
2. Историю создания и развития стандартов и их связь со смежными документами.
3. Назначение и описание стандартов.
4. Практику применения стандартов за рубежом и в России.
5. Перечень использованных информационных источников.

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 9

Системы ЗИ в ведущих мировых компаниях

Цель работы: ознакомление с основными международными стандартами, регламентирующими обеспечение защиты конфиденциальной информации.

Продолжительность работы - 6 часов.

1. Порядок выполнения работы

За две недели до занятия студентам выдается задание в виде подготовки докладов.

Темы докладов:

1. Практика компании IBM в области защиты информации.
2. Практика компании Cisco Systems в разработке сетевой политики безопасности.
3. Практика компании Microsoft в области информационной безопасности.
4. Практика компании Google в области информационной безопасности.
5. Практика компании Apple в области информационной безопасности.

2. Форма и содержание докладов

Доклад должен содержать:

1. Титульный лист.
2. Подходы компании IBM к построению корпоративных политик безопасности.
3. Особенности оценки информационных рисков компанией CISCO.
4. Характеристика подходов компании CISCO к построению корпоративных политик безопасности. Этапы реагирования на события безопасности в компании CISCO. «Матрица безопасности» CISCO.
5. Основные принципы обеспечения информационной безопасности в компании Microsoft. Политики безопасности компании Microsoft.
6. Подходы к обеспечению информационной безопасности компании Google. Обеспечение информационной безопасности пользователей ресурсами Google.
7. Обеспечение информационной безопасности компанией Apple. Особенности подходов.
8. Перечень использованных информационных источников.

По каждой теме студенты выступают с докладом, желательная форма представления с использованием презентационных материалов.

Список источников

1. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах: учебное пособие/ В.И. Аверченков и др. – М.: Флинта, 2012. - 224 с. – Режим доступа http://ibooks.ru/

2. Центр исследования компьютерной преступности [Электронный ресурс]. Г. Маклаков, Научно-методологические аспекты подготовки специалистов в области информационной безопасности, статья - http://www.crime-research.ru/

3. Обзор зарубежного законодательства в области информационной безопасности [Электронный ресурс], статья - http://www.intuit.ru/department/security/secbasics/4/4.html