МОДЕЛЬ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Л.М. Груздева (Москва)

По мере развития и усложнения корпоративных телекоммуникационных сетей (КТКС) повышается уязвимость информационных процессов и ресурсов, напрямую влияющая на производительность сети. Реализация угроз информационной безопасности (ИБ) способна создавать ситуацию невозможности эффективного выполнения основных функций КТКС, а также полностью блокировать ее работу.

Основную причину снижения производительности сетей специалисты связывают с недостаточной защищенностью информации и конкретно с информационными атаками злоумышленников.

В [1] формализована задача повышения производительности в условиях воздействия угроз информационной безопасности КТКС как задача построения системы защиты (СЗИ), которая смогла бы обеспечить максимально возможный уровень производительности сети при достоверном обнаружении и максимально эффективном противодействии угрозам ИБ. Для решения поставленной задачи была разработана модель распределенной СЗИ, позволяющая одновременно использовать различные технологии обнаружения и противодействия угрозам ИБ [1].

При реализации предложенной СЗИ авторы столкнулись с проблемой ухудшения системных характеристик КТКС. Очевидно, это происходило из-за того, что средства противодействия (СП), работая с предельной эффективностью, вносили значительные временные задержки в работу узлов сети. В результате проведенных экспериментов было выявлено, что отключение ряда СП не влекло к значительному снижению показателя защищенности, в то время как уменьшалась средняя задержка обмена информацией.

В статье предлагается алгоритм определения узлов сети, в которых должны быть инициированы средства противодействия при обнаружении угроз ИБ.

Модель КТКС. Рассмотрим разомкнутую модель КТКС, состоящую из источника пакетов (узел 0) и K СМО M/M/m_1/∞, M/M/m_2/∞, …, M/M/m_K/∞. В общем случае разомкнутая СеМО задается стохастической маршрутной матрицей $P_R = \left\| p_{ij} \right\|$, где p_{ij} – вероятность пересылки пакета из i-го узла в j-й узел, причем $\sum_{j=0}^{K} p_{ij} = 1 \ \forall i = \overline{0,\ K}$. Средняя задержка пакетов в сети является одной из основных ее характеристик производительности.

На рис.1 представлена схема алгоритма инициирования средств противодействия угрозам ИБ в разомкнутой КТКС.

Выбор варианта инициирования средств противодействия. Определим для конкретности K-й узел как защищаемый ресурс разомкнутой СеМО. В каждом i-м узле $(i = \overline{1,\ K-1})$ может быть инициировано СП, способное с вероятностью u_i противодействовать угрозам ИБ. В системе всего $2^{(K-1)} - 1$ варианта инициирования СП, его номер численно равен двоичному числу: $j = (x_1\ x_2\ \ldots\ x_{M-1})_2$, где $x_i = \begin{cases} 0, \text{ если СП не инициируется в } i-\text{м узле} \\ 1, \text{ если СП инициируется в } i-\text{м узле} \end{cases} (i = \overline{1,\ K-1})$.

Пусть в сети протекает случайный процесс распространения вредоносной программы (ВПр), предназначенной для реализации угроз информации, хранящейся в КТКС либо для скрытого нецелевого использования ресурсов, либо иного воздействия, препят-

ствующего нормальному функционированию сети. В этом случае СеМО может находиться в одном из дискретных состояний s_0, $s_1,...,s_K$. Переход из s_i состояния в s_j происходит с вероятностью p_{ij} и означает, что ВПр*i*-го узла заразила *j*-й узел $(i, j = \overline{0, K})$.

