А. Ф. Белый

МЕТОД АНАЛИЗА ДВУСТОРОННИХ ПРОЦЕССОВ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ В КРИТИЧЕСКИ ВАЖНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ НА ОСНОВЕ МОДЕЛЕЙ ДИНАМИКИ СРЕДНИХ

В основу метода положена модель динамики средних, с использованием которой анализируется исход информационного противодействия (ИП) сторон при их заданных начальных параметрах. Однако эту модель можно применить лишь к строго определенной стратегии действий сторон, прежде всего это касается действия противостоящей стороны. Этот недостаток преодолевается в теории игр, создатели которой Дж. фон Нейман и О. Моргенштерн ввели такие основные понятия, как стратегия, цена игры, и обосновали эффективный путь для отыскания оптимальной стратегии, которая может быть как чистой, так и смешанной.

Применение теории игр в области ИП имеет ограничения, что объясняется двумя основными причинами. Одна состоит в возросшей сложности и разносторонности задач ИП. Дополнительная сложность задач ИП связана с наличием большого множества стратегий действий сторон при обеспечении функциональной устойчивости критически важной информационной системы (КВИС) на основе средств защиты информации и нарушении работы КВИС путем реализации компьютерных атак. Второй причиной является отсутствие методов, приводящих к количественным оценкам эффективности применения противоборствующими сторонами своих средств до их поэлементного анализа.

Дальнейшим шагом в описании игр на базе двусторонней модели стало развитие теории дифференциальных игр, в которой используются дифференциальные уравнения. Вопрос об управляемости КВИС в условиях компьютерных атак — основной вопрос, который решается на основе теории дифференциальных игр и теории оптимального управления. Обе эти теории дополняют друг друга: задачи оптимального управления можно превратить в дифференциальные игры, если ввести еще одного участника, а методы дифференциальных игр можно применять к задачам управления, рассматривая их как игры одного игрока. При исследовании двусторонних процессов ИП в КВИС используем аппарат теории дифференциальных игр, разработанной Р. Айзексом и Л. Понтрягиным.

Под процессом информационного противодействия будем понимать процесс изменения состояний информационных ресурсов (ИР) в условиях компьютерных атак при двусторонних действиях сторон.

Метод анализа двусторонних процессов информационного противодействия в КВИС на основе моделей динамики средних предназначен для системного анализа процесса изменения состояний информационных ресурсов КВИС в условиях компьютерных атак при двусторонних действиях сторон.

Предположено, что стороны располагают на момент начала ИП соответственно $r_1(0)$ и $r_2(0)$ однородными ИР КВИС. На момент времени t ресурс сторон понизится до уровня $r_1(t)$ и $r_2(t)$. За промежуток dt он изменится соответственно

$$\begin{cases} r_1(t+dt) = r_1(t) - p_2 dn_2(t) \\ r_2(t+dt) = r_2(t) - p_1 dn_1(t), \end{cases} \quad (1)$$

где $\rho 2$ и $\rho 1$ — вероятности поражения одной единицы ИР одной компьютерной атакой соответственно для первой и второй стороны, которые являются функциями времени;

$dn_1(t)$ и $dn_2(t)$ — математические ожидания числа компьютерных атак.

Величины $dn_1(t)$ и $dn_2(t)$ равны соответственно произведению величины ИР на число компьютерных атак за промежуток времени dt

$$\begin{cases} dn_1(t) = r_1(t)\lambda_1(t)dt \\ dn_2(t) = r_2(t)\lambda_2(t)dt \end{cases}, \quad (2)$$

где $\lambda_1(t)$ и $\lambda_2(t)$ — интенсивность компьютерных атак в момент времени t.

Для наглядности и простоты описания модели ИП введем такую характеристику, как мощности сторон, которые являются математическими ожиданиями числа поражаемых ИР каждой стороны

$$m_1(t) = \frac{p_1\lambda_1 r_1(t)}{r_2(0)}, \quad (3)$$

$$m_2(t) = \frac{p_2\lambda_2 r_2(t)}{r_1(0)}, \quad (4)$$

где $r_1(0)$ и $r_2(0)$ — начальные ИР противоборствующих сторон.

