Соловьев Н.А., Цыганков А.С.
Оренбургский государственный университет

МЕТОДОЛОГИЯ АВТОМАТИЗАЦИИ ПРИНЯТИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ СРЕДСТВАМИ ЗАЩИТЫ АСУ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

В статье рассмотрены проблемы обеспечения защищенности корпоративных автоматизированных систем управления, сформулированы научные задачи, решение которых позволит реализовать систему поддержки принятия решений, позволяющую повысить оперативность принятия решений по управления средствами защиты информационных ресурсов распределенной компьютерной системы. Проанализированы методы решения поставленной задачи в условиях риска, неопределенности и активного противодействия. Предложен алгоритм ее решения.

Последние десятилетия характеризуются тенденцией слияния АСУП и АСУ ТП в единые интегрированные системы управления производством, технической основой которой становится корпоративная автоматизированная система управления (КАСУ). Опыт интегрированных производств свидетельствует о повышении роли организационного обеспечения, регламентирующего конфиденциальность, сохранность и доступность информационных ресурсов КАСУ. Основой организационного обеспечения становится система защиты информационных ресурсов (СЗИР). В последнее десятилетие уровень потерь корпораций от деструктивных воздействий на информационные ресурсы КАСУ соизмерим со стоимостью собственно автоматизированной системы. Это факт определяется, с одной стороны, скачкообразным ростом информационных объектов КАСУ, а с другой – аналогичным ростом числа информационных атак и способов несанкционированного доступа к этим объектам.

Проблемам обеспечения защищенности распределенных компьютерных систем, к классу которых относятся КАСУ, посвящены ряд работ [1, 2.3], в которых сформулировано противоречие между существенно возросшей значимостью защиты информационных ресурсов КАСУ и неадекватным уровнем автоматизации принятия решений по управлению средствами защиты.

Для преодоления противоречия между состоянием теории и требованиями практики необходимо решить ряд **задач научного характера**, одной из которых является задача определение временного интервала на принятия решений о выборе варианта защиты в условиях информационного противоборства.

Выбор решения в сложных ситуациях информационного противоборства производится в условиях риска и неопределенности. Еще более сложно дело обстоит в задачах управления активной информационной борьбой. Эти особенности принятия решений по управлению СЗИР в полной мере соответствуют формализации защищенности как функции выигрыша на основе построения формальных моделей байесовского риска в теории статистических решений.

Пусть M – множество возможных решений, а j ∈ M – его элементы. Решение j формируется с использованием имеющейся информации x о противнике, являясь результатом ее обработки. При этом информация x в идеальном конфликте представляет собой номер i варианта нападения, который выбрал противник из имеющегося множества альтернатив N и который был однозначно идентифицирован средствами контроля СЗИР. Если заданы функции распределения случайных $F_{\hat{t}}(t_i)$, $i=\overline{1,m}$ моментов времени t_i реализации m вариантов защиты и функции распределения $F_{\hat{\tau}}(t_j)$ $j=\overline{1,n}$ случайных моментов времени τ реализации n вариантов нападения, тогда, в условиях информационного конфликта i-го и j-го вариантов действий противоборствующих сторон на интервале [0, T], выигрыш защиты () заключается в реализации своего варианта действий раньше, чем будет реализован соответствующий вариант нападения

$$Zij(T)=\int_0^T F_{\hat{t}i}(\tau_j)\,dF_{\hat{\tau}_j}(\tau_j), \qquad (1)$$

где Zij(T) – показатель защищенности информационных ресурсов.

Пусть также задано распределение вероятностей $Q_j=\{q_1,\ldots,q_n\}$ обнаружения действий СИН средствами СЗИО и условные распределения $P_{i/j}(i/j)=\{p_{1/j},\ldots,p_{i/j},\ldots,p_{m/j}\}$ вероятности выбора варианта защиты при условии обнаружения таких действий.

Тогда усреднение вероятности (1) своевременной реализации варианта защиты по всем возможным альтернативам представляет собой обобщенный показатель эффективности применения заложенных в СЗИР вариантов защиты

$$Mz(T,p_{i|j})=\sum_{j=1}^{n}\sum_{i=1}^{m}\left[\int_0^T F_{\hat{t}_i}(\tau_j)\,dF_{\hat{\tau}_j}(\tau_j)\right]p_{i|j}q_j \qquad (2)$$

При этом на данный показатель влияет информационная связь между случайным номером варианта действий стороны защиты и случайным номером варианта действий стороны нападения. Эта связь по существу является количеством информации по Шеннону, которой обладает СЗИО в отношении действий системы информационного нападения (СИН) вида

$$I_{СИН} = \sum_{j=1}^{n}\sum_{i=1}^{m} p_{i|j} q_j \ln\left[\frac{p_{i|j}}{\sum_{j=1}^{n} p_{i|j} q_j}\right] \qquad (3)$$

