ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

УДК 681.3

Л. М. Груздева, М. Ю. Монахов

ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ КОРПОРАТИВНОЙ СЕТИ В УСЛОВИЯХ ВОЗДЕЙСТВИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Формализована задача повышения производительности в условиях воздействия угроз информационной безопасности корпоративной сети как задача построения системы защиты, обеспечивающей максимально возможный уровень производительности сети при достоверном обнаружении и эффективном противодействии угрозам информационной безопасности.

Ключевые слова: *корпоративная сеть передачи данных, производительность, система защиты информации, угрозы информационной безопасности.*

Введение. Основными причинами интереса к вопросам повышения производительности корпоративной сети передачи данных (КСПД) являются возрастающая структурная сложность и размерность современных сетей, характеризующихся множественными изменяющимися во времени информационными связями, а также потребности в увеличении уровня информационной безопасности.

Снижение производительности сетей связано с недостаточной защищенностью вследствие широкого использования слабозащищенных протоколов HTTP, SNMP, FTP, TCP/IP; участия в процессе обработки информации пользователей различных категорий, их непосредственного и одновременного доступа к системным ресурсам и процессам. Современная система защиты информации (СЗИ), даже включающая систему обнаружения и предотвращения атак и вторжений IPS/IDS, не может гарантировать обнаружения 70 % информационных атак, что периодически приводит к значительному возрастанию вредоносного трафика (ВТ). В настоящее время актуальны задачи повышения достоверности обнаружения информационных атак, их идентификации, а также разработки методов и средств снижения их влияния на производительность КСПД.

Постановка задачи

1. Дано множество объектов КСПД $O = \{O_1, O_2, ..., O_{NS}\}$. Линии связи абсолютно надежны, помехоустойчивы и состоят из дуплексного канала; узлы коммутации (маршрутизаторы сегментов КСПД) имеют бесконечную память; трафик состоит из пакетов одинакового приоритета и образует пуассоновский поток; длительность обработки пакетов в узлах определяется экспоненциальным законом распределения.

2. СЗИ включает модули защиты, в состав которых входит средство обнаружения (СО, SO) воздействия угроз информационной безопасности (ИБ) из множества

$SO = \{SO_1, SO_2, ..., SO_N\}$ и средство противодействия (СП, SP) угрозам ИБ из множества $SP = \{SP_1, SP_2, ..., SP_M\}$.

3. Каждый элемент множества *SO* обладает следующими характеристиками: $p_i(t)\ \left(i = \overline{1, N}\right)$ — вероятность обнаружения угроз ИБ; $\overline{p_i}(t)\ \left(i = \overline{1, N}\right)$ — вероятность возникновения „ложной тревоги“; $t_{\text{об}i}\ \left(i = \overline{1, N}\right)$ — время обнаружения угроз ИБ, за которое достигается максимальное значение вероятности обнаружения угроз ИБ, т.е. $p_i^{\max} = \lim\limits_{t \to t_{\text{об}i}} p_i(t)$.

4. Каждый элемент множества *SP* обладает следующими характеристиками: $q_j(t)\ \left(j = \overline{1, M}\right)$ — вероятность противодействия угрозам ИБ; $t_{\text{пр}j}\ \left(j = \overline{1, M}\right)$ — время противодействия, за которое достигается максимальное значение вероятности противодействия, т.е. $q_j^{\max} = \lim\limits_{t \to t_{\text{пр}j}} q_j(t)$.

Требуется: обеспечить максимально возможный уровень производительности КСПД при достоверном обнаружении и максимально эффективном противодействии угрозам ИБ:

$$\left.\begin{array}{l} \Phi(\Pi) \to \max; \\ P_{\text{об}}(t) \to \max;\ \ \overline{P_{\text{ЛТ}}}(t) \to \min;\ Q_{\text{пр}} \to \max; \\ T_{\text{об}} + T_{\text{пр}} \le T_{\text{д}}, \end{array}\right\} \qquad (1)$$

где Ф(П) — производительность КСПД; $P_{\text{об}}(t) = \varphi_1\left(p_1(t),\ p_2(t), ..., p_N(t)\right)$ — вероятность обнаружения угроз ИБ; $\overline{P_{\text{ЛТ}}}(t) = \varphi_2\left(\overline{p_1}(t),\ \overline{p_2}(t), ..., \overline{p_N}(t)\right)$ — вероятность возникновения „ложной тревоги“; $Q_{\text{пр}}(t) = \varphi_3\left(q_1(t),\ q_2(t), ..., q_M(t)\right)$ — вероятность противодействия угрозам ИБ; $T_{\text{об}} = \varphi_4\left(t_{\text{об}1}, t_{\text{об}2}, ..., t_{\text{об}N}\right)$ — время обнаружения угроз ИБ; $T_{\text{пр}} = \varphi_5\left(t_{\text{пр}1}, t_{\text{пр}2}, ..., t_{\text{пр}M}\right)$ — время противодействия угрозам ИБ; $T_{\text{д}}$ — допустимые временные затраты на обеспечение защиты (φ_1, φ_2, φ_3, φ_4 — виды соответствующих функциональных зависимостей).