Тогда процесс изменения мощностей ИР сторон опишется системой дифференциальных уравнений, представляемой в виде

$$\begin{cases} \frac{d\,m_1(t)}{dt} = -m_1(0)m_2(t) \\ \frac{d\,m_2(t)}{dt} = -m_2(0)m_1(t), \end{cases} \quad (5)$$

где

$$m_1(0) = \frac{p_1 s_1 r_1(0)}{r_2(0)}, \quad (6)$$

$$m_2(0) = \frac{p_2 s_2 r_2(0)}{r_1(0)} \quad (7)$$

есть начальные мощности ИР сторон.

Выражения (6), (7) дополним коэффициентами использования характеристик КВИС — $\hat{e}_u$, уровнями «защиты информации» на основе применения средств защиты информации — $\hat{e}_n$ и уровнями функциональной устойчивости КВИС (на основе средств регулирования параметров и восстановления информационно-вычислительного процесса) — p_f

$$m_1(0) = \frac{\hat{e}_{1\grave{e}}\hat{e}_{1\ddot{i}}\,p_{1f}p_1 s_1 r_1(0)}{r_2(0)}, \quad (8)$$

$$m_2(0)=\frac{\hat{e}_{2\grave{e}}\hat{e}_{2\ddot{i}}\,p_{2f}p_2 s_2 r_2(0)}{r_1(0)}. \qquad (9)$$

После получения дифференциальных уравнений второго порядка и интегрирования каждого из этих уравнений найдены выражения для текущих мощностей ИР сторон

$$m_1(t)=\frac{m_1(0)+\sqrt{m_1(0)m_2(0)}}{2}exp\left(-\sqrt{m_1(0)m_2(0)}t\right)+ \\ +\frac{m_1(0)-\sqrt{m_1(0)m_2(0)}}{2}exp\left(\sqrt{m_1(0)m_2(0)}\,t\right), \qquad (10)$$

$$m_2(t)=\frac{m_2(0)+\sqrt{m_1(0)m_2(0)}}{2}\exp\left(-\sqrt{m_1(0)m_2(0)}t\right)+ \\ +\frac{m_2(0)-\sqrt{m_1(0)m_2(0)}}{2}\exp\left(\sqrt{m_1(0)m_2(0)}t\right). \qquad (11)$$

Динамика изменения ИР противоборствующих сторон для заданных исходных мощностей ИР будет выглядеть следующим образом (Рис. 1).

