2. Hatamian M., Gash G. L. A 70 MHz 8-bit*8-bit parallel pipelined multiplier in 2.5 micron CMOS // IEEE J. Solid-State Circuits. 1986. Vol. SC-21, № 4. P. 505-513.

3. Hatamian M., Gash G. L. Parallel bit-level pipelined VLSI designs for High-speed signal processing // Processings of the IEEE. 1987. Vol. 75, № 9. P. 1192–1202.

S. E. Mironov, N. M. Safyannikov, A. K. Frolkin
Saint-Petersburg state electrotechnical university «LETI»

METHODIC OF STRUCTURAL AND TOPOLOGICAL OPTIMIZATION REGULAR VLSI MACRO-BLOCKS

The questions of structural optimization of VLSI regular macro-blocks layout are considered in examples the pipelined multiplier. Methodic of structure and topological optimization for regular VLSI macro-blocks to reduce area of SoC is suggested, using the analysis results processes of reorganizations of layout plans VLSI macro-blocks.

Regular VLSI macro-blocks, structural and topological optimization, pipelined multiplier

УДК: 20.53.19, 28.23.13

Е. Г. Воробьёв
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Расчет эффективности информационных атак внешнего нарушителя на объекты информатизации с распределенной инфраструктурой

Представлен математический аппарат для расчета эффективности информационных атак внешнего нарушителя на объекты информатизации с распределенной инфраструктурой. Представлены примеры расчета показателей эффективности. Материалы данной статьи могут быть использованы для градации защищенности объектов информатизации, отображаемых в целевых программных комплексах, от информационных воздействий.

Эффективность информационных атак, классы безопасности, факторы, влияющие на информацию

В настоящее время большое внимание уделяется разработке концепции обеспечения непрерывности функционирования объектов информатизации страны в условиях целенаправленных информационных атак.

Практически все известные подходы к оценке защищенности объектов информатизации базируются на анализе модели угроз и модели нарушителя, математический аппарат которых не подходит для получения точных оценок возможного ущерба. Кроме того, предполагается, что механизмы защиты действуют только внутри защищаемой системы и не оказывают ответного воздействия на внешнего нарушителя.

Тем не менее, существуют ситуации, когда возможны ответные действия, например: при обнаружении сканирования портов, что еще не является атакой, начать ответное сканирование по IP-адресу источника угрозы или отправить по нему компьютерный вирус, что позволяет в большинстве случаев сорвать атаку на объект информатизации, так как нарушитель понимает, что раскрыт. Не углубляясь в специальные области, можно считать, что на самом деле возможности конфликтующих сторон по нанесению ущерба примерно равны, если обе стороны активно к этому готовятся.

В данной статье предлагается математический аппарат, строго ориентированный на вопро-

сы такого конфликта, который объективно отражает все возможные ситуации при программно-технических воздействиях сторон друг на друга, когда обе стороны являются в современной терминологии внешними нарушителями по отношению друг к другу. Ограничения сделаны только на применение прямого антропогенного метода воздействий и влияние стихийных факторов, влияющих на информацию. И, наконец, будем рассматривать нарушителя с решительными целями – уничтожить или блокировать информацию (т. е. нарушить ее физическую целостность и доступность) посредством выведения из строя аппаратных и программных комплексов.

В настоящее время для решения математических задач, аналогичных задачам оценки результатов конфликта, применяется теория игр [1], [2]. Кроме того, как и любое оружие, информационные средства воздействия имеют характерные результаты своего применения – выведение из строя аналогичных средств конфликтующей стороны, что позволяет применять типовые подходы. Тем не менее, имеются существенные отличия в самой природе воздействий и методах реализации, которые требуется учитывать. Будем также считать, что информационная атака состоит в последовательном выполнении n информационных воздействий (в общем случае – разной природы) для получения некоторого целевого эффекта.

Расчет эффективности информационных атак на территориально распределенные вычислительные системы. Особенностью современных компьютерных технологий является возможность информационного воздействия одной атакующей вычислительной системой (АВС) на сотни тысяч и даже миллионы компьютеров, широко территориально расположенных и зачастую находящихся в разных странах мира.

Рассмотрим случай информационной атаки на вычислительные системы определенного региона в целом.

