УДК 681.3

МОДЕЛИРОВАНИЕ СИСТЕМЫ ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ В УСЛОВИЯХ ОГРАНИЧЕНИЯ ВРЕМЕННОГО РЕСУРСА

***Белокуров Сергей Владимирович**, д.т.н., доцент*
***Скрыль Сергей Васильевич**, д.т.н., профессор*
***Джоган Василий Климович**, д.т.н., доцент*
Воронежский институт ФСИН России
***Сидельников Алексей Павлович**, аспирант*
Воронежский государственный технический университет

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. Корреляция в данном контексте отличается от общеприня-

того понимания [1] 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.

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 $\tau^{o}(N)$.

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

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

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

$$R^{ф} = \frac{d^{доп}}{d^{м}} = \frac{\tau^{доп}}{\tau^{м}} . \quad (2)$$

Тогда выражение (1) представляется как

$$\tau^{о} = \tau^{м} \cdot \left(1 + \left(1 - P^{об} \cdot P^{уи}\right) \cdot R^{ф}\right). \quad (3)$$

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

$$P^{уи} = 1 - \prod_{n=1}^{N}\left(1 - P_m^{уи}\right), \quad (4)$$

$$P_m^{уи} = \frac{\theta_{K_m}^{доп.\,зн}}{\theta_{K_m}^{доп.\,зн} + \theta_{K_m}^{доп.\,нзн}}$$

где – 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 [2]:

$$\theta = \sigma \cdot \log_2 \Sigma, \quad (5)$$

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

$$P^{уи} = 1 - \left(1 - P_m^{уи}\right)^{N}. \quad (6)$$

Учитывая изложенное, а также положение о поведении вероятности обеспечения дополнительным содержанием базовых информативных признаков пространства данных основных средств регистрации признаков НСВ $P^{об}$, выражение (3) можно представить в виде зависимости времени $\tau^{о}$ от глубины покрытия N:

$$\tau^{о}(N) = \tau^{м} \cdot \left(1 + \left(1 - \left(1 - \left(1 - P_m^{об}\right)^{M}\right) \cdot \left(1 - \left(1 - P_m^{уи}\right)^{N}\right)\right) \cdot R^{ф}\right) =$$

$$= \tau^{м} \cdot \left(1 + \left(1 - \left(1 - \left(1 - \frac{\theta_{K_m}^{доп}}{\theta_{K_m}^{м} + \theta_{K_m}^{доп}}\right)^{M}\right) \cdot \left(1 - \left(1 - \frac{\theta_{K_m}^{доп.\,зн}}{\theta_{K_m}^{доп.\,зн} + \theta_{K_m}^{доп.\,нзн}}\right)^{N}\right)\right) \cdot \frac{N \cdot \theta^{доп}}{M \cdot \theta^{м}}\right). \quad (7)$$

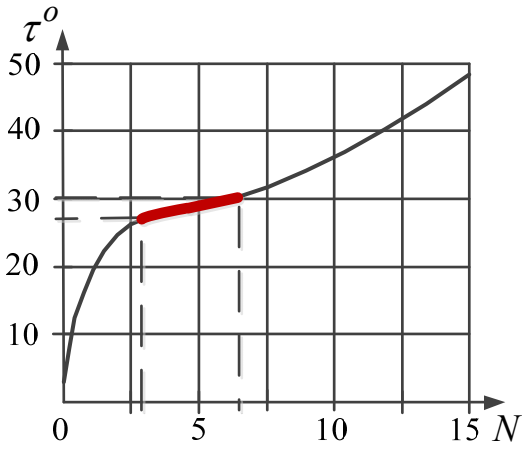

Рисунок 1. Зависимость времени реализации процесса выявления НСВ τ^o от глубины покрытия N

После дифференцирования и проведения необходимых преобразований получается трансцендентное уравнение, решаемое известными численными методами [2]. При этом, исходя из условий

$$0 < P^{об} < 1 \quad \text{и} \quad 0 < P^{уи} < 1, \tag{8}$$

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.

Таким образом, в работе показан вариант оптимизации работы системы выявления несанкционированных воздействий в условиях ограничения временного ресурса для решение задач защиты информационной системы методом рационального комплексирования разнородных признаков этих воздействий.

Список литературы

1. Основы информационной безопасности: Учебник для высших учебных заведений МВД России / Под ред. В.А. Минаева и С.В. Скрыля. - Воронеж: Воронежский институт МВД России, 2001. - 464 с.

2. Модели и алгоритмы автоматизированного контроля эффективности систем защиты информации в автоматизированных системах: монография / С.В. Белокуров, С.В. Скрыль, В.К. Джоган [и др.]. – Воронеж: Воронежский институт МВД России, 2012. – 116 с.