Для решения поставленной задачи была разработана СЗИ [1], функционирование которой удобно рассмотреть с помощью структурной модели обнаружения и противодействия атакам на ресурсы КСПД (см. рисунок).

Уровень обнаружения — совокупность СО. На выходе СО формируется сигнал $X_i(t)$ $\left(i = \overline{1, N}\right)$, принимающий значение либо единица (угроза ИБ обнаружена), либо нуль (угроза ИБ не обнаружена). Сигнал $X_i(t)$ характеризуется плотностью распределения вероятности его появления — $f_y\left(X_i(t)\right)$ — угроза ИБ есть, а также $f_n\left(X_i(t)\right)$ — угрозы ИБ нет:

$$f_y(X_i(t)) = \begin{cases} p_i(t) & \text{при } X_i(t) = 1, \\ 1 - p_i(t) & \text{при } X_i(t) = 0, \end{cases} \quad f_n(X_i(t)) = \begin{cases} \overline{p_i}(t) & \text{при } X_i(t) = 1, \\ 1 - \overline{p_i}(t) & \text{при } X_i(t) = 0. \end{cases}$$

В процессе формирования уровня обнаружения должны выполняться следующие условия:

1) возможность совместной работы объединяемых СО;

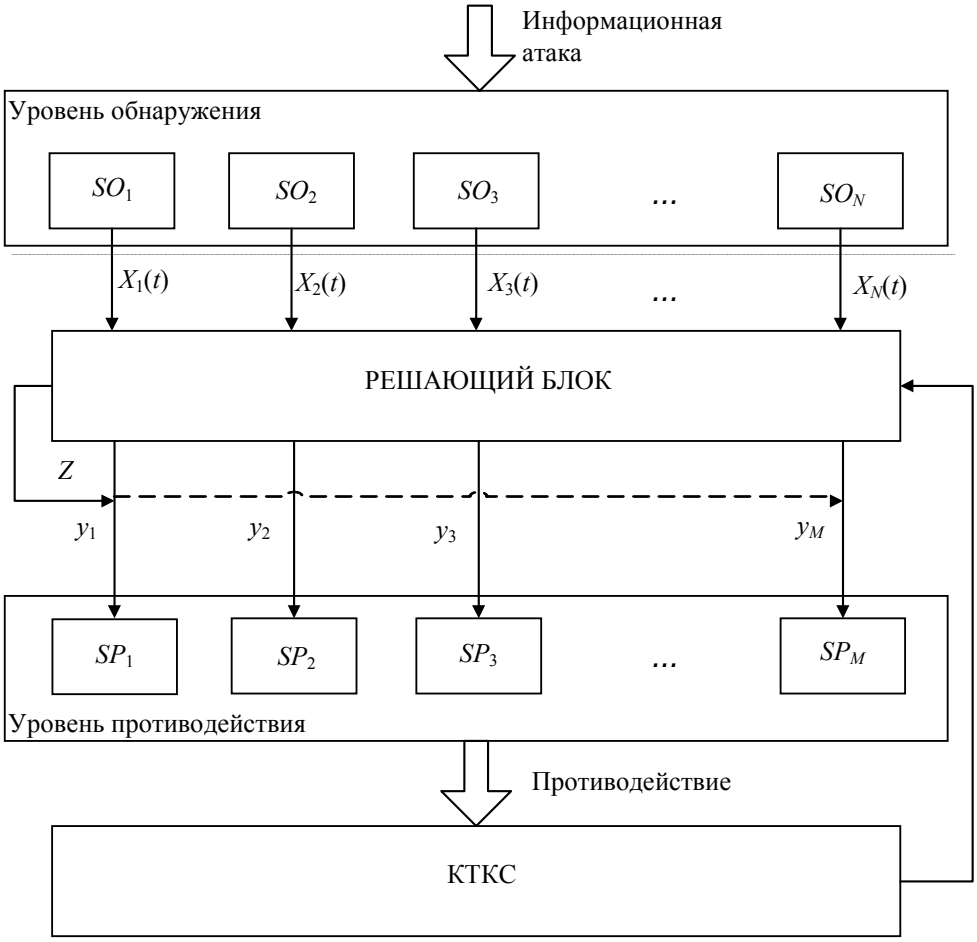
2) обеспечение оптимального времени работы по обнаружению и противодействию уг-

розам ИБ;

3) обеспечение заданной вероятности обнаружения угроз ИБ;

4) снижение средней частоты появления „ложных тревог“.

