УДК 681.322

ОПТИМИЗАЦИЯ РАБОТЫ СИСТЕМЫ ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ В УСЛОВИЯХ ОГРАНИЧЕНИЯ ВРЕМЕННОГО РЕСУРСА НА РЕШЕНИЕ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ

А.В. Душкин, Е.А. Рогозин, С.В. Скрыль

В статье рассматривается вариант оптимизации работы системы выявления несанкционированных воздействий в условиях ограничения временного ресурса на решение задач защиты информационной системы методом рационального комплексирования разнородных признаков этих воздействий

Ключевые слова: информационная система, несанкционированное воздействие, признак

Современная жизнь невозможна без информационных систем (ИС), представляющих собой взаимосвязанные между собой информационные и телекоммуникационные средства сбора, обработки и передачи информации, предназначенные для обеспечения определенных технологических циклов по формированию баз данных и управлению различными технологическими процессами (например, автоматизированные системы управления воздушным движением, транспортными потоками и т.д.). При этом нарушение последовательности операций технологических циклов, выход некоторых параметров за допустимые пределы на установленном интервале времени приводит к нарушению функционирования ИС, и, соответственно, нанесению им определенного ущерба.

Существующие меры защиты, как правило, используют большое количество средств обнаружения несанкционированных воздействий (НСВ) и реагирования на воздействия угроз. Но огромная часть информации о характеристиках воздействий и происходящих процессах зачастую дублируется или просто отсутствует, что не дает возможности определения этапа и характера воздействия и, как следствие, степени его опасности, а это, в свою очередь, приводит к неадекватному реагированию системы защиты информации (СЗИ). Кроме того, современные средства защиты, как правило, разрабатываются для сетей общего пользования и не учитывают особенностей работы ИС, выполняющих определенные технологические циклы и не приемлющих в ряде случаев стандартных универсальных решений СЗИ.

Вышесказанное определило необходимость решения задачи рациональной фильтрации разнородных признаков НСВ в рамках оптимизации процесса выявления НСВ с учетом необходимости безусловного выполнения ИС основных задач по целевому назначению. В ходе ее решения дано обоснование метода рационального комплексирования разнородных признаков несанкционированных воздействий на информационные системы**,** отличающегося от известных введением в пространство основных признаков НСВ дополнительных значимых признаков, специфичных для определенных ИС, и дополнительных математических соотношений с целью оптимизации работы системы выявления НСВ в условиях ограничения временного ресурса и достижения требуемой своевременности реагирования на воздействия.

Формирование информационного пространства признаков НСВ на ИС реализуется путем покрытия информационного пространства данных основных средств регистрации признаков воздействий информационным пространством дополнительных данных. Это связано с недостатком в пространстве основных данных мониторинга некоторых элементов, специфичных для отдельных типов воздействий, отсутствие которых может привести к низкой эффективности процесса выявления (неправильному определению вида НСВ, оценке степени его опасности и т.д.). С методической точки зрения данную процедуру можно рассматривать как процедуру дополнения одного информационного пространства другим [1], что позволяет сформулировать утверждение о ее формальном представлении.

Утверждение 1. *Процесс формирования информационного пространства данных основных средств регистрации признаков НСВ информационным пространством дополнительных данных с точки зрения формальной логики можно рассматривать как процедуру дополнения одного множества информационных элементов другим.*

Для формального представления положений утверждения введем следующие обозначе-

Душкин Александр Викторович – ВГТУ, канд. техн. наук, доцент, e-mail: a_dushkin@mail.ru

Рогозин Евгений Алексеевич – ВГТУ, д-р техн. наук, доцент, e-mail: a_dushkin@mail.ru

Скрыль Сергей Васильевич – МГТУ им. Н.Э. Баумана, д-р техн. наук, профессор, тел. (495) 632-22-47, e-mail: zi@bmstu.ru

ния: I^o – общее информационное пространство данных признаков НСВ; $I^м$ – информационное пространство данных основных средств регистрации признаков НСВ; $I^{доп}$ – информационное пространство дополнительных данных.

С учетом введенных обозначений формальное представление утверждения имеет следующий вид: *при* $I^o = I^м \bigcup I^{доп}$ *справедливо* $I^м = \bar{I}^{доп}$.