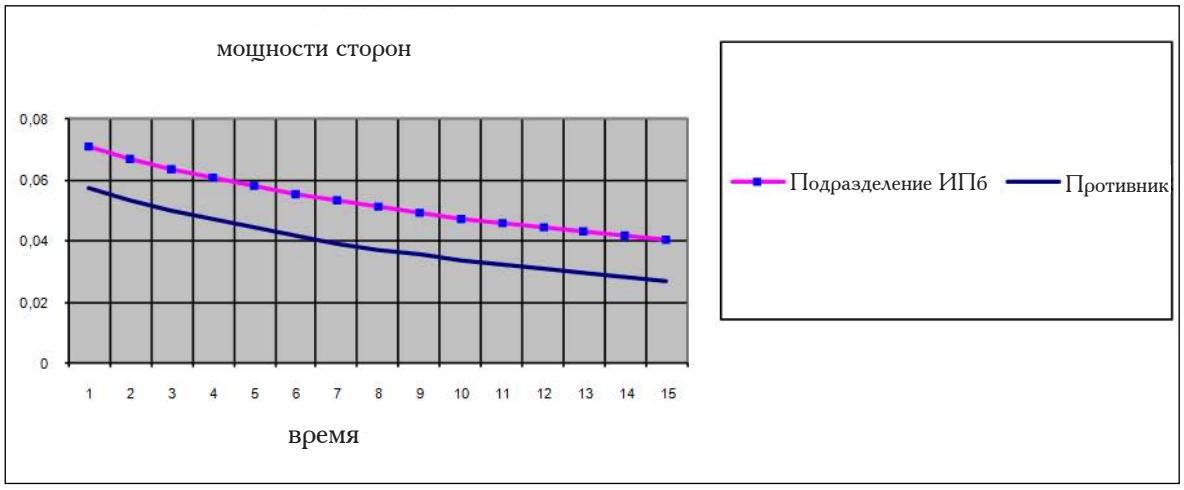


Рис. 1. Динамика изменения мощностей противоборствующих сторон

Для уточнения исходной дифференциальной модели процессов ИП в исходную модель введены элементы управления путем разбиения времени протекания процессов ИП на ряд последовательных временных участков с последовательной экстраполяцией состояния ИР по исходным данным уже не на начало технологического цикла, а на момент окончания очередного участка экстраполяции. Предложено описывать процессы ИП моделью, представляемой в виде конечных приращений (разностных уравнений первого порядка)

$$\begin{bmatrix} m1_{i+1} \\ m2_{i+1} \end{bmatrix}=\begin{bmatrix} m1_i \\ m2_i \end{bmatrix}+\begin{bmatrix} \Delta m1_i \\ \Delta m2_i \end{bmatrix}, \qquad (12)$$

где $m1_i$ и $m2_i$ — величины мощностей ИР сторон в i-й момент времени;

$\Delta m1_i$ и $\Delta m2_i$ — величины изменений мощностей ИР сторон между i-м и $i+1$-м моментами времени (на интервале $\Delta t_i = t_{i+1} - t_i$).

В окончательном виде выражение для мощности ИР сторон на i+1-й момент имеет вид

$$m1_{i+1} = \frac{m_1(t_i) + \sqrt{m_1(t_i)m_2(t_i)}}{2}\exp(-\sqrt{m_1(t_i)m_2(t_i)}\Delta t_i) + \\ + \frac{m_1(t_i) - \sqrt{m_1(t_i)m_2(t_i)}}{2}\exp(\sqrt{m_1(t_i)m_2(t_i)}\Delta t_i), \quad (13)$$

$$m2_{i+1} = \frac{m_2(t_i) + \sqrt{m_1(t_i)m_2(t_i)}}{2}\exp(-\sqrt{m_1(t_i)m_2(t_i)}\Delta t_i) + \\ \frac{m_2(t_i) - \sqrt{m_1(t_i)m_2(t_i)}}{2}\exp(\sqrt{m_1(t_i)m_2(t_i)}\Delta t_i). \quad (14)$$

Моделирование показывает, что при различных исходных мощностях сторон и различных интервалах экстраполяции модели ИП противоборствующих сторон методическая ошибка составляет в среднем примерно 10 %.

Разработанные аналитические модели открывают возможности для более эффективного учета факторов и условий ИП: объемов начальных ИР сторон; интенсивностей компьютерных атак, защищенности ИР и их функциональной устойчивости; наличия резервов ИР и, в том числе для оперативного управления результатами ИП с использованием фактора внезапности, введения резерва ИР и их восстановления.

Фактор внезапности позволяет сохранить свою начальную мощность ИР до начала действий нарушителя по применению компьютерных атак на КВИС. Он способен обеспечить превосходство в ИП при условии меньшей начальной мощности, нежели у нарушителя, если на некотором интервале внезапности удастся снизить начальную мощность ИР противоборствующих сторон до уровня

