А. В. Душкин

ОБОСНОВАНИЕ МЕТОДА РАЦИОНАЛЬНОГО КОМПЛЕКСИРОВАНИЯ РАЗНОРОДНЫХ ПРИЗНАКОВ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Введение

Современная жизнь невозможна без электронных средств информатизации общества, частью которых являются информационные системы (ИС). Они представляют собой взаимосвязанные 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 приводят к нарушению функционирования ИС и, соответственно, к 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 обычно 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.

Все 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.

1. Формализация представления процедуры комплексирования разнородных признаков НСВ на ИС

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 обозначения: 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 $I^{o} = I^{м} \cup I^{доп}$ *справедливо* $I^{м} = \overline{I}^{доп}$.

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:

$$I^{м} = (i_1^{м}, i_2^{м}, ..., i_M^{м}), \quad (1)$$

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

$$I^{доп} = (i_1^{доп}, i_2^{доп}, ..., i_N^{доп}), \quad (2)$$

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 $I^{доп}$, т. е. имеет место соотношение

$$I^{o} = (i_1^{м} \cup i_{11}^{доп} \cup i_{12}^{доп} ... \cup i_{1K_1}^{доп}, ..., i_M^{м} \cup i_{11}^{доп} \cup i_{12}^{доп} ... \cup i_{MK_M}^{доп}), \quad (3)$$

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

$$I^{o} = (i_1^{м} \cup \overline{i}_1^{м}, ..., i_M^{м} \cup \overline{i}_M^{м}), \quad (4)$$

где $\overline{i}^{м} = (i_1^{м} \cup i_2^{м} ... \cup i_{K_M}^{м})$.

Тогда для $I^{доп} = (i_1^{доп}, i_2^{доп}, ..., i_N^{доп})$ и $\overline{I}^{м} = (\overline{i}_1^{м}, \overline{i}_2^{м}, ..., \overline{i}_M^{м})$ справедливо

$$I^{доп} = \overline{I}^{м}. \quad (5)$$

Утверждение доказано.

2. Оценка количественных характеристик процедуры комплексирования разнородных признаков НСВ на ИС

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. Необходимо заметить, что 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 $\tau^{о}(N)$ от глубины покрытия N.*

Введем следующие обозначения: $\tau^{о}(N)$ — время реализации процесса выявления НСВ как функция глубины покрытия информационного пространства данных основных средств регистрации признаков НСВ дополнительными данными; $\rho^{уи}$ — 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 $I^{о}=I^{м}\cup I^{доп}$ $\exists$ *локальный интервал малого изменения* $\tau^{о}(N)$.

Доказательство. На рисунке 1 изображена формализованная схема рассматриваемого процесса.

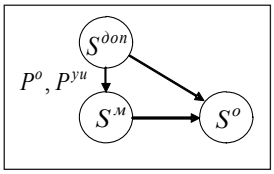

Рис. 1. Формализованная схема процесса выявления НСВ на ИС

Формирование общего информационного пространства данных признаков НСВ (состояние $S^{о}$) 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 $\rho^{уи}$ и обеспечению дополнительным содержанием информационного пространства данных основных средств регистрации признаков НСВ $\rho^{об}$.

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

$$\tau^{о} = \tau^{м} + (1- \rho^{об} \cdot \rho^{уи})\cdot \tau^{доп}. \quad (6)$$

Уровень резерва общего информационного пространства данных признаков НСВ на ИС $I^{о}$ запишем в виде

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

Тогда выражение (6) можно представить как

$$\tau^{о} = \tau^{м}\cdot 1+(1- \rho^{об} \cdot \rho^{уи})\cdot R^{ф}). \quad (8)$$

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

$$\rho^{уи} = 1 - \prod_{n=1}^{N} (1 - \rho_{m}^{уи}), \tag{9}$$

где $\rho_{m}^{уи} = \frac{\theta^{доп.зн}{}_{K_m}}{\theta^{доп.зн}{}_{K_m} + \theta^{доп.нзн}{}_{K_m}}$ — вероятность устранения информационной избыточности дополнительных данных одного базового информативного признака данных основных средств регистрации признаков НСВ; $\theta^{доп.зн}{}_{K_m}$, $\theta^{доп.нзн}{}_{K_m}$ — объемы полных подпространств $i^{доп.зн}{}_{mk}$, $i^{доп.нзн}{}_{mk}$, вычисляемых как [3]:

$$\theta = \sigma \cdot \log_2 \Sigma, \tag{10}$$

где σ — количество уникальных (неповторяющихся) сигнатур подпространств $i^{доп.зн}{}_{mk}$, $i^{доп.нзн}{}_{mk}$; Σ — общее число сигнатур подпространств $i^{доп.зн}{}_{mk}$, $i^{доп.нзн}{}_{mk}$.

