Томина Г.Д.
Киркоров С.И.

ПОДХОД К ОРГАНИЗАЦИИ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Большинство современных информационных систем (ИС) создаются на базе сетевого взаимодействия неоднородных программно-аппаратных платформ, использующих различные системно-технические решения построения ПК, ОС, сетевых и прикладных сервисов. В силу неоднородности аппаратно-программной платформы сетевой ИС, реализация механизмов анализа защищенности в каждом из структурных компонент ИС неэффективна по стоимости. Целесообразнее создать аппаратно-программный компонент, реализующий механизмы анализа безопасности ИТ и обладающий возможностью подключения в тех частях ИС, с которыми связаны наибольшие риски безопасности. Большую часть рисков, уникальных для каждой из ИС, можно согласно [1] связать с работой приложений, сервисами ОС или с сетевыми сервисами. Вследствие их широкой известности и некоторой универсальности, поиск известных слабостей ИС, как и поиск известных атак, становится технически тривиальной задачей.

При построении отечественных защищенных ИТ разработчики вынуждены соблюдать баланс между необходимостью поддержания безопасности ИС с помощью отечественных средств защиты информации и использования зарубежных прогрессивных ИТ и зарубежных компьютеров.

Авторы [2] считают, что создание защищенных систем "с нуля" от ОС до приложений – наиболее радикальный способ, но неприемлем с экономической точки зрения, поэтому защищенные системы создают из компонент, имеющихся в наличии, преодолевая присущие им недостатки с помощью построения особой архитектуры таких систем и специально разработанных отечественных средств защиты. Особое место в номенклатуре последних отводится средствам организации активной защиты, т.е. выполняющим задачи детектирования сетевых пакетов, анализа их информации по заданным критериям и выявления подозрительной активности потоков.

Разработанный нами аппаратно-программный комплекс (АПК) предназначен для решения указанных задач, называется анализатором протоколов и реализован в двух модификациях: переносной и стационарный.

Стратегия, использованная при построении анализатора протоколов

Поскольку любая сетевая ИС состоит из сегментов, при построении анализатора протоколов была реализована следующая стратегия.

1. Обеспечена возможность подключения как к локальной Ethernet сети (10 Мбит/с, 100 Мбит/с), так и к глобальной сети через базовый комплект физического интерфейса RS-232 и возможность организации многоканального взаимодействия.
2. Производится захват и предварительная обработка (по заданной уполномоченным лицом маске) пакетов специализированной платой захватчика пакетов со скоростью до 100 Мбит/с.
3. Детектируются активности сетевых пакетов, передающихся на любой компьютер локальной сети или удаленный компьютер.
4. Организовано взаимодействие ПО анализатора протоколов с уполномоченным лицом и с операционной системой анализатора по технологии "клиент–сервер".
5. Организовано хранение захваченных пакетов, результатов статистической обработки, наборов фильтров и правил генерации сигналов тревоги в базе данных анализатора протоколов.

Вследствие специфики применения анализатора протоколов либо в качестве мобильного средства для оперативного подключения к сегменту сети с целью отслеживания сетевого трафика, либо в качестве стационарного пункта наблюдения за сетевым трафиком администратором или дежурным оператором было реализовано шестое принципиальное решение.

6. Обеспечена защита от несанкционированного запуска анализатора протоколов путем включения в состав стационарного анализатора платы защиты от НСД "Амулет" и устройства контроля доступа "УКД SSR-253" в переносной и создания профилей защиты для уполномоченных лиц средствами ОС анализатора (Windows NT 4.0) и ввода пароля защищенного интерфейса ПО анализатора.

Структура анализатора протоколов

Ядром анализатора протоколов является специализированная сетевая плата (ССП) захватчика пакетов и программное обеспечение анализатора, называемого базовыми программными средствами (БПС).

ССП захватчика пакетов (см. рис. 1) подключается к Ethernet сети в режиме повторителя, что позволяет не обнаруживать анализатор при его работе в сети. Имеет двухпортовое ОЗУ, в которое может записывать "полный" или "отфильтрованный" трафик сети. Содержит контроллер 82555 Intel для согласования Ethernet 10BASE-T, 100BASE-TX с устройством предварительной обработки информации, которое реализовано на ПЛИС Altera EPF81500 и настраивается при включении питания анализатора от ПЗУ.