$$m_2(T) = m_2(0)\exp(-m_1(0)T) < m_1(0),$$

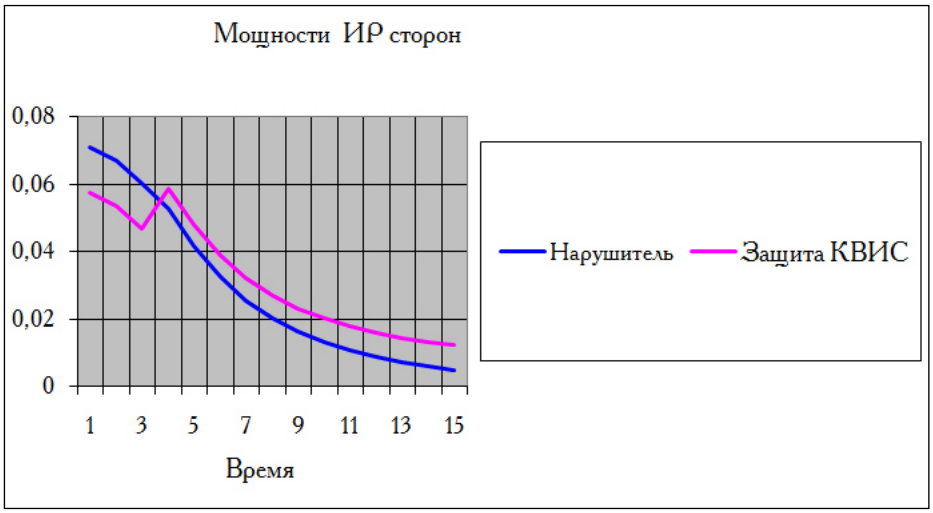
что следует из элементарной системы дифференциальных уравнений при $t < T$

$$\begin{cases} \frac{d\,m_1(t)}{dt} = 0, \\ \frac{d\,m_2(t)}{dt} = -m_2(t)\,m_1(0). \end{cases}$$

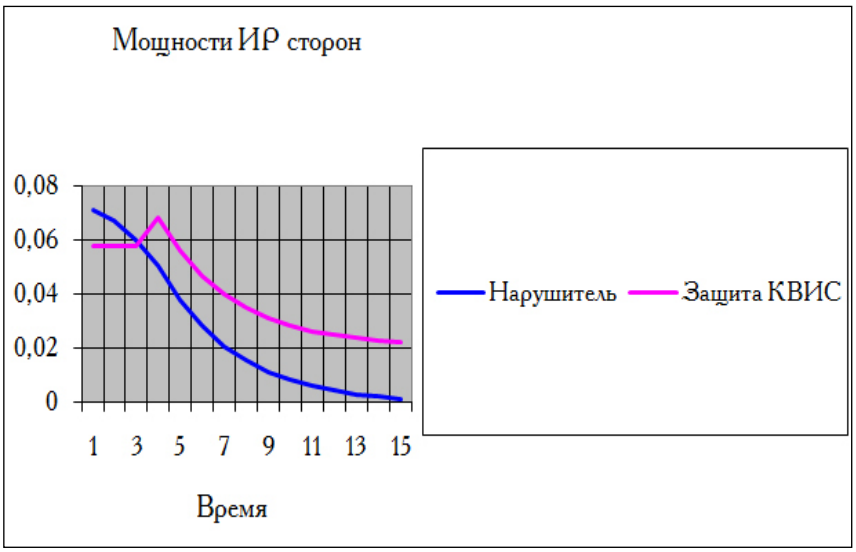
На графике (Рис. 2а и 2б) показано, как ввод резерва ИР и элемент внезапности меняют картину ИП. В модели в качестве критерия оценки результатов ИП принята вероятность W выполнения КВИС своей функциональной задачи, зависящая от разности относительных оставшихся частей ИР противоборствующих сторон на момент окончания цикла управления Т:

$$W = \{P(m1 \geq m1_{зад}, m2 < m2_{тр}), \text{ если } t < T\},$$

$$W = 0, \text{ если } t > T.$$



а)



б)

Рис. 2. Динамика ИП при целенаправленном управлении ИР: а) ввод резерва ИР; б) ввод фактора внезапности и резерва ИР

Разработанный метод позволяет формировать предложения по технологическому наращиванию ИР в соответствии с критерием «эффективность — стоимость — реализуемость».

Таким образом, разработан метод, который даёт возможность представить двусторонние процессы ИП в КВИС моделями динамики средних и разностными уравнениями первого порядка, что позволяет решать задачи анализа и синтеза функционально устойчивых КВИС с элементами ситуационного управления.