

Слайд 1

Здравствуйте, уважаемые члены аттестационной комиссии!

Тема моей ДИПЛОМНОЙ РАБОТЫ (ПРОЕКТА) – **«Разработка алгоритма защиты операционной системы Windows от троянских программ».**

В работе будут рассматриваться проблемы защиты информации от вредоносных троянских программ.

Слайд 2

Анализ условия функционирования предприятия.

В качестве объекта исследований было выбрано предприятие «Звезда» образованное в 2000 году. Численность работников которого составляет 150 человек. Офисные, производственные и технологические помещения предприятия расположены на площади 10 000 кв.м.

Предприятие предоставляет населению услуги спутниковой связи. Предприятие «Звезда» расположено в г. Краснодар на ул. Киевская 12, занимает отдельно стоящее двухэтажное здание.

Для анализа среды пользователей рассмотрим организационную структуру предприятия изображенной на рисунке, представленном на слайде.

При анализе среды пользователей следует учитывать, что любой субъект из данной структуры предприятия потенциально может нести угрозу утечки информации.

Слайд 3

АС предприятия представляет собой многомашинный, многопользовательский комплекс. Информация с ограниченным доступом предприятия по незащищенным каналам не передается. По данным признакам, в соответствии с НД ТЗИ 2.5-005-99 "Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа", АС предприятия относится к классу 2. Кроме этого АС имеет возможность выход в интернет.

Сеть предприятия, к которой подключены 50 персональных компьютеров, подключенных к интернет приведена на рис. на слайде.

Слайд 4

Несанкционированный доступ (НСД) — наиболее распространенный и

многообразный вид компьютерных нарушений.

Основные каналы НСД, через которые нарушитель может получить доступ к компонентам АС и осуществить хищение, модификацию или разрушение информации:

- штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи);
- технологические пульта управления;
- линии связи между аппаратными средствами АС;
- побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.

Слайд 5

Самым многочисленным классом вредоносных программ являются троянские программы. Это видно из представленной диаграммы массовой доли троянов на ДИАГРАММЕ.

Из представленной диаграммы видно, что массовая доля троянских программ различных видов составила 57% от общего числа существующих вредоносных программ. Поэтому следует иметь хотя бы частичное представление о троянской программе, чтобы создать мероприятия по защите информации.

Целью троянской программы может быть:

- создание помех работе пользователя (в шутку или для достижения других целей);

похищение данных представляющих ценность или тайну, в том числе информации использующейся для аутентификации;

- вандализм — уничтожение данных и оборудования, вывода из строя или отказа обслуживания компьютерных систем, сетей и т. п.

- превращение компьютера в «зомби», для выполнения заранее заданных действий (с возможным обновлением списка), например рассылки спама, прямого управления компьютером, получения

несанкционированного доступа к ресурсам самого компьютера или к третьим ресурсам.

Слайд 6

Атаки на компьютеры под управлением Windows с использованием троянских программ, задачей которых является похищение и передача злоумышленнику различной ключевой информации, содержащейся на компьютере (пользовательские пароли и идентификаторы) в последнее время стали использоваться все чаще.

Одним из способов избежать заражения такими троянскими программами является создание комплексной защиты информации на предприятии. **Определим классы мероприятий по защите:**

- 1) Организационные мероприятия;
- 2) Технические мероприятия;
- 3) Программный комплекс мероприятий.

Полноценная защита Windows XP от троянских программ возможна при использовании всех этих классов мероприятий.

Слайд 7

Одним из наиболее эффективных способов борьбы с заражением троянскими программами является использование антивирусных программ и брандмауэров.

С целью определения качественной, программной защиты ПК предприятия я воспользовался результатами тестирования антивирусных программ и брандмауэров.

Тестирование антивирусных программ проводилось по следующим критериям: защита и лечение. Тест по защите охватывает статическое и динамическое обнаружение вредоносных программ, включая тестирование атаки в реальном времени. На экране приведена статистика результатов тестирования антивирусов в 2011 году.

На основании проведенного тестирования, лидером с высокой оценкой по защите и лечению вредоносных программ, является Kaspersky Internet Security 2011, который по сравнению с установленным на предприятии антивирусом McAfee: Total Protection 2011, почти в два раза лучше по параметрам защиты и лечению различных вредоносных программ. Поэтому я рекомендую удалить установленный антивирус McAfee и для эффективной защиты ПК предприятия, установить антивирус Kaspersky Internet Security 2011

Слайд 8

Данный компонент включает проверку системной памяти, объектов автозапуска, системного тома. Также есть функция «проверки ПК во время простоя» и функция «регулярного поиска руткитов», все эти функции нужно включить.

Проверка важных областей Параметры данной проверки следует настроить на максимум и выбрать самые важные объекты проверки это системная память, объекты автозапуска, загрузочные сектора и для максимальной защиты установить режим запуска, рекомендуется каждый день, чтобы предотвратить запуск трояна с загрузкой Windows.

Слайд 9

Выбор брандмауэра и его использование является второй после выбора антивируса, важной задачей обеспечения информационной безопасности предприятия.

С целью определения выбора наилучшего многофункционального брандмауэра рассмотрим статистику тестирования брандмауэров за 2011 год представленную на рис. на слайде.

По результатам тестирования видно, что лучшим из представленных брандмауэров, является Outpost Security Suite Pro. А антивирус со встроенным брандмауэром Kaspersky Internet Security уступает Outpost на 7%, не только из-за недоработанной защиты, но и из-за недостатка. Недостаток обуславливается тем, что встроенный брандмауэр в Kaspersky Internet Security не предоставляет возможность видеть используемые порты различными приложениями, а это, по моему мнению важно, т.к. троянские программы используют их для связи со своим создателем.

Слайд 10

Настройки брандмауэра по умолчанию являются оптимальными, но для улучшения качества защиты, некоторые из настроек следует изменить следующим образом – рисунок на слайде презентации.

Слайд 11

Для того, чтобы обеспечить функционирование троянской программы, ее создатели помещают в раздел «Автозагрузка» и в реестр Windows.

1)Раздел «Автозагрузка».

2)Раздел реестра Windows.

Для того, чтобы просмотреть реестр Windows необходимо воспользоваться меню: Пуск->Панель управления -> Редактор реестра.

Если вышеизложенные способы ничего не дали, а признаки троянской программы на лицо (непонятные ошибки, нестабильность работы ОС), то необходимо просканировать ПК на наличие открытых портов. Все, что понадобится для такой операции — это хороший сканер портов. Данная процедура высокоэффективна, и с ее помощью выявляются даже самые скрытные троянские программы.

С целью предотвращения заражения известными троянскими программами рекомендую отключить порты, которые наиболее часто используются. Для этого запускаем "Локальные параметры безопасности".

Слайд 12

ВЫВОДЫ

В данной работе были разработаны мероприятия по защите ОС Windows XP от троянских программ, которые позволили улучшить систему защиты и поднять ее на новый более высокий уровень.

Из перечисленных мероприятий по защите информации самыми эффективными являются программные средства защиты информации. Данные мероприятия позволили повысить уровень защиты предприятия от троянских программ почти в два раза. Для достижения более высокой эффективности защиты программных средств, разработаны рекомендации по оптимальной их настройке.

Таким образом, Цель работы достигнута.

Спасибо за внимание! Доклад окончен.