УДК 004.056

Обоснование архитектуры перспективной системы обнаружения и предотвращения вторжений

М.П. Сычев [1], А.В. Астрахов [1], К.Б. Здирук [1, 2], И.И. Подвойский [1]

[1] МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

[2] ОАО «НИИАА им. академика В.С. Семенихина», Москва, 117393, Россия

Проведен сравнительный анализ алгоритмов и технологий современных систем обнаружения и предотвращения вторжений, а также методов обработки сетевой информации. Разработана архитектура перспективной системы обнаружения и предотвращения вторжений (СОПВ), использующей компоненты аппаратной виртуализации и многоуровневую систему обработки информации, которая поступает с датчиков. Проведено имитационное моделирование компонентов системы в среде Matlab.

E-mail: zi@bmstu.ru

Ключевые слова: *системы обнаружения и предотвращения вторжений, имитационное моделирование, верификация, валидация.*

Актуальность исследования. Сетевые и информационные технологии изменяются настолько быстро, что статичные защитные механизмы, к которым относятся системы разграничения доступа, межсетевые экраны, системы аутентификации, во многих случаях не могут обеспечить эффективной защиты. В связи с этим требуются динамические методы, позволяющие оперативно обнаруживать и предотвращать нарушения безопасности. Одной из технологий, обеспечивающей обнаружение нарушений, которые не могут быть идентифицированы с помощью традиционных моделей контроля доступа, является технология обнаружения вторжений.

Системы обнаружения и предотвращения вторжений (СОПВ) появились в 1980-х годах. Разработкой подобных систем занимаются крупнейшие корпорации, такие как IBM и Hewlet Packard [1]. Тем не менее проблематика в данной области существует и в настоящее время ввиду непрерывного совершенствования компьютерных технологий и, как следствие, появления новых видов компьютерных атак.

С 15 марта 2012 г. вступил в силу приказ ФСТЭК России от 6 декабря 2011 г. № 638 [2], регламентирующий требования к системам обнаружения вторжений. Согласно приказу, предписано наличие систем обнаружения вторжений в составе средств защиты информации при обработке информации, составляющей государственную тайну.

Сравнительный анализ существующих СОПВ и алгоритмов обработки сетевой информации. При проведении сравнительного анализа существующих СОПВ рассмотрены как зарубежные, так и отечественные системы: коммерческие и бесплатные с открытым ис-

ходным кодом. В результате выделены основные недостатки существующих систем: отсутствие сертификатов ФСТЭК и ФСБ; отсутствие средств противодействия атакам, использующим технологию аппаратной виртуализации. Основные достоинства данных систем приняты в качестве базовых требований к разрабатываемой СОПВ.

Ключевым элементом СОПВ является модуль классификации состояний автоматизированной системы. Для выбора математических алгоритмов, лежащих в основе данного модуля и дополнительных модулей (оценки аномальности распределения сетевого трафика и оценки аномальности сетевых протоколов), проведен сравнительный анализ методов обработки сетевой информации.

В качестве алгоритма модуля классификации состояния автоматизированной системы выбраны экспертные системы с элементами нечеткой логики [3] (алгоритм Мамдани [4]). Данный алгоритм состоит из нескольких этапов:

– формирование базы правил вида *RULE_1: IF "Condition_1" THEN "Conclusion_1" (F1) AND "Conclusion_2" (F2)*;

– фаззификация входных переменных. На вход поступают сформированная база правил и массив входных данных $\boldsymbol{A} = \{a_1, ..., a_m\}$, где m — количество входных переменных. В массиве содержатся значения всех входных переменных. Целью этапа является получение значений истинности для всех подусловий из базы правил, т. е. для каждого из подусловий находится значение $b_i = \mu(a_i)$. Таким образом, получается множество значений b_i, где $i = 1, \ldots, m$;

– агрегирование подусловий. Условие правила может быть составным, т. е. включать подусловия, связанные между собой с помощью логической операции *AND*. Целью этого этапа является определение степени истинности условий для каждого правила системы нечеткого вывода. Упрощенно говоря, для каждого условия находим минимальное значение истинности всех его подусловий. Формально это выглядит так: $c_j = \min\{b_i\}$, где $j = 1, \ldots, n$; n — количество условий;