В статье [2] предложен алгоритм работы уровня обнаружения, основанный на понятии „критическая область угроз“ (КОУ). Достоинством алгоритма является учет возможного взаимного влияния различных СО, так как КОУ строится по вероятностным характеристикам уровня обнаружения, а не его отдельных модулей.



Уровень противодействия — совокупность СП, каждое из которых может быть задействовано при обнаружении угрозы ИБ.

Решающий модуль реализует следующий алгоритм: на основании показаний СП $\left(X_1(t),\ X_2(t),...,X_N(t)\right)$ принимается решение о наличии или отсутствии угроз ИБ:

$$Z=\begin{cases}1,\ \text{если угроза ИБ обнаружена,}\\ 0 \text{ — в противном случае.}\end{cases}$$

Если $Z=1$, то вырабатывается управляющее воздействие $\left(y_1,\ y_2,...,y_M\right)$, иначе — конец алгоритма.

В работе [1] предложен алгоритм определения узлов КСПД, в которых должны быть использованы СП при обнаружении угроз ИБ:

1) для каждого варианта инициирования уровня противодействия вычисляются вероятность $Q_{\text{пр}}(t)$ и производительность $\Phi(\Pi)$;

2) выбирается вариант использования СП, которому соответствует максимально возможная вероятность $Q_{\text{пр}}(t)$ при $\Phi(\Pi)\to\max$.

Реализация алгоритма позволяет обеспечить максимально возможное противодействие угрозам ИБ при максимально высоком уровне производительности.

Алгоритм работы СЗИ

Шаг 1. Запуск средств обнаружения. Время обнаружения $t = 0$.

Шаг 2. Снятие показаний, генерируемых СО $\left(X_1(t),\ X_2(t),...,X_N(t)\right)$.

Шаг 3. Если $X_1(t) = X_2(t) = ... = X_N(t) = 0$, то угроза ИБ не обнаружена $(Z = 0)$ и запуск средств уровня противодействия не производится, переход к шагу 2. В противном случае — $Z = 1$.

Шаг 4. Определение вероятностных характеристик:

$P_{\text{об}}(t) = \varphi_1\left(p_1(t),\ p_2(t),...,p_N(t)\right)$ — вероятность обнаружения угроза ИБ системой защиты; $\overline{P_{\text{ЛТ}}}(t) = \varphi_2\left(\overline{p_1}(t),\ \overline{p_2}(t),...,\overline{p_N}(t)\right)$ — вероятность возникновения „ложной тревоги“ СЗИ; $\Phi(P_{\text{об}}(t),\ \overline{P_{\text{ЛТ}}}(t))$ — критерий достоверности.

Шаг 5. Если $\Phi(P_{\text{об}}(t),\ \overline{P_{\text{ЛТ}}}(t)) \le \Phi_{\text{пор}}$ (значение критерия достоверности ниже порогового), то угроза ИБ не обнаружена и запуск средств уровня противодействия не производится, переход к шагу 2. В противном случае — $Z = 1$.

Шаг 6. Определение стохастической маршрутной матрицы $P_R(t)$.

Шаг 7. Запуск алгоритма определения узлов КСПД, в которых должны быть инициированы средства противодействия. Вырабатывается управляющее действие $Y = \left(y_1,\ y_2,...,y_M\right)$.

Шаг 8. Инициирование уровня противодействия в соответствии с $Y = \left(y_1,\ y_2,...,y_M\right)$. Конец алгоритма.

Выводы. Реализация предложенной модели организации защитных механизмов в КСПД позволяет обеспечивать требуемый уровень производительности за счет выбора алгоритма раннего и достоверного обнаружения угроз ИБ и оперативного использования средства противодействия угрозам ИБ в наиболее уязвимых узлах КСПД.

СПИСОК ЛИТЕРАТУРЫ

1. *Груздева Л. М.* Модели повышения производительности корпоративных телекоммуникационных сетей в условиях воздействия угроз информационной безопасности: Дис. … канд. техн. наук. Владимир: Изд-во Владим. гос. ун-та, 2011.

2. *Груздева Л. М., Монахов М. Ю.* Алгоритм раннего обнаружения атак на информационные ресурсы АСУП // Автоматизация в промышленности. 2008. № 3. С. 12—14.

3. *Груздева Л. М., Монахов М. Ю.* Алгоритм оптимизации функционирования распределенной системы защиты // Вестн. Костромского гос. ун-та им. Н. А. Некрасова. Сер. Техн. и естеств. науки „Системный анализ. Теория и практика“. 2008. Т. 14, № 2. С. 80—82.

Сведения об авторах

Людмила Михайловна Груздева — канд. техн. наук; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: glm@vlsu.ru

Михаил Юрьевич Монахов — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; заведующий кафедрой; E-mail: mmonakhov@vlsu.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.