Математическое ожидание доли успешно атакованных средств распределенной вычислительной системы (РВС) при n информационных воздействиях определяется по формуле

$$\mu(n) = 1 - \prod_{i=1}^{n} (1 - \mu_i),$$

где μ_i – математическое ожидание доли успешно атакованных средств распределенной вычислительной системы i-м информационным воздействием. Если математические ожидания доли успешно атакованных средств распределенной вычислительной системы каждым информационным воздействием одинаковы, то

$$\mu(n) = 1 - (1 - \mu)^n.$$

Если значения μ_i невелики, то можно пользоваться формулой

$$\mu(n) = 1 - \exp\left(-\sum_{i=1}^{n} \mu_i \right)$$

и определять математическое ожидание общего количества удачно атакованных средств распределенной вычислительной системы при n успешных информационных воздействиях по формуле

$$\bar{S}_{\text{РВС}} = S_{\text{РВС}} \left[1 - \exp\left(-\frac{1}{S_{\text{РВС}}} \sum_{i=1}^{n} \bar{S}_i \right) \right], \qquad (1)$$

где S_i – математическое ожидание общего количества успешно атакованных средств, достигаемое i-м информационным воздействием.

Если для всех видов атак S_i – одинаковы ($S_1 = S_2 = ... = S_n = S_0$), то формула (1) примет вид

$$\bar{S}_{\text{РВС}} = S_{\text{РВС}} \left[1 - \exp\left(-\frac{\bar{S}_0 n}{S_{\text{ц}}} \right) \right],$$

где $S_{\text{ц}}$ – математическое ожидание количества успешно атакованных целевых систем.

До воздействия по целевой системе защищающейся стороной может быть оказано противодействие как самим АВС – превентивными информационными или физическими воздействиями, так и применяемым видам информационных атак – использованием системы защиты информации (СЗИ).

Если для выполнения каждой отдельной задачи в ходе информационной атаки производится несколько (n) информационных воздействий, то в результате противодействия защищающейся стороны с определенными вероятностями возможны следующие гипотезы: все воздействия будут нейтрализованы; достигнут цели одно, два и т. д. (в общем случае m); окажутся успешными все воздействия.

Ранее были даны методы расчета показателя эффективности при условии, что на целевую систему оказывается определенное (n) число информационных воздействий. Безусловный пока-

затель эффективности выполнения задачи в ходе информационного конфликта с учетом противодействия защищающейся стороны вычисляется по формуле

$$\tilde{W} = \sum_{m=1}^{n} Q_m W(m), \qquad (2)$$

где Q_m – вероятность того, что в результате противодействия будут эффективными ровно m информационных воздействий:

$$Q_m = C_n^{n-m} p^{n-m} (1-p)^m = C_n^m p^{n-m} (1-p)^m; \quad (3)$$

$W(m)$ – показатель эффективности, вычисленный при условии, что АВС оказывают ровно m воздействий на целевую систему; n – общее число воздействий для выполнения отдельной информационной атаки.

Расчет можно проводить как для одной АВС, последовательно реализующей все воздействия, так и для параллельной работы АВС.

Пример 1. Для DDOS-атаки РВС в определенном регионе страны применяются 3 АВС (n = = 3). Воздействие каждой АВС независимо от других может быть нейтрализовано с вероятностью p = 0.20. Если воздействовать сможет одна АВС, средняя доля успешно атакованных информационных систем РВС в регионе $\mu(1)$ = 0.40, если две АВС – $\mu(2)$ = 0.60, если 3 АВС – $\mu(3)$ = = 0.70. Найти среднюю долю успешно атакованных информационных систем в указанном регионе с учетом противодействия.

Решение. Для определения Q_m – вероятности того, что сохранится m АВС (m = 1, 2, 3), воспользуемся формулой (3).

Получим:

$$Q_1 = 3p^2(1-p) = 3 \cdot 0.2^2 (1 - 0.2) = 0.096;$$
$$Q_2 = 3p(1-p)^2 = 3 \cdot 0.2 (1 - 0.2)^2 = 0.384;$$
$$Q_3 = (1-p)^3 = (1 - 0.2)^3 = 0.512.$$

По формуле (2) найдем

$$\mu = \sum_{m=1}^{3} Q_m \mu(m) =$$
$$= 0.096 \cdot 0.4 + 0.384 \cdot 0.6 + 0.512 \cdot 0.7 = 0.63.$$

Расчет вероятности достижения цели информационной атаки. Защищающаяся сторона может противодействовать применяемым АВС, блокируя опасные информационные воздействия раньше, чем они дойдут до цели, например посредством создания многоуровневых СЗИ. При независимых воздействиях, показательном законе поражения информационных систем, одинаковой вероятности достижения цели (p) для всех воздействий и числе пропущенных СЗИ воздействий, подчиняющемся биномиальному закону, вероятность достижения цели информационной атаки определяется по формуле

$$W_n = 1 - \left(1 - \frac{pQ(n)}{\omega}\right)^n, \qquad (4)$$

где $Q(n)$ – средняя вероятность того, что каждый из применяемых видов (сценариев) воздействий в ходе атаки не будет перехвачен (блокирован) СЗИ.

