УДК 004

АРХИТЕКТУРА СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Асхатова Ляйсан Ильдаровна
канд. экон. наук
Казанский федеральный университет, Казань

Галимов Эдвард Раифович
студент

Габдуллин Ильдар Масхутович
студент
Казанский национальный исследовательский технический университет им. А.Н. Туполева, Казань

author@apriori-journal.ru

Аннотация. Рассматривается система обнаружения вторжений и 3 вида сетевых экранов: сетевой уровень, сеансовый уровень и уровень приложений.

Ключевые слова: архитектура; фильтр; система.

ARCHITECTURE OF INTRUSION DETECTION SYSTEM

Askhatova Laysan Ildarovna
candidate of economical sciences
Kazan Federal University, Kazan

Galimov Edward Raifovich
student

Gabdullin Ildar Maskhutovich
student
Kazan National Research Technical University, Kazan

Abstract. Considered an intrusion detection system and 3 types of fire-walls: network layer, session layer and application layer.

Key words: architecture; the filter; system.

Межсетевым экраном называют локальное или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы. Также встречаются общепринятые названия брандмауэр и firewall. В общем случае, МЭ могут применяться для разграничения внутренних подсетей корпоративной сети организации.

Задачами МЭ, как контрольного пункта, являются:

- Контроль всего трафика, входящего во внутреннюю корпоративную сеть;
- Контроль всего трафика, исходящего из внутренней корпоративной сети.

Контроль информационных потоков состоит в их фильтрации и преобразовании в соответствие с заданным набором правил. Поскольку в современных МЭ фильтрация может осуществляться на разных уровнях эталонной модели взаимодействия открытых систем (OSI), МЭ удобно представить в виде системы фильтров. Каждый фильтр на основе анализа проходящих через него данных, принимает решение – пропустить дальше, перебросить за экран, блокировать или преобразовать данные.

Неотъемлемой функцией МЭ является протоколирование информационного обмена. Ведение журналов регистрации позволяет администратору выявить подозрительные действия, ошибки в конфигурации МЭ и принять решение об изменении правил МЭ.

В зависимости от уровня, на котором происходит контроль доступа, существует разделение на сетевые экраны, работающие на:

- сетевом уровне, когда фильтрация происходит на основе адресов отправителя и получателя пакетов, номеров портов транспортного уровня модели OSI и статических правил, заданных администратором;
- сеансовом уровне – отслеживающие сеансы между приложениями, не пропускающие пакеты нарушающих спецификации TCP / IP, ча-

сто используемых в злонамеренных операциях – сканировании ресурсов, взломах через неправильные реализации TCP / IP, обрыв / замедление соединений, инъекция данных;

- уровне приложений, фильтрация на основании анализа данных приложения, передаваемых внутри пакета. Такие типы экранов позволяют блокировать передачу нежелательной и потенциально опасной информации на основании политик и настроек.

Система обнаружения вторжений (IDS – Intrusion Detection Systems) представляет собой программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть, либо несанкционированного управления ими в основном через Интернет. Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

У систем обнаружения вторжений целесообразно различать локальную и глобальную архитектуру. В рамках локальной архитектуры реализуются элементарные составляющие, которые затем могут быть объединены для обслуживания корпоративных систем (рис. 1).

Первичный сбор данных осуществляют сенсоры. Регистрационная информация может извлекаться из системных или прикладных журналов, либо добываться из сети с помощью соответствующих механизмов активного сетевого оборудования или путем перехвата пакетов посредством установленной в режим мониторинга сетевой карты.

На уровне агентов (сенсоров) может выполняться фильтрация данных с целью уменьшения их объема. Это требует от агентов некоторого интеллекта, но зато разгружает остальные компоненты системы.