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

$$\rho^{уи} = 1 - (1 - \rho^{уи}{}_{m})^{N}. \tag{11}$$

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

$$\begin{aligned} \tau^{о}(N) &= \tau^{м} \cdot (1 + (1 - (1 - (1 - \rho^{об}{}_{m})^{M}) \cdot (1 - (1 - \rho^{уи}{}_{m})^{N})) \cdot R^{ф}) = \\ &= \tau^{м} \cdot \left(1 + \left(1 - \left(1 - \left(1 - \frac{\theta^{доп}{}_{K_m}}{\theta^{м}{}_{K_m} + \theta^{доп}{}_{K_m}}\right)^{M}\right) \cdot \left(1 - \left(1 - \frac{\theta^{доп.зн}{}_{K_m}}{\theta^{доп.зн}{}_{K_m} + \theta^{доп.нзн}{}_{K_m}}\right)^{N}\right)\right) \cdot \frac{N \cdot \theta^{доп}}{M \cdot \theta^{м}}\right). \end{aligned} \tag{12}$$

После дифференцирования и проведения необходимых преобразований получается трансцендентное уравнение, решаемое известными численными методами [4, 5]. При этом исходя из условий

$$0 < \rho^{об} < 1 \text{ и } 0 < \rho^{уи} < 1 \tag{13}$$

корень уравнения не может быть равным нулю или отрицательным.

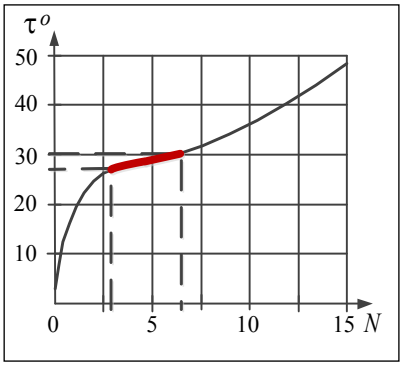

Рис. 2. Зависимость времени реализации процесса выявления НСВ $\tau^{о}$ от глубины покрытия N

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 (рисунок 2), что свидетельствует о возможности оптимизации процесса выявления за счет учета только действительно значимых дополнительных данных.

3. Оценка соотношения необходимого и возможного резерва признакового пространства НСВ на ИС

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. Сформулируем и докажем соответствующее утверждение.

Утверждение 3. *Необходимость использования в процессе распознавания наряду с данными основных средств регистрации признаков НСВ дополнительных данных зависит от частоты их использования.*

Доказательство. Введем следующие обозначения: $\bar{\tau}^{o}_{m}$ — среднее время реализации m-го процесса выявления ($m = 1, 2, \ldots, M$); $\tau^{доп}_{m}$ — время обработки дополнительных данных; a_m — число реализаций m-го процесса выявления на интервале $[t_н, t_к]$; $t_н$ — время начала наблюдения; $t_к$ — время окончания наблюдения.

Суммарное время реализации типового процесса выявления на рассматриваемом интервале $[t_н, t_к]$

$$\tau^{\Sigma o}_{k} = \sum_{[t_н, t_к]} \bar{\tau}^{o}_{m} = a_m \cdot \bar{\tau}^{o}_{m}. \qquad (14)$$

Тогда суммарное время обработки дополнительных данных

$$\tau^{\Sigma доп}_{k} = \sum_{[t_н, t_к]} \bar{\tau}^{доп}_{m} = a_m \cdot \bar{\tau}^{доп}_{m}. \qquad (15)$$

При условии, что $t_к - t_н >> \tau^{\Sigma o}_{k}$, предположим, что случайное распределение процессов выявления $\bar{\tau}^{o}_{m}$ на временном интервале $\tau^{\Sigma o}_{k}$ (рисунок 3) удовлетворяет следующим условиям [1, 2]:

- вероятность реализации процесса выявления зависит только от длины временного интервала $\tau^{\Sigma o}_{k}$ и не зависит от его положения на временной оси, из чего следует, что процессы выявления проводятся с одинаковой средней плотностью $\bar{\rho}^{\Sigma o}_{k}$;
- отдельные процессы выявления признаков НСВ распределяются на временной оси независимо друг от друга.