Принимая распределение числа пропущенных воздействий подчиняющимся закону Пуассона, получим

$$W_n = 1 - \exp\left(-\frac{npQ(n)}{\omega}\right). \qquad (5)$$

Обе формулы являются приближенными вследствие допущения о законе распределения числа пропущенных воздействий. При малом значении $pQ(n)/\omega$ результаты расчетов по формулам (4) и (5) практически совпадают. При больших $pQ(n)/\omega$ расчет по формуле (5) даст значение меньшее по сравнению с расчетом по формуле (4). Следует иметь в виду, что замена истинного закона поражения целевой информационной системы показательным при малом числе атакующих информационных воздействий, а также неучет зависимости между видами воздействий и способами их реализации ведут к завышению результата.

Пример 2. По информационной системе планируется осуществить n = 8 информационных воздействий; вероятность получения целевого эффекта в результате каждого воздействия p = 0.10; среднее число воздействий для реализации цели атаки на информационную систему ω = 2.5. Средства защиты информации способны обнаружить и блокировать каждое из воздействий с вероятностью $P(n)$ = 0.25. Найти вероятность достижения цели информационной атаки.

Решение. Вероятность того, что каждое из воздействий не будет обнаружено и блокировано системой защиты, равна $Q(n) = 1 - P(n) = 1 - 0.25 =$ = 0.75.

По формуле (4) имеем результат расчета 0.22.

Результат, вычисленный по формуле (5), будет равен 0.21.

Противодействие атакующим вычислительным системам. Защищающаяся сторона может оказать противодействие АВС, лишая их дееспособности раньше, чем они смогут провести хотя бы одно информационное воздействие. Это может быть не только активное воздействие на вычислительные и другие средства атакующей стороны, но и пассивное, например блокирование известных IP-адресов настройкой листов доступа межсетевого экрана. Если для решения задачи выделено N АВС, то число сохранивших дееспособность к моменту применения в ходе информационной атаки будет случайным. АВС, сохранившие дееспособность, осуществляют информационное воздействие, которому также может быть оказано противодействие.

Если число АВС, сохранивших способность к воздействиям, считать подчиняющимся биномиальному закону распределения, вероятность сохранения дееспособности каждой из АВС – одинаковой, закон поражения целевой информационной системы – показательным, то вероятность достижения цели информационной атаки определяется по формуле

$$W_n = \sum_{m=0}^{N} C_N^m p_{\text{дАВС}}^m \left(1-p_{\text{дАВС}}\right)^{N-m}\left[1-\left(1-\frac{pQ}{\omega}\right)^{n'm}\right], \quad (6)$$

где N – общее число АВС, выделяемое для решения задачи; $p_{\text{дАВС}}$ – вероятность сохранения дееспособности каждой из АВС к моменту применения в ходе атаки; n' – количество информационных воздействий, используемых в ходе атаки одной АВС; Q – вероятность того, что каждое из n применяемых информационных воздействий не будет блокировано противником.

Если Q является функцией числа n' одной АВС ($Q = Q(n')$), но не зависит от общего числа сохранивших дееспособность АВС, формула (6) принимает вид

$$W_n = 1-\left\{1-p_{\text{дАВС}}\left[1-\left(1-\frac{pQ(n')}{\omega}\right)^{n'}\right]\right\}^N. \quad (7)$$

Если Q зависит от общего числа воздействий в ходе информационной атаки ($\bar{n} = n'm$), т. е. от случайного числа m АВС, сохранивших дееспособность, то, принимая $\bar{n}$ равным среднему ожидаемому числу воздействий в ходе информационной атаки ($\bar{n} = Np_p n'$), можно пользоваться вместо формулы (7) приближенной формулой

$$W_n = 1-\left\{1-p_{\text{дАВС}}\left[1-\left(1-\frac{pQ(\bar{n})}{\omega}\right)^{n'}\right]\right\}^N. \quad (8)$$

Пример 3. Для информационной атаки центрального сервера в составе объектов информатизации выделено $N = 3$ АВС, каждая из которых в ходе информационной атаки применяет $n' = 4$ информационных воздействия. Вероятность сохранения дееспособности АВС к моменту начала информационной атаки $p_{\text{дАВС}} = 0.80$, вероятность того, что каждое из воздействий не будет обнаружено и блокировано системой защиты: $Q(\bar{n}) = 0.60$. Вероятность достижения цели одного воздействия по отношению к центральному серверу $p = 0.70$, среднее число удачных результатов воздействий для достижения цели информационной атаки w (ω) = 4. Определить вероятность достижения цели информационной атаки.