– активизация подзаключений. На этом этапе происходит переход от условий к подзаключениям. Для каждого подзаключения находится степень истинности $d_i = c_i F_i$, где $i = 1, \ldots, q$; q — количество подзаключений. Затем опять же каждому i-му подзаключению ставится множество $\boldsymbol{D}_i$ с новой функцией принадлежности. Ее значение определяется как минимум из d_i и значения функции принадлежности терма из подзаключения. Этот метод называется min-активизацией, который формально записывают следующим образом: $\mu'_i(x) = \min\{d_i, \mu_i(x)\}$, где $\mu'_i(x)$ — «активизированная» функция принадлежности; $\mu_i(x)$ — функция принадлежности терма; d_i — степень истинности i-го подзаключения. Цель этого этапа — получение совокупности «активизированных» нечетких множеств $\boldsymbol{D}_i$ для каждого из подзаключений в базе правил ($i = 1, \ldots, q$);

– аккумуляция заключений. Целью этого этапа является получение нечеткого множества для каждой из выходных переменных (или их объединения). Выполняется этап таким образом: *i*-й выходной переменной ставится объединение множеств $\boldsymbol{E}_i = \cup \boldsymbol{D}_j$, где j — номера подзаключений, в которых участвует *i*-я выходная переменная ($i = 1, \ldots, s$). Объединением двух нечетких множеств является третье нечеткое множество с функцией принадлежности $\mu'_i(x) = \max\{\mu_1(x), \mu_2(x)\}$, где $\mu_1(x)$, $\mu_2(x)$ — функции принадлежности объединяемых множеств;

– дефаззификация выходных переменных, целью которой является получение количественного значения для каждой из выходных лингвистических переменных. Формально это происходит следующим образом: рассматривается *i*-я выходная переменная и относящееся к ней множество $\boldsymbol{E}_i$ ($i = 1, \ldots, s$), затем с помощью метода дефаззификации находится итоговое количественное значение выходной переменной. В данной реализации алгоритма используется метод центра тяжести, в котором значение *i*-й выходной переменной рассчитывается по формуле

$$y_i = \frac{\int\limits_{\min}^{\max} x\mu_i(x)dx}{\int\limits_{\min}^{\max} \mu_i(x)dx},$$

где $\mu_i(x)$ — функция принадлежности соответствующего нечеткого множества $\boldsymbol{E}_i$; min и max — границы универсума нечетких переменных; y_i — результат дефаззификации.

Для дополнительных модулей выбраны статистические методы [2].

Оценка аномальности распределения сетевого трафика реализуется следующим алгоритмом:

– за интервал времени t накапливается статистика наблюдений величины $(x_1, \ldots, x_n)$, где x_i — число полученных пакетов в течение 1 с;

– вычисляется математическое ожидание $\mu = \sum x_i / n$, где $i = 1, \ldots, n$; n — число наблюдений;

– вычисляется среднеквадратическое отклонение

$$\sigma = \sqrt{\frac{(x_1^2 + \ldots + x_n^2)}{n-1} - \mu^2};$$

– новое наблюдение является аномальным, если оно не укладывается в границах доверительного интервала $\overline{0, \mu + \sigma}$.

Выбор сделан на основании таких преимуществ данных методов, как отделение управляющего решения от формулировки, универсальность данных методов, использование уже отработанного и зарекомендовавшего себя аппарата математической статистики. Данные ме-

тоды наименее требовательны к вычислительным ресурсам, поэтому их использование целесообразно в системах реального времени.

Архитектура перспективной СОПВ состоит из двух компонентов (рис. 1): глобальной системы обнаружения вторжений (Главная машина, модуль GIPS) и локальной (автоматизированное рабочее место (АРМ), модуль HIPS). *Глобальную систему* размещают на наиболее производительную вычислительную установку (ВУ). Эта система выполняет функции сигнатурного анализа входящего трафика, а также классификацию состояния всей системы. *Локальная система* находится на автоматизированных рабочих местах, так как является менее требовательной к вычислительным ресурсам. В состав данной системы входят модули: классификации состояния ВУ, межсетевого экрана, разграничения доступа к объектам операционной системы (ОС), разграничения доступа к сетевым ресурсам, оценки аномальности распределения сетевого трафика, оценки аномальности протоколов и модуль гипервизора. Функциональная схема взаимодействия данных подсистем и их компонентов представлена на рис. 2.

