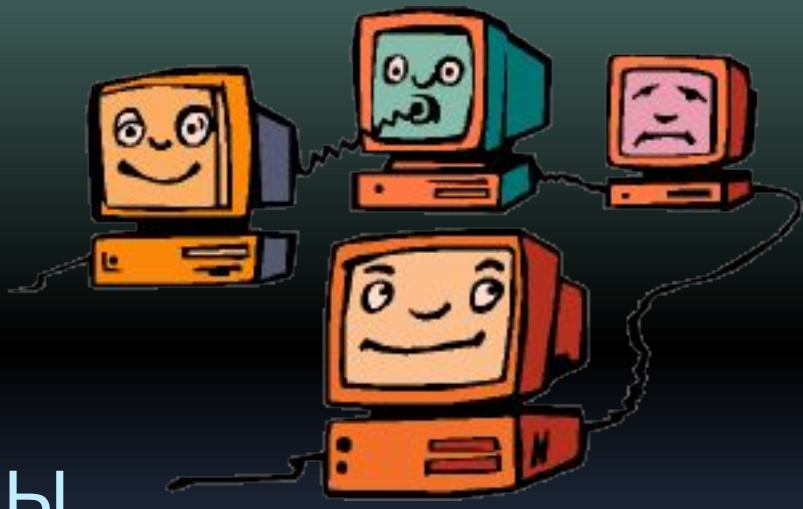
Проблемы компьютерной безопасности: тактика и контрмеры.



РАБОТА РЫЖЕНКО ЕЛЕНЫ ВЛАДИМИРОВНЫ, УЧИТЕЛЯ ИНФОРМАТИКИ И МАТЕМАТИКИ МБОУ Г. АСТРАХАНИ «СОШ № 64»

Введение.

«Информация – это кислород современной эпохи. Она проходит сквозь заборы, обвитые колючей проволокой, и ей нипочем границы, обозначенные высоковольтными проводами».
Рональд Рейган.

Как защитить информацию и дать возможность использовать ее по назначению и вовремя? Решение этого вопроса было и до сих пор остается одной из самых актуальных задач.

Совокупность факторов, представляющих опасность для функционирования информационной среды, называют информационными угрозами.

Противоправные воздействия на информационную среду могут наносить ущерб интересам человека и общества, поэтому одной из задач информатизации является обеспечение информационной безопасности.

Основными целями обеспечения информационной безопасности общества являются:

1. защита национальных интересов;
2. обеспечение человека и общества достоверной и полной информацией;
3. правовая защита человека и общества при получении, распространении и использовании информации.

Глава 1. Тайные проникновения.

«Я работаю по ночам».

Агент ФБР.

Тайные проникновения классифицируют как:

- ✔ Физические проникновения – взлом помещения, где мы не имеем права находиться.
- ✔ Сетевые проникновения.
- ✔ Запланированные проникновения.
- ✔ Случайные проникновения (при благоприятном стечении обстоятельств).
- ✔ Санкционированные правительством проникновения.

Контрмеры.

Одна из главных ошибок состоит в поддержке сетевых мер защиты информации при отсутствии должных мер безопасности против физического проникновения.

Меры физической безопасности можно разделить на:

- Контроль доступа различных лиц (пропуска, жетоны, биометрические сканеры).
- Электронные системы безопасности (датчики перемещения, электромагнитные детекторы, детекторы давления).
- Архитектурные особенности здания (бронированные двери, продуманная прокладка кабелей, узкие вентиляционные каналы и т.д.).
- Охранники.
- Освещение.
- Замки.
- Защитные барьеры.

Политика безопасности – четкий, структурированный и исчерпывающий набор правил и практических мер, связанных с защитой информации.

Глава 2. Проникновение в систему.

«И когда обрушается стены…»
Деф Лепард
исполнитель «тяжелого металла»
«Когда обрушается стены».

Перед тем как начать использование уязвимых мест на внешних уровнях компьютерной защиты, необходимо определить характеристики компьютера, с которым придется работать.

Слабые места:

- Тип Bios.
- Тип операционной системы.
- Пароль Bios.
- Запасные пароли.
- Извлечение жесткого диска.
- Обнуление CMOS.
- ЭСКАЛАЦИЯ ПРИВЕЛЕГИЙ.
- МЕНЕДЖЕР УЧЕТНЫХ ЗАПИСЕЙ В СИСТЕМЕ ЗАЩИТЫ.

Контрмеры.

