УДК 681.32

ОБОСНОВАНИЕ МЕТОДА ДОПОЛНЕНИЯ СОСТАВА ПОДСИСТЕМЫ ВЫЯВЛЕНИЯ НЕСАНКЦИОНИРОВАННЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ В УСЛОВИЯХ ОГРАНИЧЕНИЯ ВРЕМЕННОГО РЕСУРСА

С.В. Скрыль, А.В. Душкин, В.В. Киселев

В работе рассматриваются вопросы оптимизации процессов обнаружения признаков и выявления несанкционированных воздействий на основе использования метода дополнения состава подсистемы выявления в условиях ограничения временного ресурса

Ключевые слова: информационная система, признак, выявление

Для правильной работы подсистемы выявления несанкционированных воздействий (НСВ) на информационные системы (ИС) в условиях ограничения временного ресурса и меняющейся обстановки, когда информационная ценность элементов ИС также подвержена колебаниям, для оптимизации процессов обнаружения признаков и выявления НСВ целесообразно использование метода дополнения состава вышеуказанной подсистемы. Он основан на целенаправленном повышении характеристик по обнаружению признаков и выявлению НСВ в элементах ИС за счет добавления комплексов и средств в условиях ограничения временного ресурса /1/. Особенностью является то, что дополнительные средства дают различный эффект при распределении их на различные элементы ИС. Условие данной задачи может быть записано в следующем виде: $A^{вып} = \{a_1, a_2, \ldots, a_{k1}, \ldots, a_{K1}\}$ – множество элементов ИС, на которых выполняются требования по обнаружению и выявлению НСВ в момент времени t; $A^{невып} = \{a_{K1+1}, a_{K1+2}, \ldots, a_{k2}, \ldots, a_K\}$ – множество элементов ИТКС, на которых не выполняются требования по обнаружению и выявлению НСВ в момент времени t; $C_k^{инф}(t)$ – информационная ценность k-го элемента ИС в момент времени t; $B^{доп} = \{b_{1'}^{доп}, b_{2'}^{доп}, \ldots, b_{j'}^{доп}, \ldots, b_{J'}^{доп}\}$ – множество дополнительных средств обнаружения признаков и выявления НСВ на ИС; $T^{доп} = \{\tau_{1'}^{доп}, \tau_{2'}^{доп}, \ldots, \tau_{j'}^{доп}, \ldots, \tau_{J'}^{доп}\}$ – допустимое время, которое можно использовать для работы дополнительных средств обнаружения признаков и выявления НСВ на ИС.

Необходимо найти такой вариант добавления этих средств в элементы ИС, при котором достигается максимальное приращение относительного показателя выявления НСВ на ИС по отношению к допустимому временному ресурсу дополнительных средств:

$$\frac{\Delta Q_{ИС}^{доп}}{T_{ИС}^{доп}} \to \max, \qquad (1)$$

где $\Delta Q_{ИС}^{доп} = \{\Delta Q_{K1+1}^{доп}, \Delta Q_{K1+2}^{доп}, \ldots, \Delta Q_{k2}^{доп}, \ldots, \Delta Q_K^{доп}\}$ – приращение относительного показателя выявления дополненной подсистемы выявления НСВ на ИС; $\Delta Q_{k2}^{доп}$ – приращение относительного показателя выявления дополненного комплекса или дополнительного средства обнаружения признаков и выявления НСВ в $k2$-м элементе ИС; $T_{ИС}^{доп} = \{\tau_{K1+1}^{доп}, \tau_{K1+2}^{доп}, \ldots, \tau_{k2}^{доп}, \ldots, \tau_K^{доп}\}$ – допустимое время, которое можно использовать для работы дополнительных комплексов и средств подсистемы выявления НСВ на ИС; $\tau_{k2}^{доп}$ – временной ресурс дополнительного комплекса или средства обнаружения признаков и выявления НСВ в $k2$-м элементе ИС.