Основным отличием предложенной системы от существующих аналогов является модуль, в котором используется технология аппаратной виртуализации, — модуль гипервизора. Он позволяет защититься от класса атак с применением технологий сокрытия присутствия в системе (rootkit).

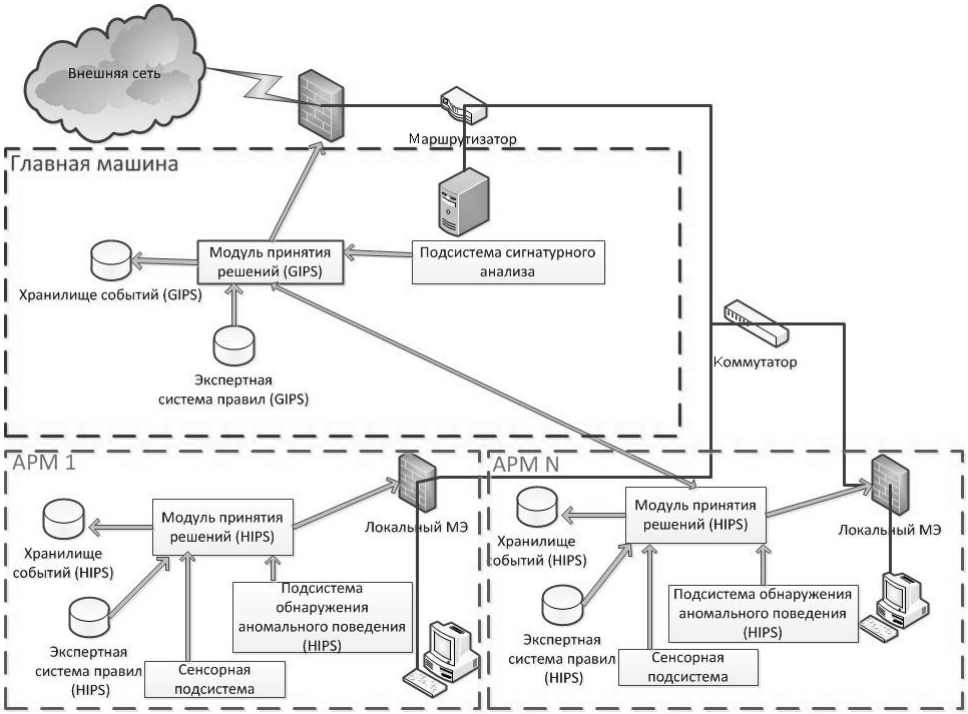

Рис. 1. Архитектура перспективной системы обнаружения вторжений

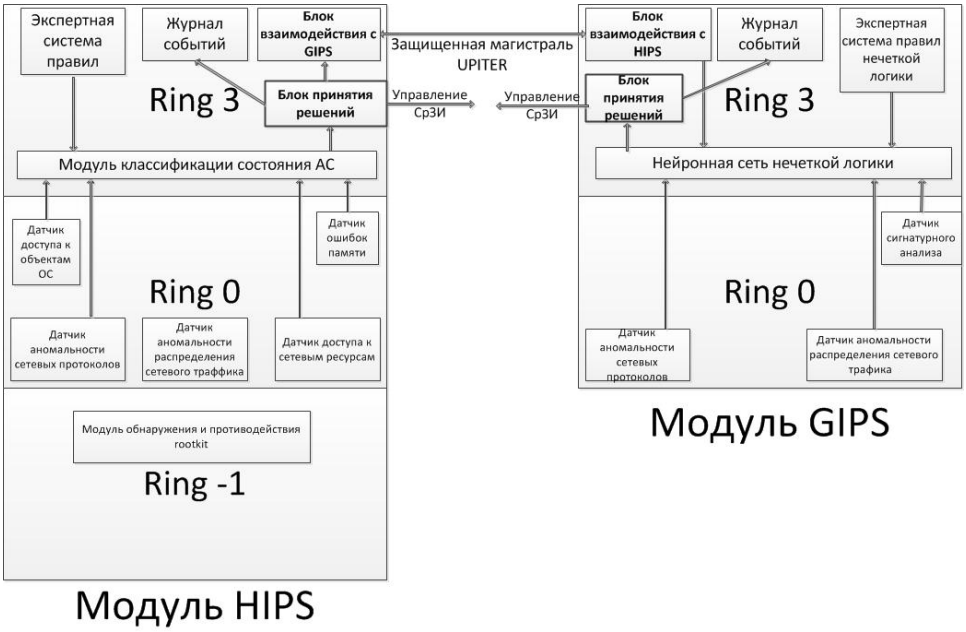

Рис. 2. Функциональная схема взаимодействия элементов системы обнаружения вторжений