Решение. Используя формулу (8) получим:

$$W_n = 1-\left\{1-p_{\text{дАВС}}\left[1-\left(1-\frac{pQ(\bar{n})}{\omega}\right)^{n'}\right]\right\}^N = 0.64.$$

Влияние технической надежности атакующих вычислительных систем. В период выполнения информационной атаки возможны технические неисправности АВС и средств реализации информационных воздействий (как программных, так и аппаратных), которые использует АВС.

Считая независимой техническую надежность каждого из применяемых в атаке средств реализации информационных воздействий, а также каждой используемой АВС в целом, эффективность реализации информационной атаки можно определить по приближенной формуле

$$W_{N_m} = 1-\left\{1-p_{\text{дАВС}}Q_{\text{т.н}}\left[1-\left(1-\frac{pQ(\bar{n})Q_{\text{т.к}}}{\omega}\right)^{n'}\right]\right\}^N,$$

где W_{N_m} – эффективность реализации информационной атаки с учетом противодействия СЗИ противника средствам реализации информационных воздействий, АВС и технической надежности средств реализации информационных воздействий, а также каждой используемой АВС в целом; $Q_{\text{т.н.}}$ – техническая надежность АВС (например, как средства вычислительной техники), т. е. вероятность того, что за период выполнения информационной атаки она не выйдет из строя вследствие технических неисправностей; $Q_{\text{т.к}}$ – техническая

надежность применяемых в ходе информационной атаки средств реализации информационных воздействий (например, специальных прикладных программ).

Противодействие СЗИ при массированном использовании информационных воздействий. При массированном использовании информационных воздействий в ходе информационных атак число их, преодолевших СЗИ, можно считать подчиняющимся пуассоновскому закону распределения. Если в ходе информационной атаки используются однотипные информационные воздействия (например, в ходе DOS-атаки генерируются сотни тысяч однотипных запросов), защищающаяся сторона будет стремиться распределять потенциал СЗИ по объектам и элементам своей вычислительной системы (сети) равномерно. Математическое ожидание доли пораженных объектов (средняя вероятность поражения каждого из объектов информатизации) определяется по формуле

$$W = 1 - \exp\left(- \frac{\alpha \exp\left(- \frac{\beta}{n_{\text{в}}} \right)}{N_{\text{ц}}} \right),$$

где α – общий поражающий потенциал информационных воздействий в ходе информационной атаки; β – общий защитный потенциал СЗИ против информационных воздействий, создаваемых АВС; $n_{\text{в}}$ – количество информационных воздействий в ходе атаки; $N_{\text{ц}}$ – количество целевых информационных систем или их элементов, по которым производятся информационные воздействия. Математическое ожидание числа пораженных объектов информатизации или их элементов

$$\bar{N}_0 = N_0 W = N_0 \left[1 - \exp\left(- \frac{\alpha \exp\left(- \frac{\beta}{n_{\text{в}}} \right)}{N_{\text{ц}}} \right) \right], \quad (9)$$

где N_0 – количество объектов информационных воздействий.

В общем случае $N_{\text{ц}} \neq N_0$. В условиях противодействия СЗИ, создаваемого защищающейся стороной, в частности по технологии HoneyNet, АВС могут проводить информационную атаку по целевым системам, в числе которых не только назначенные объекты N_0, имеющие реальную ценность, но и ложные объекты информатизации и элементы вычислительных комплексов и сетей. При отсутствии таких ложных объектов $N_0 = N_{\text{ц}}$. В общем же случае

$$N_{\text{ц}} = N_0 + N_{\text{л.о}},$$

где $N_{\text{л.о}}$ – количество ложных объектов и элементов, по которым распределяются информационные воздействия, создаваемые АВС. Если в результате действий СЗИ кроме главных объектов атакуются второстепенные (например, сами механизмы защиты), то они должны включаться в число $N_{\text{л.о}}$.

Значение α определяется по формуле

$$\alpha = \frac{P_{\text{в}} n_{\text{в}} N_{\text{АВС}}}{\omega_{\text{в}}},$$

где $P_{\text{в}}$ – вероятность достижения цели информационного воздействия; $n_{\text{в}}$ – число информационных воздействий в ходе атаки, применяемых АВС; $\omega_{\text{в}}$ – среднее число информационных воздействий, необходимое для реализации цели информационной атаки; $N_{\text{АВС}}$ – число АВС.