При этом необходимо учитывать следующие ограничения:

$$Q_{k2}^{доп}(t) \geq \alpha_{k2}, \qquad (2)$$

Скрыль Сергей Васильевич – МГТУ им. Н.Э. Баумана, д-р. техн. наук, профессор, e-mail: zi@bmstu.ru

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

Киселев Валим Вячеславович – ВИ МВД России, ст. преподаватель, тел. (473) 2-62-33-76

$$\sum_{j=1}^{J}\left(\tau_{j'}^{доп}\cdot h_{jk2}^{доп}\right)\le T^{доп}, \qquad (3)$$

где $Q_{k2}^{доп}$ – относительный показатель выявления дополненного комплекса или средства обнаружения признаков и выявления НСВ в $k2$-м элементе ИС; α_{k2} – требования по выявлению НСВ в $k2$-м элементе ИС; $\tau_{j'}^{доп}$ – временной ресурс дополнительного j'-го средства обнаружения признаков и выявления НСВ; $h_{j'k2}^{доп}$ – коэффициент использования j'-го дополнительного средства обнаружения признаков и выявления НСВ в $k2$-м элементе ИС:

$$h_{j'k2}^{доп}=\begin{cases}0, \text{ если в } a_{k2} \text{ не используется } b_{j'}^{доп},\\ 1, \text{ если в } a_{k2} \text{ используется } b_{j'}^{доп}.\end{cases}$$

Задача может быть решена подобно [2] следующим образом.

Относительный показатель выявления в $k2$-м элементе ИС до добавления дополнительных средств обнаружения признаков и выявления НСВ в $k2$-м элементе ИС имеет вид

$$Q_{k2}(t)=1-\frac{C_{k2}^{инф}(t)}{\max\limits_{k}C_{k}^{инф}}\cdot\left(1-\min_{i}\left(1-\mu_{ik2}(t)\cdot(1-\alpha_{ik2})\right)\right), \qquad (4)$$

где $C_{k2}^{инф}(t)$ – информационная ценность $k2$-го элемента ИС в момент времени t; $\mu_{ik2}(t)$ – показатель эффективности реализации i-го НСВ в $k2$-м элементе ИС в момент времени t; $i\in\{1,2,\ldots,i,\ldots,I\}$ – номер реализуемого НСВ на ИС; I – общее количество реализуемых НСВ на ИС.

Суммарный показатель выявления i-го НСВ в $k2$-м элементе ИС может быть записан в виде:

$$\alpha_{ik2}=\prod_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}, \qquad (5)$$

где α_{ijk2} – показатель выявления i-го НСВ j-м средством в $k2$-м элементе ИС; h_{jk2} – коэффициент использования j-го средства обнаружения признаков и выявления НСВ в $k2$-м элементе ИС:

$$h_{jk2}=\begin{cases}0, \text{ если в } a_{k2} \text{ не используется } b_{j},\\ 1, \text{ если в } a_{k2} \text{ используется } b_{j}.\end{cases}$$

Задачу целесообразно решать методом теории игр, рассматривая функции выигрыша, в случае добавления дополнительного средства обнаружения признаков и выявления НСВ в состав элемента ИС, и проигрыша, в отсутствие такового.

Относительный показатель выявления подсистемы выявления НСВ на ИС может быть записан в виде:

$$Q_{ИС}(t)=\frac{\sum\limits_{k1=1}^{K1}Q_{k1}(t)+\sum\limits_{k2=K1+1}^{K}Q_{k2}(t)}{K}. \qquad (6)$$

Исходя из условия задачи изменение приращения относительного показателя выявления системы в процессе добавления средств обнаружения признаков и выявления НСВ может происходить за счет изменения приращения относительного показателя выявления в элементах ИС, на которых не выполняются требования по обнаружению и выявлению НСВ в момент времени t. Таким образом, для каждого шага r добавления дополнительных средств в элементы ИС можно записать функцию изменения (выигрыша/проигрыша) относительного показателя выявления:

$$Q_{ИС\,r}^{доп}(t)=\frac{1}{K}\cdot\sum_{k2=K1+1}^{K}Q_{k2}(t). \qquad (7)$$

Соответственно приращение этой функции будет иметь вид

$$\Delta Q_{ИС\,r}^{доп}(t)=\frac{1}{K}\cdot\left(\Delta Q_{ИС\,r}^{+}(t)-\Delta Q_{ИС\,r}^{-}(t)\right). \qquad (8)$$