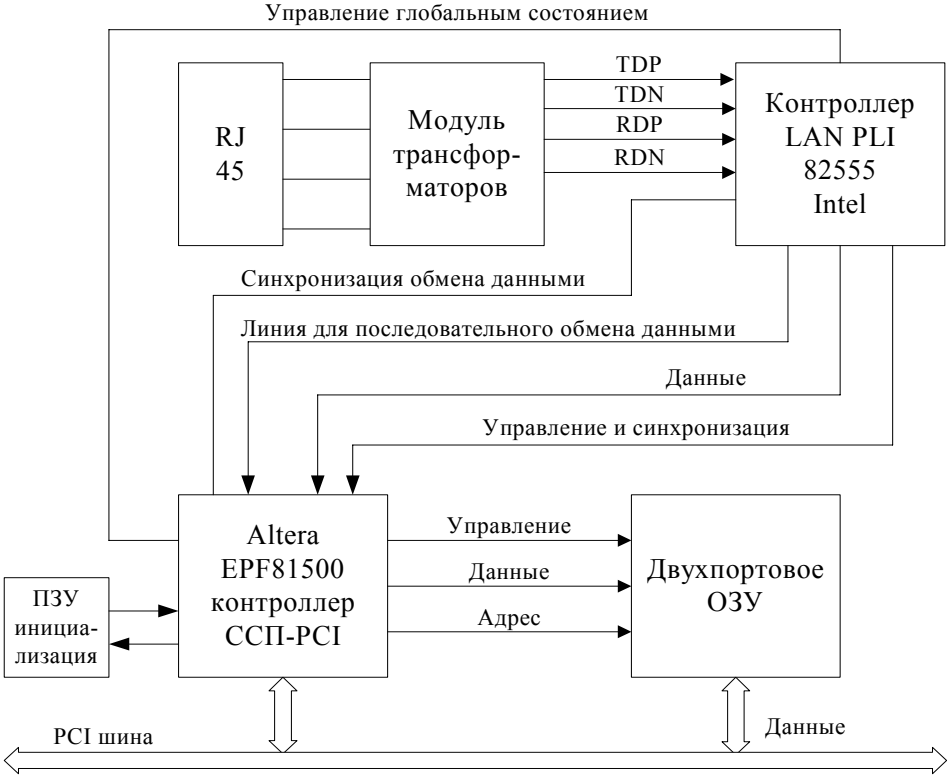

Рисунок 1 – Структурная схема ССП захватчика пакетов

БПС анализатора протоколов (см. рис. 2) реализованы в виде двух процессов пользовательского режима и двух драйверов, работающих в режиме ядра ОС. Процесс интерфейса пользователя взаимодействует, с одной стороны, интерактивно с уполномоченным пользователем, с другой – с процессом сервиса БПС, который является посредником в доступе к библиотеке протоколов, сервису обслуживания базы данных и драйверу ССП. Структура базы данных управляется набором функций сервиса обслуживания базы данных и открытым интерфейсом ODBC.

Функциональные возможности анализатора протоколов

Задача автоматического детектирования и анализа сетевых пакетов решается совместно ССП захватчика пакетов и БПС анализатора.

БПС анализатора протоколов обеспечивают средства управления специализированной платой захватчика пакетов, создания и сохранения на жестком диске базы полей и характеристик фильтрации пакетов, декодирование протоколов и анализ захваченных пакетов, обеспечивают интерфейс для задания правил фильтрации уполномоченным лицом (просмотр, редактирование фильтров, установка активных), регистрацию и учет результатов анализа, сохранение захваченных пакетов в базе данных и отображение их на экран.

К задачам автоматического детектирования и анализа пакетов логически присоединяется задача автоматического выявления несанкционированных действий и подозрительной активности. Для ее решения в БПС анализатора производят обработку результатов анализа и сохранение статистики, обеспечивают интерфейс для задания фильтров событий, правил генерации сигналов тревоги (звуковой сигнал или электронная почта), настраиваемых на события из базы полей и характеристик фильтрации пакетов или на изменения статистических параметров работы сети. Производят поиск признаков широковещательной активности и распознавание активных источников IP-адресов. Обеспечивают возможность просмотра и редактирования полей захваченных пакетов в сочетании с функцией Send, а также архива пакетов.

Следует заметить, что анализируется тип протоколов (IP, TCP, UDP, SMB, RIP, ARP, NetBios, IPX, SPX), адрес отправителя и получателя пакетов, параметры пакета (время перехвата, номер кадра, длина пакета), строка контекстного поиска в пакете. Автоматическая фильтрация производится по типу протокола, портам, адресам, выбору произвольного сегмента поля, по активным источникам IP-адресов.

Защита от несанкционированного запуска анализатора протоколов разбивается на две фазы: защита от включения анализатора протоколов, защита от несанкционированного запуска функций БПС.