Доказательство. Рассмотрим детально механизм информационного покрытия. Для однозначного определения корреляции основных и дополнительных данных мониторинга информационного пространства осуществим разбиение пространств $I^м$ и $I^{доп}$ на M и N непересекающихся подпространств (фрагментов) соответственно. При этом в пространстве $I^м$ формируется M фрагментов базовых информативных признаков, а в пространстве $I^{доп}$ – N фрагментов значимых информативных признаков, обеспечивающих соответствующие базовые признаки. Тогда можно записать следующее соотношение:

$$I^м = \left(i_1^м, i_2^м, \ldots, i_M^м\right), \qquad (1)$$

где $i_m^м$ – m-й ($m = 1, 2, \ldots, M$) базовый информационный признак информационного пространства данных основных средств регистрации признаков НСВ;

$$I^{доп} = \left(i_1^{доп}, i_2^{доп}, \ldots, i_N^{доп}\right), \qquad (2)$$

где $i_n^{доп}$ – n-й ($n = 1, 2, \ldots, N$) значимый информационный признак информационного пространства данных дополнительных средств регистрации признаков НСВ.

Общее информационное пространство данных признаков НСВ на ИС СН формируется на основе информационного пространства данных основных средств регистрации признаков НСВ $I^м$ и информационного пространства дополнительных данных $I^{доп}$, то есть имеет место соотношение

$$I^o = \left(i_1^м \bigcup i_{11}^{доп} \bigcup i_{12}^{доп} \cdots \bigcup i_{1K_1}^{доп}, \ldots, i_M^м \bigcup i_{11}^{доп} \bigcup i_{12}^{доп} \cdots \bigcup i_{MK_M}^{доп}\right), \qquad (3)$$

где K_m – число значимых признаков пространства $I^{доп}$, дополняющих отсутствующую часть смыслового содержания базового признака $i_m^м$ пространства $I^{доп}$.

Характеристику $\sum_{m=1}^{M} K_m = N$ процесса покрытия одного информационного пространства другим будем называть степенью или глубиной покрытия. При этом, (3) примет вид

$$I^o = \left(i_1^м \bigcup \bar{i}_1^м, \ldots, i_M^м \bigcup \bar{i}_M^м\right), \qquad (4)$$

где $\bar{i}^м = \left(i_1^м \bigcup i_2^м \cdots \bigcup i_{K_M}^м\right)$.

Тогда для $I^{доп} = \left(i_1^{доп}, i_2^{доп}, \ldots, i_N^{доп}\right)$ и $\bar{I}^м = \left(\bar{i}_1^м, \bar{i}_2^м, \ldots, \bar{i}_M^м\right)$ справедливо

$$I^{доп} = \bar{I}^м. \qquad (5)$$

Утверждение доказано.

Процедура информационного покрытия при управлении процессом выявления признаков НСВ на ИС позволяет рассматривать обеспечение информативных признаков информационного пространства данных основных средств регистрации признаков НСВ информационным пространством дополнительных данных как процесс резервирования общего информационного пространства данных признаков воздействий. Наиболее полной характеристикой процесса покрытия информационного пространства данных основных средств регистрации признаков атак информационным пространством дополнительных данных является вероятность обеспечения дополнительным содержанием базовых информативных признаков.

Следующий момент, который необходимо рассмотреть, это зависимость времени выявления НСВ на ИС от глубины покрытия. Корреляция в данном контексте отличается от общепринятого понимания [2] и носит смысловой характер. Она заключается в определении в дополнительных данных только значимых информативных признаков, которые соответствуют базовым признакам данных основных средств регистрации признаков НСВ. Таким образом, можно оптимизировать время выявления по критерию минимальное время/необходимое качество. Для достижения этой цели сформулируем следующее утверждение.

Утверждение 2. *При покрытии информационного пространства данных основных средств регистрации признаков НСВ* $I^м$ *информационным пространством дополнительных данных* $I^{доп}$ *существует локальный интервал малого изменения функции времени реализации процесса выявления НСВ* $\tau^o(N)$ *от глубины покрытия* N.

Введем следующие обозначения: $\tau^o(N)$ – время реализации процесса выявления НСВ как функция глубины покрытия информационного пространства данных основных средств регистрации признаков НСВ дополнительными данными; $P^{уи}$ – вероятность устранения информационной избыточности дополнительных данных, характеризующая степень корреляции

данных мониторинга основных средств регистрации признаков НСВ и дополнительных данных за счет информационного покрытия.