Каждый модуль помимо функций защиты реализует функции сбора информации о событиях политики безопасности, т. е. является датчиком.

Ключевым элементом модуля HIPS является подсистема классификации состояний автоматизированной системы (АС) — модуль классификации состояний АС. Схема взаимодействия датчиков СОПВ с модулем классификации состояний АС представлена на рис. 3.

Полученная оценка состояния направляется в блок принятия решений, который передает принятую информацию модулю GIPS и генерирует управляющее действие средствам защиты информации.

Имитационное моделирование в среде Matlab. Наиболее значимым из разрабатываемых элементов СОПВ является модуль классификации состояния АС. Моделирование данного элемента осуществлено в среде Matlab с использованием модуля Fuzzy Logic Toolbox.

Модуль классификации состояния представляет собой нечеткую экспертную систему, которая в зависимости от входных параметров должна выдавать численный результат — оценку состояния системы по шкале от 0 до 50:

0…10 — нормальное состояние;

10…20 — осуществляется сканирование хоста;

20…30 — осуществляется попытка DOS-атаки;

30…40 — осуществляется попытка несанкционированного доступа (НСД);

40…50 — осуществляется сетевая атака.

Входными параметрами модуля классификации состояния АС (stateclassificator) служит информация, поступающая со следующих датчиков:

– суммарного трафика (allpackets);
– аномальности распределения сетевого трафика (antraf);
– аномальности протоколов (anproto);
– доступа к сетевым ресурсам (fwm);
– доступа к объектам ОС (syscalls).

Рис. 3. Схема взаимодействия датчиков СОПВ с модулем классификации состояний АС

На рис. 4 и 5 представлены поверхности, графически отображающие зависимость результата вычисления (ось аппликат «result») от входных параметров. Согласно полученным результатам моделирования, можно сделать вывод о том, что модель адекватно описывает блок классификации состояния автоматизированной системы, экспертная система правил составлена верно, функции принадлежности входных и выходных параметров выбраны правильно.

Программная реализация компонентов. Разработанные элементы СОПВ написаны на языках Си и Си++, реализованы в виде модуля ядра ОС Linux. Поддерживаемые версии ядра 2.4–2.6, процессор 32/64-битовой архитектуры с поддержкой аппаратной виртуализации.

Для тестирования была разработана программа, осуществляющая генерацию пакетов с заданными полями, использован сканер уязвимостей XSpider 7.0.

Тестирование проведено в несколько этапов:

– проверка работоспособности компонентов СОПВ в нормальных условиях;

– проверка реакции компонентов СОПВ в условиях атаки «отказ в обслуживании» (DOS);