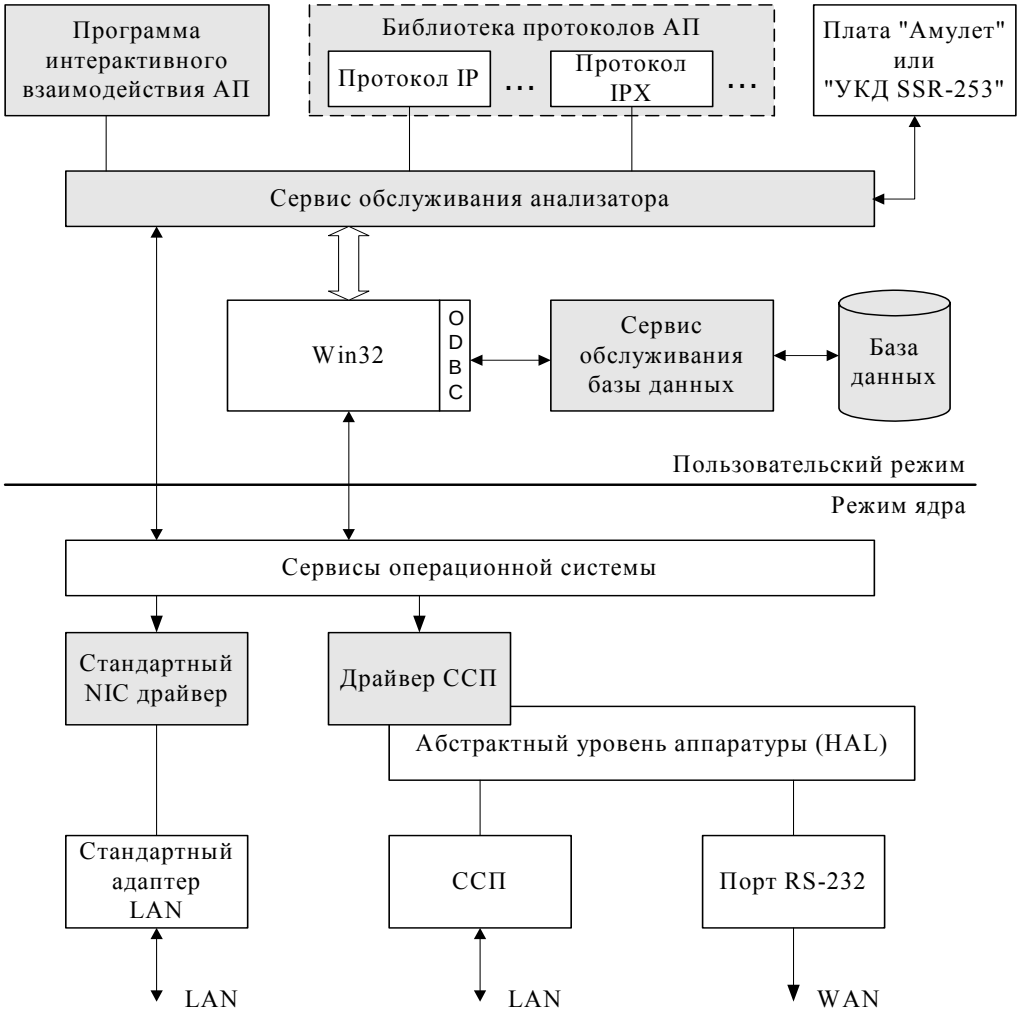

Рисунок 2 – Структура БПС анализатора протоколов

В первой фазе защиты используется плата НСД "Амулет" или устройство контроля доступа "УКД SSR-253" для стационарного и мобильного анализаторов соответственно, которые требуют предъявления полномочий на включение анализатора. Далее производится загрузка ОС и БПС анализатора, которые обеспечивают защиту от НСД второй фазы: ввод пароля инициализации оконного интерфейса, запуск только разрешенных в профиле защиты администратора или уполномоченного лица функций анализатора и контроль целостности БПС анализатора.

Заключение

Средства анализа защищенности сетевых ИС должны использоваться всегда, если к ИС предъявляются повышенные требования безопасности или они работают в условиях повышенного риска безопасности. Представленный в этой статье подход к организации активной защиты, построенный на детектировании сетевых пакетов, анализе информации о протоколах и пакетах по заданным критериям, выявлении подозрительной активности потоков информации, основан на практическом опыте анализа нарушений безопасности сетевых сервисов. Что позволило предложить стратегию построения аппаратно-программного компонента, реализующего механизмы анализа безопасности сетевых сервисов, для подключения либо в тех частях ИС, с которыми связаны наибольшие риски безопасности (переносной анализатор протоколов), либо в качестве стационарного пункта наблюдения за трафиком сети (стационарный анализатор).

Литература

1. И.Трифоненко. Инструментальные средства изучения защищенности информационных систем, Jet Infosystems.
2. Зегжда Д.П., Ивашко А.М. Технология создания безопасных систем обработки информации на основе защищенной ОС. Ж-л Проблемы информационной безопасности. Компьютерные системы, №2, 1999 г.