Неотрицательное приращение функции выигрыша может быть выражено как разница функций выигрыша между последующим шагом r и предыдущим $r-1$:

$$\Delta Q_{ИС\,r}^{+}(t)=Q_{ИС\,r}^{+}(t)-Q_{ИС\,r-1}^{+}(t). \qquad (9)$$

Неположительное приращение функции потерь может быть выражено как разница функций выигрыша между последующим шагом r и предыдущим $r-1$:

$$\Delta Q_{ИС\,r}^{-}(t)=Q_{ИС\,r}^{-}(t)-Q_{ИС\,r-1}^{-}(t). \qquad (10)$$

Функцию выигрыша до добавления дополнительного j'-го средства на шаге $r-1$ можно записать как

$$Q^{+}_{ИС\,r-1}(t)=\sum_{k2=K1+1}^{K}1-\frac{C^{инф}_{k2}(t)}{\max\limits_{k}C^{инф}_{k}}\cdot\times$$
$$\times\left(1-\min_{i}\left(1-\mu_{ik2}(t)\cdot\left(1-\prod_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}\right)\right)\right). \quad (11)$$

Функция выигрыша после добавления дополнительного j'-го средства на шаге r имеет вид

$$Q^{+}_{ИС\,r}(t)=\sum_{k2=K1+1}^{K}1-\frac{C^{инф}_{k2}(t)}{\max\limits_{k}C^{инф}_{k}}\cdot\left(1-\min_{i}(1-\mu_{ik2}(t)\times\right.$$
$$\left.\times\left(1-\prod_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}\cdot\prod_{j'=1}^{J'}\left(\alpha_{ij'k2}\right)^{h_{j'k2}}\right)\right)\Bigg), \quad (12)$$

где $\alpha_{ij'k2}$ – показатель выявления i-го НСВ j'-м средством в $k2$-м элементе ИС; $h_{j'k2}$ – коэффициент использования j'-го средства обнаружения признаков и выявления НСВ в $k2$-м элементе ИС:

$$h_{j'k2}=\begin{cases}0, \text{ если в } a_{k2} \text{ не используется } b_{j'},\\ 1, \text{ если в } a_{k2} \text{ используется } b_{j'}.\end{cases}$$

Функцию проигрыша до добавления дополнительного j'-го средства на шаге $r-1$ можно записать как

$$Q^{-}_{ИС\,r-1}(t)=\sum_{k2=K1+1}^{K}1-\frac{C^{инф}_{k2}(t)}{\max\limits_{k}C^{инф}_{k}}\times$$
$$\times\left(1-\min_{i}\left(1-\mu_{ik2}(t)\cdot\left(1-\prod_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}\right)\right)\right). \quad (13)$$

Функция проигрыша после добавления дополнительного j'-го средства на шаге r имеет вид

$$Q^{-}_{ИС\,r}(t)=\sum_{k2=K1+1}^{K}1-\frac{C^{инф}_{k2}(t)}{\max\limits_{k}C^{инф}_{k}}\times$$
$$\times\left(1-\min_{i}\left(1-\mu_{ik2}(t)\cdot\left(1-\frac{\prod\limits_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}}{\prod\limits_{j'=1}^{J'}\left(\alpha_{ij'k2}\right)^{h_{j'k2}}}\right)\right)\right). \quad (14)$$

После подстановки выражений (9)-(14) в (9) получаем:

$$\Delta Q^{доп}_{ИС\,r}(t)=\frac{1}{K}\cdot\left(\sum_{k2=K1+1}^{K}1-\frac{C^{инф}_{k2}(t)}{\max\limits_{k}C^{инф}_{k}}\times\right.$$
$$\times\left(1-\min_{i}\left(1-\mu_{ik2}(t)\cdot\left(1-\prod_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}\cdot\prod_{j'=1}^{J'}\left(\alpha_{ij'k2}\right)^{h_{j'k2}}\right)\right)\right)$$
$$-\sum_{k2=K1+1}^{K}1-\frac{C^{инф}_{k2}(t)}{\max\limits_{k}C^{инф}_{k}}\cdot\left(1-\min_{i}\left(1-\mu_{ik2}(t)\cdot\left(1-\prod_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}\right)\right)\right)-$$
$$-\sum_{k2=K1+1}^{K}1-\frac{C^{инф}_{k2}(t)}{\max\limits_{k}C^{инф}_{k}}\cdot\left(1-\min_{i}\left(1-\mu_{ik2}(t)\cdot\left(1-\frac{\prod\limits_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}}{\prod\limits_{j'=1}^{J'}\left(\alpha_{ij'k2}\right)^{h_{j'k2}}}\right)\right)\right)+$$
$$\left.+\sum_{k2=K1+1}^{K}1-\frac{C^{инф}_{k2}(t)}{\max\limits_{k}C^{инф}_{k}}\cdot\left(1-\min_{i}\left(1-\mu_{ik2}(t)\cdot\left(1-\prod_{j=1}^{J}\left(\alpha_{ijk2}\right)^{h_{jk2}}\right)\right)\right)\right). \quad (15)$$