Отсюда следует постановка вариационной задачи максимизации показателя защищенности $Mz_l(T, p_{i/j})$ при ограничениях на информационное обеспечение принятия решений в СЗИО, где варьируемыми являются вероятности условного распределения $p_{i/j}(i/j)$

$$\left.\begin{array}{l} Mz(T, p_{i|j}) \to \max\limits_{p_{i|j}} \\ I_{СИН}(p_{i|j}) = const \end{array}\right\} \qquad (4)$$

В [3] предложен алгоритм на основе неопределенных множителей Лагранжа, позволяющий найти аналитическое решение вариационной задачи (4).

Однако, предложенный методических аппарат оценки защищенности адекватен реальным процессам информационного противоборства только при условии стационарности воздействий СИН. Для построения модели оценки требуемой оперативности принятия решений, описывающей динамику изменения условий информационного противоборства и соответствующие реакции участвующих в нем сторон, целесообразно воспользоваться математическим аппаратом многошаговых динамический игр.

Возникает достаточно прозрачная противоречивая ситуация. В интервалы времени между принятием решений в СЗИР происходит накопление информации о действиях противника, которая позволяет снять неопределенность в отношении выбранного варианта нападения. Очевидно, что количество полученной информации является функцией времени, поскольку средства обнаружения деструктивных воздействий также функционируют во времени. Представляется справедливым утверждение, что с течением времени количество информации о противнике, которой располагает СЗИР, возрастает, приближаясь к некоторому уровню насыщения. При этом, чем больше информации о противнике будет получено, тем точнее будет принято решение о выборе адекватного варианта защиты и, следовательно, тем больше будет выигрыш СЗИР. Однако, с другой стороны, увеличение интервала ожидания новой информации о противнике для СЗИР не выгоден, поскольку, в этот период продолжает действовать СИН, тем самым, снижая суммарный выигрыш СЗИО в информационной борьбе.

Формально задача оценки оперативности принятия решений по управлению защитой информационных ресурсов КАСУ поставлена следующим образом

$$t_{zopt} = \underset{t_z \in T}{\mathrm{Arg\,max}}\, Mz(t),$$

где $Mz(t) = f(Iсин(t), Iсзи(t))$ – функция суммарного выигрыша (защищенности) СЗИР между очередными воздействиями противников.

Предложен алгоритм решения этой задачи.

1. Используя характеристики средств получения информации, сформировать базовые узлы и выполнить экстраполяцию функции накопления количества информации о действиях СИН на l-ом цикле развития игровой ситуации – $I_{lсин}(t)$.

2. Сформировать зависимость выигрыша СЗИ на основе полученного количества информации – $Mz_l(T, P_{i/j})$.

3. На основе характеристик ущерба от воздействий противника сформировать прогноз ущерба в виде функции выигрыша СЗИО с момента реализации своего решения противником на l–1-ом цикле развития игровой ситуации – $Mz_{l-1}(T, Q_{i/j})$.

4. Найти оптимальный временной интервал принятия решений t_{zopt}, являющийся корнем дифференциального уравнения вида

$$\frac{dMz_l(T, P_{i/j}) + Mz_{l-1}(T, Q_{i/j})}{dt} = 0 \qquad (5)$$

Результат реализация предложенного алгоритма в процессе имитационного моделирования двух прототипов КАСУ представлена на рисунке 1.

Анализ результатов моделирования свидетельствует, что администратору безопасности для принятия решений на изменение правил защиты, например, от подбора пароля авторизованного доступа с помощью программного генератора паролей, будет выделено времени от 50 до 60 с.

Следовательно, администратор безопасности работает в условиях острого дефицита времени по управлению механизмами защиты и без средств автоматизации принятия решений с задачей защиты информационных ресурсов КАСУ не справится.

Для обеспечения требуемой оперативности работы администратора безопасности, особенно в критических ситуациях, необходимо пересмот-

реть технологию управления средствами разграничения доступа. Новая технология должна предусматривать автоматическое принятие решений на уровне МЭ в случае обнаружения вторжения и аномальной активности объектов сегмента АСУ. На рисунке 2 предложена такая технология управления средствами разграничения доступа, в качестве которого используется МЭ.

Контур адаптивного управления реализации новой технологии управления защитой информационных ресурсов КАСУ на основе МЭ *FareWall*-1 [2] представлен на рисунке 3.

Предложенный контур управления МЭ является развитием архитектуры межсетевого экрана с поддержкой функции управления при обнаружении вторжения и аномальной активности [2].