Формальное представление утверждения имеет вид: *при* $I^o = I^м \bigcup I^{доп}$ $\exists$ *локальный интервал малого изменения* $\tau^o(N)$.

Доказательство. Формирование общего информационного пространства данных признаков НСВ (состояние S^o) осуществляется путем дополнения пространства базовых признаков данных основных средств регистрации признаков НСВ (состояние $S^м$) значимыми информационными признаками дополнительных данных (состояние $S^{доп}$) с соответствующими вероятностными характеристиками по устранению информационной избыточности $P^{уи}$ и обеспечению дополнительным содержанием информационного пространства данных основных средств регистрации признаков НСВ $P^{об}$.

Пусть $\tau^м$ – временная характеристика состояния $S^м$, а $\tau^{доп}$ – временная характеристика состояния $S^{доп}$. Тогда, учитывая характеристики $P^{об}$ и $P^{уи}$, а также соотношение состояний $S^{доп}$ и $S^м$, временную характеристику состояния S^o, правомерно

$$\tau^o = \tau^м + \left(1 - P^{об} \cdot P^{уи}\right) \cdot \tau^{доп}. \qquad (6)$$

Уровень резерва общего информационного пространства данных признаков НСВ на ИС I^o запишем в виде

$$R^ф = \frac{d^{доп}}{d^м} = \frac{\tau^{доп}}{\tau^м}. \qquad (7)$$

Тогда выражение (6) представляется как

$$\tau^o = \tau^м \cdot \left(1 + \left(1 - P^{об} \cdot P^{уи}\right) \cdot R^ф\right). \qquad (8)$$

Вероятность $P^{уи}$, характеризующую степень корреляции данных основных средств регистрации признаков НСВ и дополнительных данных за счет информационного покрытия, можно представить в виде

$$P^{уи} = 1 - \prod_{n=1}^{N} \left(1 - P_m^{уи}\right), \qquad (9)$$

где $P_m^{уи} = \dfrac{\theta_{K_m}^{доп.\,зн}}{\theta_{K_m}^{доп.\,зн} + \theta_{K_m}^{доп.\,нзн}}$ – вероятность устранения информационной избыточности дополнительных данных одного базового информативного признака данных основных средств регистрации признаков НСВ; $\theta_{K_m}^{доп.\,зн}$, $\theta_{K_m}^{доп.\,нзн}$ – объемы полных подпространств $i_{mk}^{доп.\,зн}$, $i_{mk}^{доп.\,нзн}$, вычисляемых как [3]:

$$\theta = \sigma \cdot \log_2 \Sigma, \qquad (10)$$

где σ – количество уникальных (неповторяющихся) сигнатур подпространств $i_{mk}^{доп.\,зн}$, $i_{mk}^{доп.\,нзн}$; Σ – общее число сигнатур подпространств $i_{mk}^{доп.\,зн}$, $i_{mk}^{доп.\,нзн}$.

Тогда при равномерном разбиении пространства $I^{доп}$ на фрагменты имеем

$$P^{уи} = 1 - \left(1 - P_m^{уи}\right)^N. \qquad (11)$$

Учитывая изложенное, а также положение о поведении вероятности обеспечения дополнительным содержанием базовых информативных признаков пространства данных основных средств регистрации признаков НСВ $P^{об}$, выражение (8) можно представить в виде зависимости времени τ^o от глубины покрытия N:

$$\begin{aligned}\tau^o(N) &= \tau^м \cdot \left(1 + \left(1 - \left(1 - \left(1 - P_m^{об}\right)^M\right) \cdot \left(1 - \left(1 - P_m^{уи}\right)^N\right)\right) \cdot R^ф\right) = \\ &= \tau^м \cdot \left(1 + \left(1 - \left(1 - \left(1 - \frac{\theta_{K_m}^{доп}}{\theta_{K_m}^{м} + \theta_{K_m}^{доп}}\right)^M\right) \cdot \left(1 - \left(1 - \frac{\theta_{K_m}^{доп.\,зн}}{\theta_{K_m}^{доп.\,зн} + \theta_{K_m}^{доп.\,нзн}}\right)^N\right)\right) \cdot \frac{N \cdot \theta^{доп}}{M \cdot \theta^м}\right).\end{aligned} \qquad (12)$$