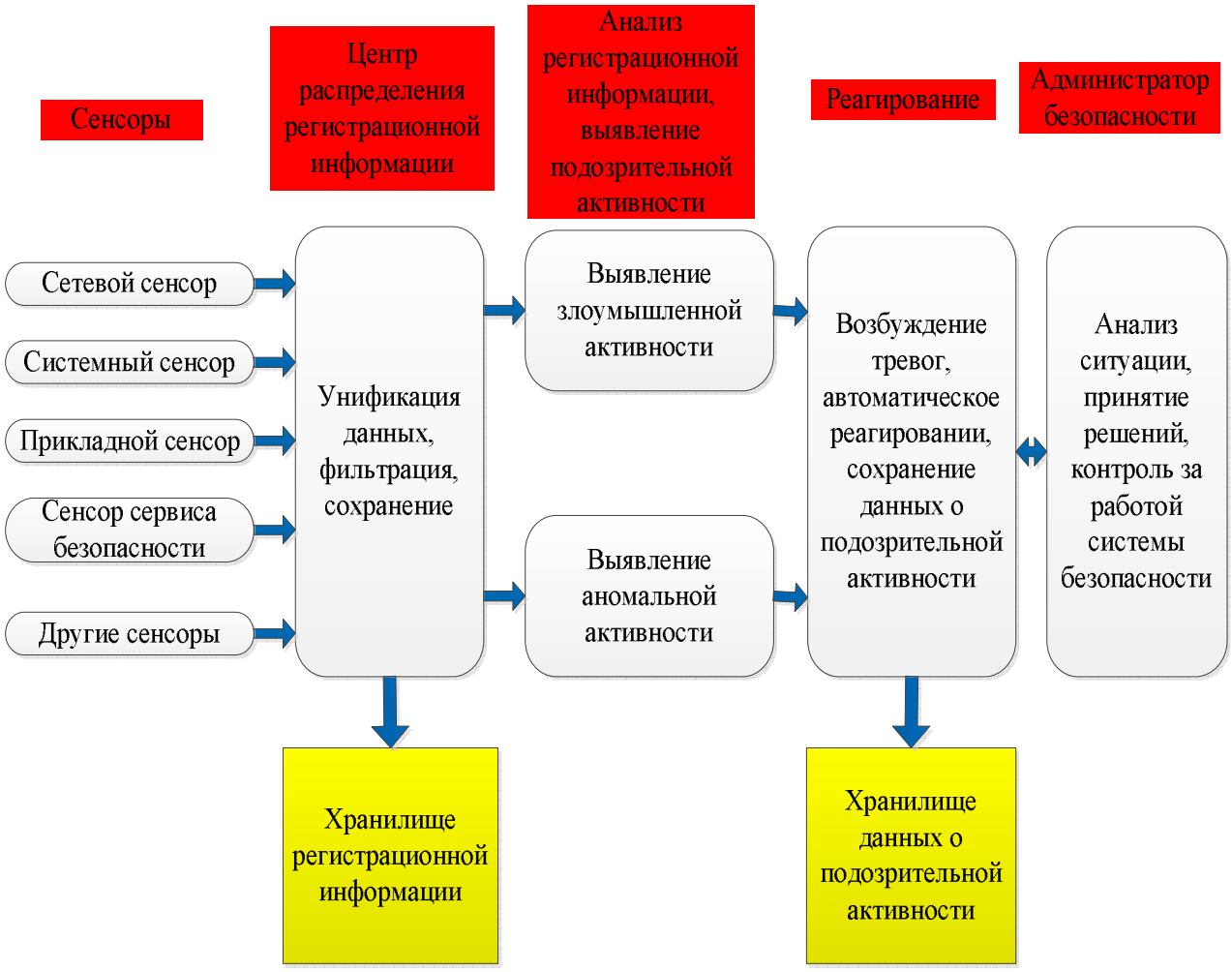

Рис. 1. Основные элементы локальной архитектуры систем обнаружения вторжений

Агенты передают информацию в центр распределения, который приводит ее к единому формату, возможно, осуществляет дальнейшую фильтрацию, сохраняет в базе данных и направляет для анализа статистическому и экспертному компонентам. Один центр распределения может обслуживать несколько сенсоров.

Содержательный активный аудит начинается со статистического и экспертного компонентов. Если в процессе статистического или экспертного анализа выявляется подозрительная активность, соответствующее сообщение направляется решателю, который определяет, является ли тревога оправданной, и выбирает способ реагирования.

Глобальная архитектура подразумевает организацию одно-ранговых и разно-ранговых связей между локальными системами обнаружения вторжений (рис. 2).

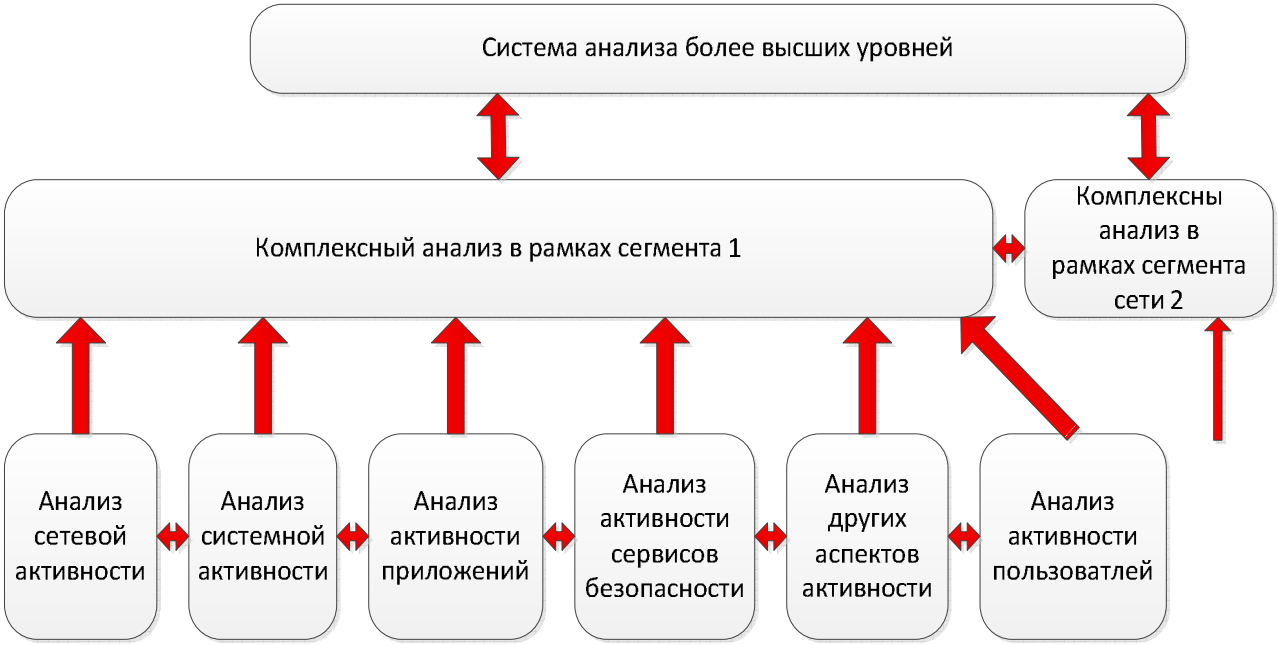

Рис. 2. Глобальная архитектура систем обнаружения вторжений

На одном уровне иерархии располагаются компоненты, анализирующие подозрительную активность с разных точек зрения. Когда один компонент обнаруживает что-то подозрительное, то во многих случаях целесообразно сообщить об этом соседям либо для принятия мер, либо для усиления внимания к определенным аспектам поведения системы.