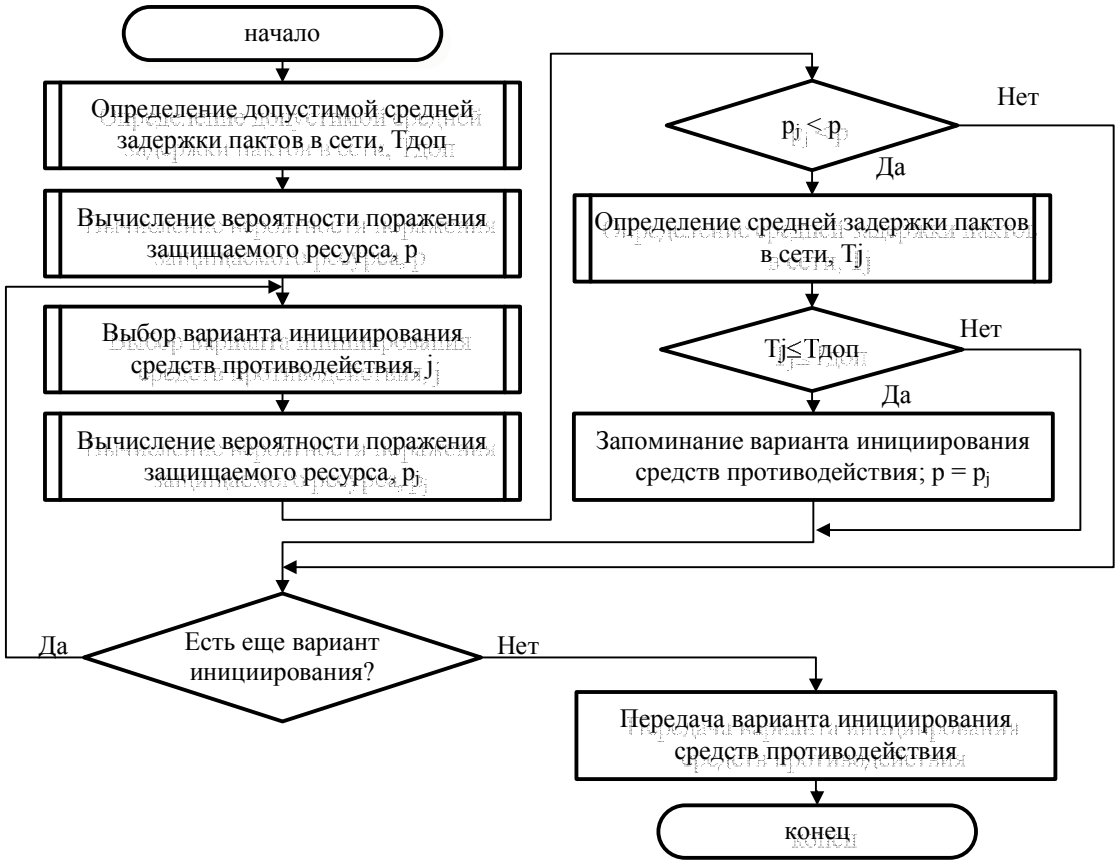

Рис. 1. Схема алгоритма инициирования СП разомкнутой КТКС

Пусть в начальный момент времени СеМО находится в состоянии s_0, т.е. ВПр находится в нулевом узле (источнике пакетов), при этом остальные узлы не заражены. В результате случайного процесса распространения ВПр происходит заражение восприимчивых узлов.

Алгоритм вычисления вероятности противодействия простым одиночным угрозам ИБ без возвращений.

Шаг 1. Построить матрицу Q на основе элементов матрицы P_R, введя в нее поглощающие состояния s_0 и s_K (ВПр может покинуть систему без заражения *K*-го узла).

$$Q = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ p_{10} & p_{11} & p_{12} & \cdots & p_{1K} \\ p_{20} & p_{21} & p_{22} & \cdots & p_{1K} \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}. \quad (1)$$

Шаг 2. Если в системе нет СП, то перейти на шаг 3. В противном случае по номеру *j* ввести в (1) противодействие угрозам ИБ. Под противодействием будем понимать выброс ВПр в 0-й узел.

$$Q=\begin{pmatrix} 1 & 0 & \dots & 0 \\ p_{10} & p_{11} & \dots & p_{1K} \\ p_{i0}+u_i\cdot(1-p_{i0}) & (1-u_i)p_{i1} & \dots & (1-u_i)p_{iK} \\ 0 & 0 & \dots & 1 \end{pmatrix}, \quad (2)$$

где $u_i (i=\overline{1,\ K-1})$ – вероятностью противодействия ВП.

Шаг 3. Задать вектор распределения вероятностей на нулевом шаге: $e=(0,\ p_{01}, p_{01},...,p_{0K}\ )$.

Шаг 4. Найти распределение вероятностей состояний на *n*-м шаге по формуле: $q(n)=e\cdot Q^n$. Будем считать процесс распространения ВПр завершенным на шаге *n*, если $p_1(n)=p_2(n)=...=p_{K-1}(n)=0$. Вероятность поражения защищаемого ресурса $p_j=p_K(n)$, вероятность противодействия $Q_{ПР}(t)=p_0(n)$. Конец алгоритма.