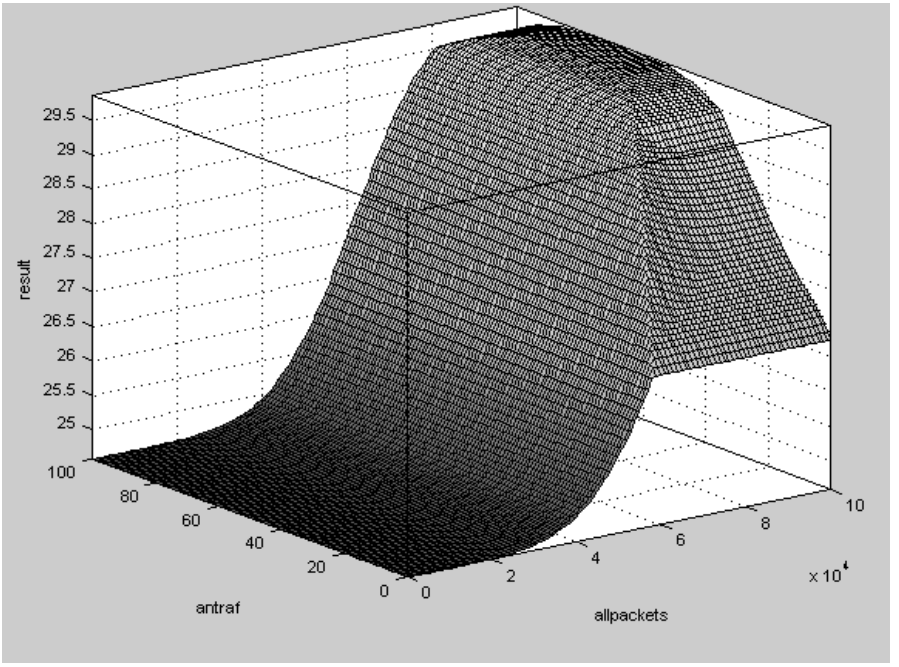

Рис. 4. Поверхность, отображающая зависимость результата вычислений от аномальности распределения сетевого трафика и общего числа пакетов

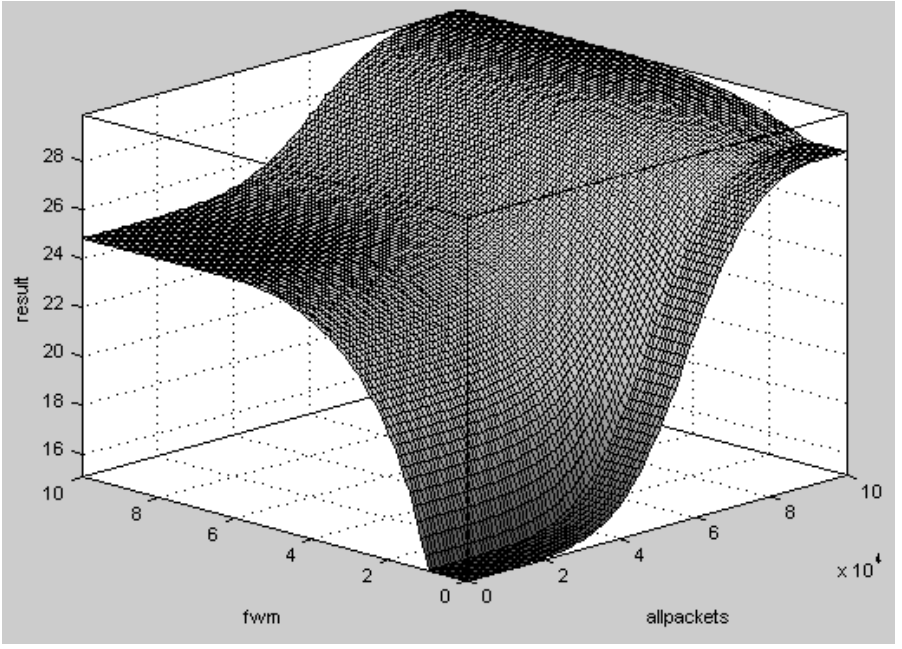

Рис. 5. Поверхность, отображающая зависимость результата вычислений от количества заблокированных обращений к сетевым ресурсам и общего числа пакетов

– проверка реакции компонентов СОПВ в условиях атаки «сканирование хоста» и воздействия вредоносного программного обеспечения;

– проверка производительности ОС при использовании компонентов СОПВ.

В ходе тестирования было оценено снижение производительности АС, возникающее в ходе функционирования системы СОПВ. Максимальная задержка выполнения операций составила 12,21 мс.

В заключение отметим, что основным отличием предложенной архитектуры СОПВ от существующих аналогов является использование модуля аппаратной виртуализации, применение комбинированных методов обработки информации и разделение функций системы на два уровня (локальный и глобальный). Программная реализация прототипа СОПВ и проведенное тестирование подтвердили возможность формирования предложенной архитектуры для организации эффективной защиты от вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. Лукацкий А.В. Обнаружение атак. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2003. 608 с.
2. Приказ ФСТЭК России от 06.12.2011 г. № 638. URL: http://www.fstec.ru/
3. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику. Винница: Изд-во Винницкого гос. техн. ун-та, 2001. 198 с.
4. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ-Петербург, 2003. 736 с.

Статья поступила в редакцию 25.10.2012