Общий оборонительный потенциал β слагается из потенциала встроенных средств защиты информации защищаемого объекта β_1 и защитного потенциала внешних по отношению к защищаемому объекту элементов СЗИ β_2. Если $\beta_2 = 0$, то отражение информационного воздействия производится только собственными (встроенными) механизмами защиты. При $\beta_1 = 0$ защищаемые объекты атаки не имеют встроенных средств защиты информации. Потенциалы β_1 и β_2 определяются по формулам:

$$\beta_1 = \sum_{i=1}^{N_r} \left(\frac{P_{\beta_i} n_{\beta_i}}{\omega_{\beta_i}} \right),$$

$$\beta_2 = \sum_{j=1}^{N_S} \left(\frac{P_{\beta_j} n_{\beta_j}}{\omega_{\beta_j}} \right).$$

где P_{β_i} и P_{β_j} – вероятности блокирования информационного воздействия i-го встроенного средства защиты (СЗ) и j-го внешнего СЗ; n_{β_i} и n_{β_j} – число уровней защиты, создаваемых i-м и j-м СЗ; ω_{β_i} и ω_{β_j} – среднее число операций i-го и j-го средств защиты, необходимое для выявления и блокирования информационного воздействия; N_r и N_s – число встроенных и внешних СЗ соответственно.

Пример 4. Объект информатизации в составе $N_0 = 6$ серверов атакуется $N_{\text{АВС}} = 9$ АВС. Каждая АВС применяет по $n_{\text{в}} = 4$ информационных воздействия. Вероятность реализации информаци-

онного воздействия на какой-либо из серверов $P_в = 0.45$. Среднее число необходимых информационных воздействий для реализации атаки на сервер $\omega_в = 2.5$. На серверах отсутствуют встроенные средства защиты информации. Система защиты состоит из подсистемы, реализованной активным сетевым оборудованием посредством создания защищенного периметра сети, которая использует $N_{r_1} = 8$ СЗ с характеристиками $P_{\beta_1} = 0.60$; $n_{\beta_1} = 2$, $\omega_{\beta_1} = 1$, и СЗ, основанным на применении АМДЗ, $N_{r_2} = 6$ комплексов с $P_{\beta_2} = 0.40$, $n_{\beta_2} = 2$, $\omega_{\beta_2} = 1$. Найти математическое ожидание числа пораженных серверов.

Решение. Общий потенциал СЗИ

$$\beta = N_{r_1}\left(\frac{P_{\beta_1} n_{\beta_1}}{\omega_{\beta_1}}\right) + N_{r_2}\left(\frac{P_{\beta_2} n_{\beta_2}}{\omega_{\beta_2}}\right).$$

Атакующий потенциал АВС $\alpha = \frac{P_в n_в N_{АВС}}{\omega_в} =$ = 6.5 реализованных информационных воздействий (округление необходимо проводить в меньшую сторону).

Математическое ожидание удачно атакованных серверов находим по формуле (9):

$$\bar{N}_0 = N_0 W = N_0\left[1 - \exp\left(-\frac{\alpha \exp\left(-\frac{\beta}{n_в}\right)}{N_ц}\right)\right] = 1.5 \text{ сервера.}$$

Округлять полученный результат в данном случае следует в меньшую сторону.

С помощью приведенного в статье математического аппарата для расчета эффективности программно-технических информационных воздействий в различных условиях информационных конфликтов возможна оценка предполагаемых потерь информации в центрах обработки данных и распределенных вычислительных системах, что увеличивает возможности экспертов при проведении оценки рисков и аудитов информационной безопасности.

Материалы данной статьи могут быть использованы также для градации защищенности информационно-технических объектов от информационных воздействий, отображаемых в специализированных программных комплексах.

СПИСОК ЛИТЕРАТУРЫ

1. Оуэн Г. Теория игр. М.: Изд-во ЛКИ, 2007.

2. Итеративные методы в теории игр и программировании / В. З. Беленький, В. А. Волконский, С. А. Иванков и др. М.: Наука, 1974.

E. G. Vorobiev
Saint-Petersburg state electrotechnical university «LETI»

CALCULATION OF EFFICIENCY OF INFORMATION ATTACKS OF THE EXTERNAL VIOLATOR TO OBJECTS OF INFORMATIZATION WITH THE DISTRIBUTED INFRASTRUCTURE

The mathematical method for calculation of efficiency of information attacks of the external violator to objects of informatization with the distributed infrastructure is presented in article. Examples of calculation of indicators of efficiency are presented. Materials of this article can be used for gradation of security of the objects of informatization displayed in target program complexes from information influences.

Efficiency of information attack, graduation of security, information influences