Базовым процессом в контуре управления принятием решений является моделирование трафика информационного обмена. В интересах настоящего исследования модель трафика представлена временным рядом суммы трех компонентов: Y(t) – составляющая, описывающая нормальное среднесуточное изменения трафика; G(t) – составляющая, учитывающая изменение трафика сети за счет проявления сетевых угроз безопасности; ε(t) – случайная последовательность, учитывающая ошибки процесса моделирования.

С учетом сказанного модель сетевого трафика представляется в виде:

$$F(t) = Y(t) + G(t) + \varepsilon(t). \qquad (6)$$

Отсюда, определение составляющей G(t) является целевой функцией контура управления принятием решений на изменение базы правил МЭ, которая характеризует превышение уровня сетевого трафика в случае проявления сетевых угроз и аномальной активности объектов сети.

В [3] предложена методика регистрации сетевого трафика с помощью счетчика накопительного типа и его преобразование в классическую случайную последовательность, для которой применимо статистическое оценивание.

В связи с изменением уровня сетевого трафика во времени введен индекс изменения I_t математического ожидания M_t

$$I_t = \frac{M_t - M_{t-1}}{M_t} \qquad (7)$$

Для описания динамики изменения индекса математического ожидания во времени и определения критичности события для анализа сегмента сети введена функцию вида

$$f(t) = \sum_{i=1}^{n} c_i \sigma(t, a_i), \qquad (8)$$

где $c_i = M_{t_{i+1}} - M_{t_i} = I_{t_{i+1}} M_{t_{i+1}}$ $\sigma(t,a) = \begin{cases} 0, t < a \\ 1, t \geq a \end{cases}$

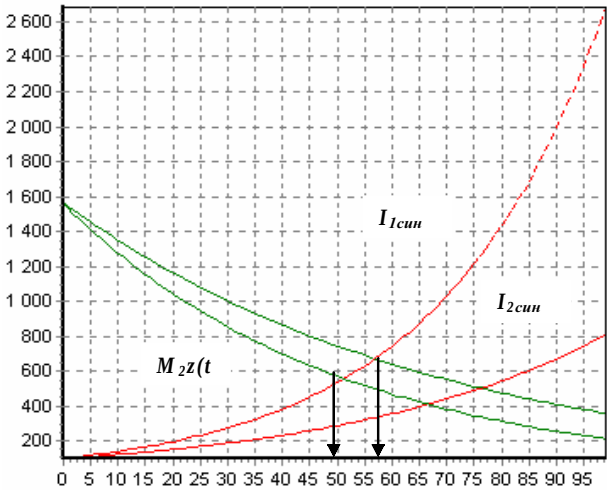

Рисунок 1. Оперативность принятия решений при атаке типа подбор пароля авторизованного доступа с помощью программного генератора паролей

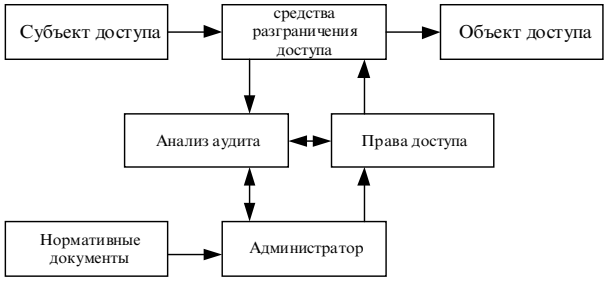

Рисунок 2. Технология управление МЭ с автоматическим принятием решения на изменение прав доступа к информационным ресурсам КАСУ

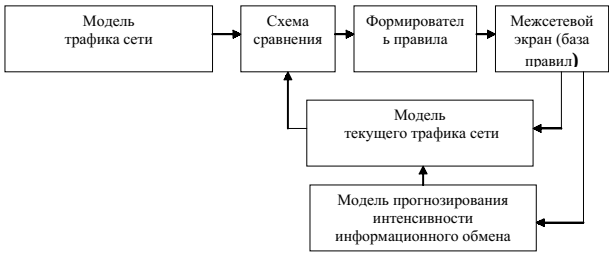

Рисунок 3. Контур адаптивного управления МЭ

Таблица 1. Порядок действий системы защиты КАСУ

Код уровня	Уровень опасности сети	Действия
1	Отсутствие или низкий	Информировать текущее состояние
2	Средний	Информировать администратора
3	Высокий	Применять систему противодействия на межсетевом экране

Таблица 2. Типы зависимости и уровни опасности

Тип зависимости	Интервалы для R_l
Низкая	$0 <= R_l < 0,7$
Высокая	$0,7 <= R_l <= 1$

Отсюда модель сетевого трафика контура управления принятием решений примет вид

$$F(t) = \sum_{i=1}^{n} I_i M_i \sigma(t, a_i) \qquad (9)$$

Проявлением информационной атаки является повышение уровня информационного обмена, который регистрируется в журнале событий МЭ. В [3] соответствующему уровню сетевого трафика присвоен соответствующий код опасности.