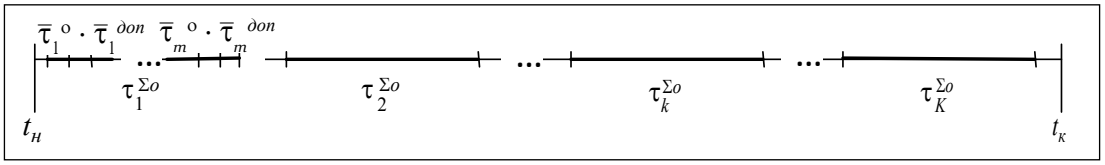

Рис. 3. Временные соотношения в типовом процессе выявления НСВ на ИС

Это позволяет вероятность того, что за время $\tau^{\Sigma o}_{k}$ m-й процесс выявления проявится в k временных интервалах $\tau^{\Sigma o}_{k}$, считать распределением по закону Пуассона:

$$\rho^{o}_{k} = \frac{\bar{\rho}^{\Sigma o}_{k} \cdot \tau^{\Sigma o}_{m}}{k!} \cdot e^{\bar{\rho}^{\Sigma o}_{k} \cdot \tau^{\Sigma o}_{m}}, \qquad (16)$$

а вероятность проявления хотя бы в одном $\tau^{\Sigma o}_{k}$ — по экспоненциальному закону:

$$\rho^{o}_{m} = 1 - e^{\bar{\rho}^{\Sigma o}_{k} \cdot \tau^{\Sigma o}_{m}}. \qquad (17)$$

Тогда для любой пары значений $\tau^{\Sigma o}_{i}$ и $\tau^{\Sigma o}_{j}$ справедливо условие:

если $\tau^{\Sigma o}_{i} > \tau^{\Sigma o}_{j}$, то $\rho^{o}_{i} > \rho^{o}_{j}$. (18)

Из этого следует, что для i-го процесса выявления должна быть обеспечена вероятность $\rho^{об}_{i}$ обеспечения дополнительными данными соответствующего базового информативного признака пространства $I^{м}$ не ниже ее уровня $\rho^{об}_{j}$, необходимого для обеспечения j-го процесса выявления, т. е.

для $\rho^{o}_{i} > \rho^{o}_{j}$ необходимо $\rho^{об}_{i} > \rho^{об}_{j}$. (19)

При этом вероятность $\rho^{об}_{m}$ обеспечения дополнительными данными базового информативного признака пространства $I^{м}$, соответствующего m -му процессу выявления, определяется согласно выражению

$$\rho^{об}_{m} = \frac{\theta^{доп}_{Km}}{\theta^{м}_{m} + \theta^{доп}_{Km}}, \quad (20)$$

в котором $\theta^{м}_{m}$ — объем информационного пространства базового признака $i^{м}_{m}$; $\theta^{доп}_{Km}$ — объем информационного пространства соответствующих значимых признаков $i^{м}_{m} = i^{доп}_{1} \cup i^{доп}_{2} \ldots \cup i^{доп}_{Km}$.

Учитывая вышеизложенное, а также условия (18), (19) и выражение (20), справедливо соотношение: для $\tau^{\Sigma o}_{i} > \tau^{\Sigma o}_{j}$ необходимо обеспечить $K_i > K_j$, что и требовалось доказать. Кроме того, увеличению значения резерва дополнительных данных любого из M базовых информативных признаков данных основных средств регистрации признаков НСВ соответствует снижение значения своевременности реагирования на воздействия, свидетельствующее об ограниченности возможностей резервирования дополнительных данных [6].

Заключение

Таким образом, в работе дано обоснование метода рационального комплексирования разнородных признаков несанкционированных воздействий на информационные системы. 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.

СПИСОК ЛИТЕРАТУРЫ:

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. *Гмурман В. Е.* Руководство к решению задач по теории вероятностей и математической статистике: Учебное пособие для студентов вузов. М.: Высшая школа, 2003. – 405 с.

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

6. *Душкин А. В.* О потребностях и возможностях функционального резервирования дополнительных средств мониторинга информационного пространства информационно-телекоммуникационной системы // Системы управления и информационные технологии. 2006. № 4.1 (26). С. 144–145.