Перед тем как изменять какие-либо настройки операционной системы, убедитесь в том, что для вашей версии Windows установлены все текущие пакеты обновления, включая свежие «заплаты» системы безопасности. Своевременное обновление системы уменьшает шансы злоумышленников на успешное проведение локальных или удаленных атак.

Глава 3. Мониторинг клавиатуры.

«Я никогда не печатаю на пишущей машинке, мой друг».
The Posies, «Farewell, Typewriter», Success.

Keylogger, или средство мониторинга клавиатуры, - это такое программное или аппаратное обеспечение, которое позволяет запоминать последовательность клавиш.

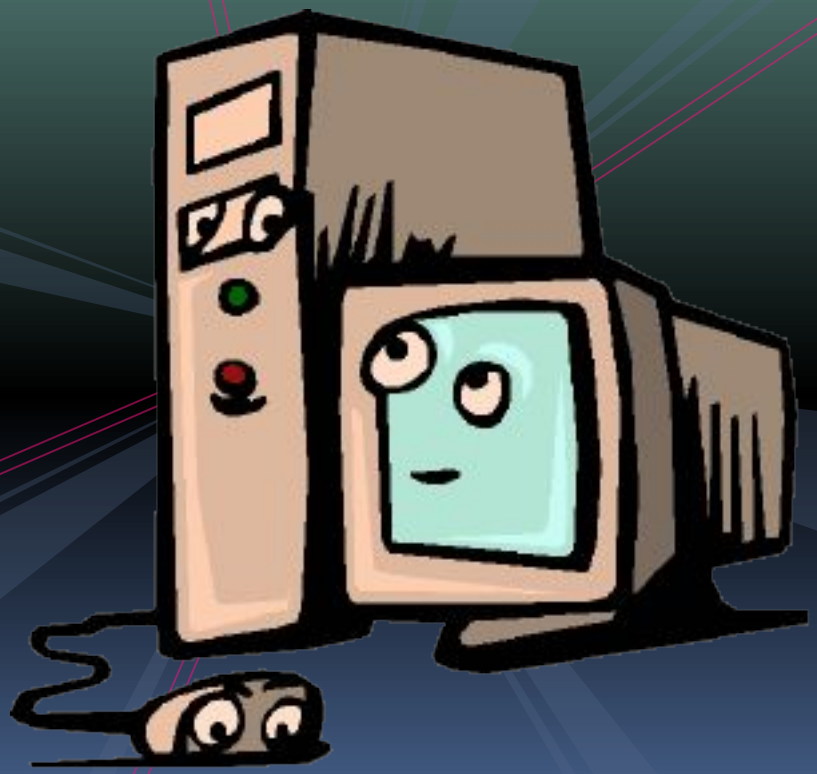
Анализируя эту последовательность можно:

- Узнать пароль;
- Получить конфиденциальную информацию;
- Найти доказательства незаконной деятельности.

Использовать Keylogger можно 2-мя способами:

1. Локально – для установки программы Keylogger понадобится 1-5 минут при наличии физического доступа к целевому компьютеру.
2. Удаленно – можно отослать электронную почту с «троянским конем», содержащую программу Keylogger.

Наилучшая контрмера – обеспечение физической безопасности рабочего места и безопасность в работе с сетью.