После дифференцирования и проведения необходимых преобразований получается трансцендентное уравнение, решаемое известными численными методами [4]. При этом, исходя из условий

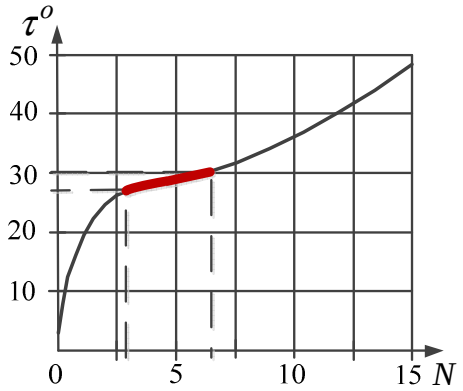
$$0 < P^{об} < 1 \quad \text{и} \quad 0 < P^{уи} < 1, \qquad (13)$$

корень уравнения не может быть равным нулю или отрицательным.

Из этого следует, что локальный интервал малого изменения зависимости времени реализации процесса выявления НСВ как функции глубины покрытия информационного пространства данных основных средств регистрации признаков НСВ дополнительными данными существует (рис. 1), что свидетельствует о возможности оптимизации процесса выявления

за счет учета только действительно значимых дополнительных данных.

В соответствии с принципами оптимизации управления процессом выявления НСВ на ИС возникает необходимость оптимального распределения резерва дополнительных средств мониторинга информационного пространства. Целевую функцию в данной задаче определяют потребности в резервировании, а функцию ограничения – возможности по его внесению. В [5] показано, что увеличению значения резерва дополнительных данных любого из M базовых информационных признаков данных основных средств регистрации признаков НСВ соответствует снижение значения своевременности реагирования на воздействия, свидетельствующее об ограниченности возможностей резервирования дополнительных данных.



Зависимость времени реализации процесса выявления НСВ τ^o от глубины покрытия N

Таким образом, в работе показан вариант оптимизации работы системы выявления несанкционированных воздействий в условиях ограничения временного ресурса на решение задач защиты информационной системы методом рационального комплексирования разнородных признаков этих воздействий. Он основан на том положении, что при покрытии информационного пространства данных основных средств регистрации признаков НСВ информационным пространством дополнительных данных существует локальный экстремум или интервал малого изменения функции времени реализации процесса выявления признаков НСВ от глубины покрытия. Это свидетельствует о возможности оптимизации процесса выявления за счет учета только действительно значимых дополнительных признаков НСВ. Использование данного метода позволяет оптимизировать работу системы выявления НСВ в условиях ограничения временного ресурса на решение задач защиты и дает возможность достижения требуемой своевременности реагирования на воздействия с учетом необходимости безусловного выполнения ИС основных задач по целевому назначению.

Литература

1. Заряев А.В. О возможности формального представления процедуры интегрирования разнородных информационных процессов в интересах подготовки специалистов в области информационной безопасности // Информация и безопасность. 2002. №1. С. 48-49.

2. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения. М.: Наука, 1988. 480 с.

3. Холстед М.Х. Начала науки о программах / Пер. с англ. М.: Финансы и статистика, 1981. 128 с.

4. Бахвалов И.В., Жидков Н.П., Кобельков Г.М. Численные методы. М.: Лаборатория базовых знаний, 2000. 624 с.

5. Душкин А.В. Методическое обеспечение системы выявления несанкционированных воздействий на информационные телекоммуникационные системы специального назначения в условиях ограничения временного ресурса. Монография. Воронеж: ВАИУ, 2010. 192 с.

Воронежский государственный технический университет

Московский государственный технический университет им. Н.Э. Баумана

OPTIMIZATION WORK SYSTEM REVEALING OF THE UNAPPROVED INFLUENCES IN THE CONDITIONS RESTRICTION OF THE TIME RESOURCE ON THE DECISION PROBLEMS PROTECTION OF INFORMATION SYSTEM

A.V. Dushkin, E.A. Rogozin, S.V. Skryl

In article the variant of optimisation work system revealing of the unapproved influences in the conditions restriction of the time resource on the decision problems protection of information system by a method rational complexes diverse signs of these influences is considered

Key words: information system, unapproved influence, a sign