Далее рассчитываем матрицу значений приращений функции изменения (выигрыша/проигрыша) относительного показателя выявления подсистемы выявления НСВ на каждом r-м шаге добавления дополнительных средств в $k2$-е элементы ИС с помощью выражения (16). Необходимо заметить, что различные значения функций изменения (выигрыша/проигрыша) в случае добавления одного и того же дополнительного средства обнаружения признаков и выявления НСВ в состав разных элементов ИС определяются их различной информационной ценностью. Кроме того, составляем матрицу допустимого временного ресурса $\tau^{доп}_{k2}$ дополнительных комплексов или средств обнаружения признаков и выявления НСВ в $k2$-х элементах ИС. После чего находим оптимальные значения по критерию (1) с учетом ограничений (2)-(3).

На рис. 1-2 показаны варианты оптимизации дополненного состава подсистемы выявления НСВ в условиях ограничения временного ресурса на основе приращения относительного показателя выявления подсистемы без учета и с учетом временного ресурса дополнительных средств. В ходе решения задачи происходило распределение 8 дополнительных средств обнаружения признаков и выявления НСВ на 6 элементов ИС.

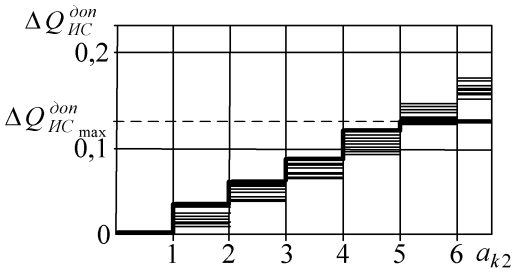

Рис. 1. Вариант оптимизации дополненного состава подсистемы выявления НСВ в условиях ограничения временного ресурса на основе приращения относительного показателя выявления подсистемы без учета временного ресурса дополнительных средств

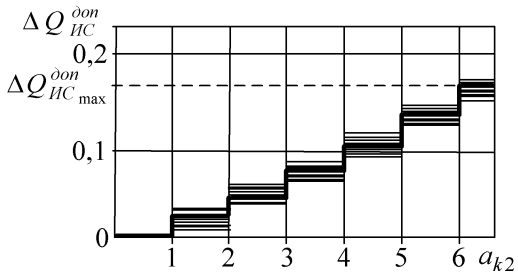

Рис. 2. Вариант оптимизации дополненного состава системы выявления НСВ в условиях ограничения временного ресурса на основе приращения относительного показателя выявления подсистемы с учетом временного ресурса дополнительных средств

Из анализа полученных зависимостей видно, что применение второго варианта в этих условиях обладает большей эффективностью, так как оптимизация проводится по критерию «максимальное качество за минимальное (ограниченное) время».

Таким образом, рассмотрен метод дополнения состава подсистемы выявления НСВ за счет добавления комплексов и средств обнаружения признаков и выявления НСВ в условиях ограничения временного ресурса, позволяющий в процессе эксплуатации ИС повысить относительный показатель выявления подсистемы.

Литература

1. Душкин А.В. Методы оптимизации структуры адаптивной системы распознавания угроз несанкционированного воздействия на защищенные информационные телекоммуникационные системы / А.В. Душкин, П.С. Молоканов, А.В. Проскуряков // Системы управления и информационные технологии. 2007. №4.2(30). С. 243-247.

2. Воробьев А.А. Адаптивное управление защищенностью информации в автоматизированных системах / А.А. Воробьев, А.В. Непомнящих // Информационные технологии. 2003. №12. С. 26-30.

Московский государственный технический университет им. Н.Э. Баумана
Воронежский государственный технический университет
Moscow State Technical University named after N. E. Bauman
Voronezh State Technical University

SUBSYSTEM STRUCTURE ADDITION METHOD FOR DETECTION OF UNAUTHORIZED ACTIONS ON INFORMATION SYSTEMS UNDER LIMITED TIME RESOURCE CONDITIONS

S.V. Skryl', A.V. Dushkin, V.V. Kiselev

The article considers issues of indications detection processes optimization and unauthorized actions detection on the basis of detection subsystem structure addition methods under limited time resource conditions

Keywords: information system, indication, detection