Результаты моделирования. Для реализации данного алгоритма было проведено имитационное моделирование процесса распространения ВПр в сети из семи узлов. При обработке данных по всем вариантам инициирования СП $\left(2^{(7-1)}-1=63\right)$ было выявлено: в действующей сети без СП вероятность поражения p_0 = 0,550; при инициировании СП (u = 0,9) в каждом узле сети – p_{63}= 0,112, средняя задержка пакета в сети T увеличилась на ≈30%; при включении СП только в первом, втором и третьем узлах сети – p_{56} = 0,176, значение T увеличилось на ≈ 8%.

Алгоритм вычисления вероятности противодействия угрозам ИБ простым одиночным угрозам ИБ с возвращением.

Шаг 1. Построить матрицу Q на основе элементов матрицы P_R, введя в нее поглощающее состояния s_K (атака будет продолжать до тех пор пока не будет заражен *K*-й узел).

$$Q=\begin{pmatrix} 0 & p_{01} & p_{02} & \dots & p_{0K} \\ p_{10} & p_{11} & p_{12} & \dots & p_{1K} \\ p_{20} & p_{21} & p_{22} & \dots & p_{1K} \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}. \quad (3)$$

Шаг 2. Если в узлах нет СП, то перейти на шаг 3. В противном случае по номеру j ввести в (3) противодействие угрозам ИБ. Под противодействием будем понимать выброс ВПр в (K+1)-й узел.

$$Q=\begin{pmatrix} 0 & p_{01} & \dots & p_{0K} & 0 \\ p_{10} & p_{11} & \dots & p_{1K} & 0 \\ (1-u_i)\cdot p_{i0} & (1-u_i)\cdot p_{i1} & \dots & (1-u_i)\cdot p_{iK} & u_i \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}. \quad (4)$$

Шаг 3. Задать вектор распределения вероятностей на нулевом шаге $e=(1,\ 0,\ 0,...,0\ )$.

Шаг 4. Найти распределение вероятностей состояний на *n*-м шаге по формуле: $q(n)=e\cdot Q^n$. Будем считать процесс распространения ВПр завершенным на шаге *n*, если $p_1(n)=p_2(n)=...=p_{K-1}(n)=0$. Вероятность поражения защищаемого ресурса $p_K(n)$, вероятность противодействия $Q_{ПР}(t)=p_{K+1}(n)$. Конец алгоритма.

Результаты моделирования. Имитационное моделирование показало, что реализация угрозы ИБ с помощью ВПр в разомкнутой СеМО без СП будет успешной на 45 шаге. Если инициировать СП только в 1-м узле сети, то будет достигнута наибольшая вероятность противодействия угрозам ИБ – $Q_{ПР}(t) = p_8(22) = 0{,}546$ (табл. 1).

Таблица 1

Вероятности противодействия при инициировании СП в одном узле разомкнутой сети

Вероятность противодействия	Номер варианта инициирования СП					
	$j = 32$	$j = 16$	$j = 8$	$j = 4$	$j = 2$	$j = 1$
	Шаг окончания случайного процесса					
	$n = 22$	$n = 33$	$n = 40$	$n = 41$	$n = 34$	$n = 43$
$Q_{ПР}(t)$	0,546	0,405	0,498	0,408	0,435	0,398

При обработке данных по всем вариантам инициирования СП $\left(2^{(7-1)} - 1 = 63\right)$ было выявлено: в действующей сети без СП вероятность поражения $p_0 = 1{,}000$; при инициировании СП ($u = 0{,}7$) в каждом узле сети – $p_{63} = 0{,}145$, средняя задержка пакета в сети T увеличилась на ≈30%; при включении СП только в 1-м, 2-м, 3-м и 4-м узлах сети – $p_{60} = 0{,}158$, значение T увеличилось на ≈ 10%.

Выводы

Оперативное инициирование средства противодействия угрозам ИБ в наиболее уязвимых узлах КТКС позволяет обеспечить максимально возможное противодействие угрозам ИБ без значительного увеличения средней задержки пакетов в КТКС. Результаты моделирования подтвердили практическую ценность предложенного подхода.

Литература

1. Груздева Л.М., Монахов М.Ю. Повышение производительности корпоративной сети АСУ в условиях воздействия угроз информационной безопасности // Известия высших учебных заведений. Приборостроение. – 2012. – Т. 55. – № 8. – С.53–56.