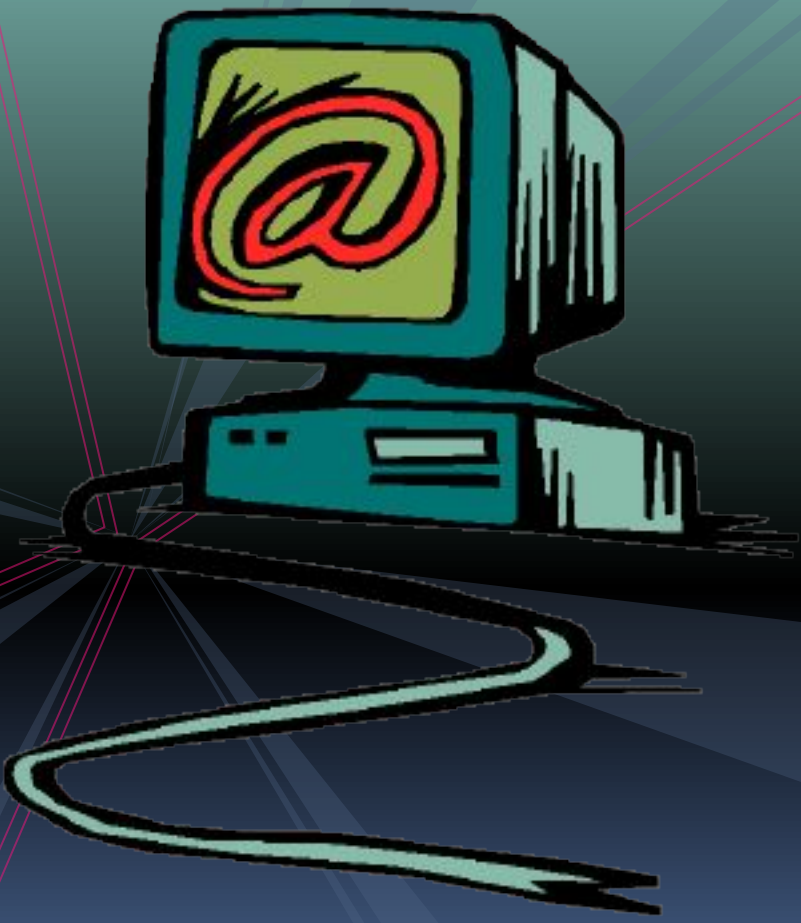
Глава 4. Взлом защищенных данных.

Когда заходит речь о защите информации, принимают во внимание два фактора, способных ввести пользователя в заблуждение о надежности защиты данных:

- ✔использование нестойких алгоритмов шифрования, которые легко взломать;
- ✔ненадёжность пароля, который легко угадать,
- ✔причём оба фактора тесно взаимосвязаны.

Контрмеры.

1. Стойкое шифрование.
2. Политика паролей.
3. Альтернативы паролю.
4. Смарт-карты.
5. Распознавание символов.



Глава 5. «Троянские кони»

«Я въезжаю в ваш город на большом черном троянском коне»
The Cure, «Club America», Wild Mood Swings

«Троянский конь» обозначает внешне безобидное приложение, внутри которого на самом деле спрятан враждебный программный код. Троянский конь может быть в игре, почтовом вложении или даже на веб-странице.

Троянских коней делят на 3 группы:

- Приложения, предназначенные для локального доступа к системе.
- Приложения, предназначенные для вредительских действий.
- Приложения, предназначенные для удаленного доступа к системе.

Контрмеры.

- Анализ сетевых подключений.
- Использование брандмауэров
- Мониторинг сетевого трафика.
- Использование мониторов реестра и программ проверки целостности файлов.
- Использование антивирусного программного обеспечения
- Использование специального ПО для обнаружения троянских коней.

Заключение.

Многие люди уделяют внимание исключительно обеспечению сетевой безопасности, напрочь забывая о должных мерах физической безопасности, отсутствие которых позволяет шпионам легко проникать в само здание и похищать конфиденциальную информацию.

Первыми линиями обороны на пути шпиона, получившего физический доступ к компьютеру, являются защита при помощи пароля BIOS и авторизация пользователя при входе в систему.

Информация и доказательства, которые кажутся защищенными, на самом деле не всегда оказываются таковыми. Нестойкие алгоритмы шифрования и ненадежные пароли – верная лазейка для шпиона, стремящегося взломать защищенные данные при помощи различных широко распространенных и простых в использовании утилит.

Троянские кони являются весьма эффективным средством компьютерного шпионажа, в особенности против неосведомленных и неподготовленных лиц. Большинство атак с использованием троянских коней осуществляется при помощи вложений электронной почты, веб-страниц либо загружаемых пользователем модифицированных приложений, содержащих код троянского коня, обеспечивающего тайный вход для шпиона.

Список использованной литературы.

1. Информатика и ИКТ. Учебник.11 класс. Базовый уровень/Под.ред.проф.Н.В.Макаровой.-СПб.: Питер,2008.
2. Угринович Н.Д. Информатика и информационные технологии. Учебник для 10-11 классов.-Москва.:БИНОМ. Лаборатория знаний,2003.
3. Макнамара Д. Секреты компьютерного шпионажа: Тактика и контрмеры. - Москва.: БИНОМ. Лаборатория знаний.2006.
4. Информатика. Учебное пособие для среднего профессионального образования./ Под общ. Ред. И. А. Черноскутовой – СПб. : Питер, 2005.
5. Новиков Ю., Черепанов А. Персональные компьютеры: аппаратура, системы, Интернет. Учебный курс. – СПб.: Питер, 2001.