Для прогнозирования угроз безопасности сегментов КАСУ в закон управления принятием решений на изменение базы правил МЭ введены две составляющие. Первая – для прогнозирования текущего состояния сети (использован метод кусочно – полиномиальной экстраполяции сплайнами 2-го порядка.), вторая – для выявления скрытых закономерностей сетевой безопасности. Для выявления скрытых угроз безопасности применим спектральный анализ временного ряда.

Экстраполяция сплайном 2-го порядка определяется зависимостью

$$\tilde{y}_t = b_0 + b_1 t + b_2 t^2 + \varepsilon_t \qquad (10)$$

Коэффициенты полинома (10) определяются методом наименьших квадратов.

С целью определения уровня опасности введен индекс:

$$I_{(t+1)} = \frac{y_{(t+1)} - y_{(t)}}{y_{(t+1)}} \qquad (11)$$

где $y_{(t)}$ определяется по зависимости (10).

Для комплексной оценки опасности сегмента корпоративной сети предложены уровни опасности и действия сетевой системы защиты информационного обеспечения, представленной в таблице 1.

В [3] определены условия перехода на соответствующий уровень.

Следовательно, использование на этапе оперативного управления сплайна 2-го порядка позволяет предсказать угрозы безопасности корпоративной АСУ. Для решения задачи принятия решений по управлению защитой информационного обеспечения КАСУ введены индексы опасности [3], позволяющие корректировать контур управления МЭ.

При спектральном анализе сетевого трафика для выявления скрытых закономерностей логично предположить, что временной ряд является суммой или спектром многих волнообразных изменений, которые можно описать с помощью тригонометрических функций. Целью спектрального анализа является отыскание скрытых периодичностей и оценка их интенсивности. Для описания волнообразных колебаний динамического временного ряда использована периодическая функция Фурье

$$\bar{y}_t = a_0 + \sum (a_l \cos\frac{360t}{l} + b_l \sin\frac{360t}{l}),\ l = \frac{n}{k} \qquad (12)$$

где a_0 — средний уровень ряда;

l – длина волны;

k – номер гармоники;

t – порядковый номер временного периода;

n – длина ряда, т. е. число уровней в нем.

Для нахождения параметров (12) использованы зависимости вида:

$$a_0 = \frac{\sum y}{n};\ a_l = \frac{2}{n}\sum y \cos\frac{360t}{l};\ b_l = \frac{2}{n}\sum y \sin\frac{360t}{l}$$

Для определения наличие циклов и первоначальной длины периода несанкционированного доступа к информационным ресурсам КАСУ использована автокорреляционная функция вида

$$R_l = \frac{(n-l)\sum_{i=1}^{n-l} y(i)\cdot y(i+l) - \left[(\sum_{i=1}^{n-l} y(i))\cdot(\sum_{i=l}^{n} y(i))\right]}{\sqrt{(n-l)\cdot\sum_{i=1}^{n-l} y^2(i) - \sum_{i=1}^{n-l} y^2(i)}\cdot\sqrt{(n-l)\cdot\sum_{i=l}^{n} y^2(i) - \sum_{i=l}^{n} y^2(i)}}$$

При условии, что l изменяется от 1 до n/2.

В таблице 2 показана зависимость величины R и соответствующие ей уровни опасности. Для высокой степени зависимости R_l используется функция на основании рядов Фурье.

Следовательно, на этапе прогнозирования с целью выявления внутренних циклов и закономерностей целесообразно использовать спектральный анализ временного ряда, позволяющий находить периодические закономерности опасности корпоративной АСУ.

Таким образом, предложенная методология автоматизации существенно повысит оперативность принятия решений по управления средствами защиты информационных ресурсов корпоративных АСУ в условиях информационного противоборства.

Список использованной литературы:

1. Гаценко О.Ю. Защита информации. – СПб.: «Сентябрь», 2001.-225с.
2. Лебедь С.В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. М.: Изд-во МГТУ им. Н.Э. Баумана, 2002. – 301с.
3. Соловьев Н.А. и др. Отчет о НИР «Разработка специальных алгоритмов и программ защиты информационного и программного обеспечения корпоративных АСУ». – Оренбург: РИК ГОУ ОГУ, 2004 г. – 156 с.