МИНОБРНАУКИ РОССИИ
Федеральное бюджетное образовательное учреждения высшего образования
«Ижевский государственный технический университет
имени М.Т. Калашникова»
(ФГБОУ ВО «ИжГТУ имени М.Т. Калашникова»)

Курсовая работа

на тему:

«Безопасность информационных технологий»

по дисциплине:

«применение инженерно-технических средств защиты информации»

Выполнил: Волкова А.С.
Студент гр. 6-36-1 БШ

Проверил: Опоева Л.М.
Преподаватель

Ижевск 2016

Безопасность информационных технологий

Волкова А.С.

Цель работы

- Изучить Безопасность информационных технологий
- Рассмотреть некоторые методы защиты и обеспечения безопасности информации.

Технические средства обеспечения безопасности информационных технологий

- "горячее" дублирование системы
- "холодное" резервирование и поддержание склада запасных частей и устройств.
- аварийные сервисы различных масштабов
- - применение оборудования с повышенной отказоустойчивостью, источников бесперебойного питания, специализированных систем диагностики и контроля;
- применение специализированных программных или аппаратных средств для защиты от хакерских атак
- "горячие линии" поддержки
- подписка на антивирусное обслуживание, в том числе и с аварийным выездом специалистов;

Криминогенные аспекты глобальной сети Интернет

- мошенничество при заключении сделок через Интернет, хищения из виртуальных магазинов, создания виртуальных финансовых пирамид.
- совершения сделок и операций, скрытых от налоговых органов.
- нарушения авторских и патентных прав, использования различных информационных баз правоохранительных и контролирующих органов.
- совершения преступлений в сфере компьютерной информации - неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ, нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети).

Защита информации и прав субъектов в области информационных процессов и информатизации

- **Цели защиты:**

*** предотвращение утечки, хищения, утраты, искажения, подделки информации;**

*** предотвращение угроз безопасности личности, общества, государства;**

*** предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;**

* защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
* сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
* обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Права и обязанности субъектов в области защиты информации

- Собственник документов, массива документов устанавливают порядок предоставления пользователю информации с указанием места,
- Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.
- Владелец обеспечивает уровень защиты информации
- Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств.

- **Собственник может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.**
- **Владелец обязан оповещать собственника информационных ресурсов и информационных систем о всех фактах нарушения режима защиты информации.**
- **обеспечивают условия доступа пользователей к информации.**

Защита прав субъектов в сфере информационных процессов и информатизации

- осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.
- Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти РФ и субъектов РФ.
- За правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством РФ.

Защита права на доступ к информации

- Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.
- Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.
- Руководители, другие служащие органов государственной власти организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

Безопасность информационных технологий

Состояние защищенности информации и ресурсов информационных технологий от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность информационных технологий выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

- Защита данных становится одной из самых открытых проблем в современных информационно-вычислительных системах. На сегодняшний день сформулировано три базовых принципа информационной безопасности, задачей которой является обеспечение:
- - целостности данных - защита от сбоев, ведущих к потере информации или ее уничтожения;
- - конфиденциальности информации;
- - доступности информации для авторизованных пользователей.

Сетевые черви.

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

* проникновения на удаленные компьютеры;
* запуска своей копии на удаленном компьютере;
* дальнейшего распространения на другие компьютеры в сети.

Борьба с компьютерными вирусами

- Для борьбы с компьютерными вирусами наиболее часто применяются антивирусные программы, реже - аппаратные средства защиты. Однако, в последнее время наблюдается тенденция к сочетанию программных и аппаратных методов защиты. Среди аппаратных устройств используются специальные антивирусные платы, вставленные в стандартные слоты расширения компьютера. Корпорация Intel предложила перспективную технологию защиты от вирусов в сетях, суть которой заключается в сканировании систем компьютеров еще до их загрузки.

Административные меры защиты

- Проблема защиты информации решается введением контроля доступа и разграничением полномочий пользователя.
- Распространённым средством ограничения доступа является система паролей.
- Более надёжное решение состоит в организации контроля доступа в помещения или к конкретному ПК в ЛВС с помощью идентификационных пластиковых карточек различных видов.
- пластиковые карточки с встроенной микросхемой – так называемые микропроцессорные карточки (МП – карточки, smart – card).

ЗАКЛЮЧЕНИЕ

- Безопасность информационных технологий – очень актуальная проблема сегодня. В данной курсовой работе были рассмотрены некоторые методы защиты и обеспечения безопасности информации. Можно сказать, что не существует одного абсолютно надежного метода защиты. Наиболее полную безопасность можно обеспечить только при комплексном подходе к этому вопросу. Необходимо постоянно следить за новыми решениями в этой области. В крупных организациях я бы рекомендовал ввести должность специалиста по информационной безопасности.

спасибо за внимание!