В. В. Киселев

ОСНОВНЫЕ ТЕОРЕМЫ ТЕОРИИ СИНТЕЗА СИСТЕМ РАСПОЗНАВАНИЯ ВРЕДОНОСНЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ В ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Основополагающими теоремами при решении проблемы синтеза систем распознавания вредоносных воздействий на информационные процессы защищенных информационных систем являются **теорема об объективности факторов угроз информационной безопасности и защиты от их вредоносного воздействия** и **теорема о наличии причинно-следственных связей при реализации угроз.**

В соответствии с первой теоремой защищенные информационные системы различных классов, их компоненты и обрабатываемая в них информация являются объектом воздействия различных угроз, а следовательно, и объектом защиты и обеспечения информационной безопасности.

Для доказательства этого, на первый взгляд, простого положения воспользуемся аппаратом теории множеств и по аналогии с [1] установим соответствия между закономерностями функционирования защищенных информационных систем, возникновения угроз информационной безопасности и реализации механизмов защиты информации.

При этом рассмотрим два случая определения областей отправления и прибытия соответствий.

В первом случае областью отправления соответствия $\{X\}$ будет множество закономерностей функционирования защищенной информационной системы, в качестве области прибытия соответствия — множество $\{Y\}$ закономерностей возникновения угроз, их возможностей по воздействию на информацию, циркулирующую в защищенной информационной системе.

Во втором случае областью отправления соответствия будет множество $\{Y\}$, в качестве области прибытия соответствия — множество $\{Z\}$ закономерностей реализации механизмов защиты информации.

Доказательство теоремы предлагается осуществлять на основе определения способа сопоставления элементов этих множеств. Таким образом, выявляются и представляются в виде композиции соответствия q, областей интересов злоумышленника к защищенной информационной системе и механизмов защиты информации к злоумышленнику. При этом допускается сопоставление не полного, а ограниченного количества элементов множеств $\{X\}$, $\{Y\}$, $\{Z\}$, представляющих наиболее характерные закономерности угроз информационной безопасности защищенным информационным системам и защиты от их воздействия. Это можно представить выражениями $q = (X, Y, Q)$ и $s = (Y, Z, S)$ соответственно,

где $\{X\}$ — совокупность элементов, сопоставляемых с элементами $\{Y\}$;

$\{Y\}$ — совокупность элементов, сопоставляемых с элементами $\{X\}$ и $\{Z\}$;

$\{Z\}$ — совокупность элементов, сопоставляемых с элементами $\{Y\}$;

$\{Q \subset X \times Y\}$ — множество, определяющее закон, в соответствии с которым осуществляется определение q, представляющее собой перечисление всех пар (x, y), участвующих в сопоставлении;

$\{S \subset Y \times Z\}$ — множество, определяющее закон, в соответствии с которым осуществляется определение s, представляющее собой перечисление всех пар (y, z), участвующих в сопоставлении.

Рассмотрим содержание наиболее характерных закономерностей воздействия угроз на защищенные информационные системы.

Любая защищенная информационная система в силу своего исключительного предназначения, разнообразия используемых технических средств и решаемых задач является объектом вредоносных воздействий в силу следующих закономерностей:

- наличие информационного потока — x_1;
- наличие стандартных правил организации вычислительного процесса — x_2;
- наличие механизмов закрытия информации — x_3;

- использование в качестве носителей информации пакетов данных, подвергающихся трассировке, искажению, перехвату и выделению содержащейся в них информации, — x_4;
- наличие узлов концентрации технических средств обработки и передачи информации, объективно отражающих архитектуру и топологию защищенной информационной системы, способствующее вскрытию и определению механизмов сбора, обработки и обмена информацией, — x_5;
- наличие объективных демаскирующих признаков, обеспечивающих реализацию вредоносных воздействий, — x_6;
- наличие стандартных данных в массивах защищаемой информации, способствующих получению нарушителем достоверной информации, — x_7.

Основными объективными закономерностями вредоносного воздействия являются:
- отсутствие защитных механизмов в реализации правил пакетообразования, проявляющихся при передаче данных , — y_1 ;
- возможность использования злоумышленником в качестве источников информации физических линий передачи данных —y_2;
- возможность использования технических средств для решения задач перехвата и трассирования пакетов данных — y_3;
- возможность модификации пакетов передаваемых данных и введения в них ложной информации — y_4;
- возможность анализа данных о средствах защиты информации, архитектуре и топологии их использования в механизмах обработки и хранения данных — y_5;
- возможность внесения изменений в процесс функционирования защищенной информационной системы с целью придания вредоносных свойств программному обеспечению — y_6;
- обеспечение признаковой доступности, позволяющей осуществлять привязку средств обработки информации к конкретным центрам обработки информации, — y_7;
- способность выделения при функционировании защищенной информационной системы различных видов информации, что позволяет вести прямой ее перехват с использованием недокументированных возможностей программно-аппаратных средств, — y_8.

Аналогичным образом вредоносные воздействия на информацию являются объектом противодействия угрозам информационной безопасности в силу возможности выявления действий злоумышленника, связанных с попытками:
- анализа защищенности информационной системы — z_1;
- вскрытия механизмов обеспечения защищенности — z_2;
- внедрения ложного доверенного субъекта* доступа к защищенной информационной системе — z_3;
- анализа информации, проходящей через внедренный доверенный объект, —z_4;
- несанкционированного воздействия на информацию — z_5;
- сокрытия следов несанкционированного воздействия на информацию — z_6.

Рассмотренные основные закономерности свойств и признаков информационной системы и вредоносных воздействий можно представить соответственными областями отправления (1), (2) и прибытия (2), (3):

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}; \quad (1)$$

$$Y = \{y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8\}; \quad (2)$$

$$Z = \{z_1, z_2, z_3, z_4, z_5, z_6\}. \quad (3)$$

Содержательное описание законов соответствия, $Q \subset X \times Y$ и $S \subset Y \times Z$ представим прямым произведением множеств:

$$X \,\&\, Y = \{(x_i, y_j) \mid x_i \in X,\ y_j \in Y,\ i = 1, 2, \ldots, 7,\ j = 1, 2, \ldots, 8\}; \quad (4)$$

$$Y \,\&\, Z = \{(y_j, z_k) \mid y_j \in Y,\ z_k \in Z,\ j = 1, 2, \ldots, 8,\ k = 1, 2, \ldots, 6\}. \quad (5)$$

Эти множества дают возможность получить ряд известных соответствий $q = (X, Y, Q)$ и $s =$

* Субъект доступа — лицо или процесс, действия которого регламентируются правилами закрытия информации.

(Y, Z, S), подтверждающих, что защищенные информационные системы объективно являются как объектом угроз информационной безопасности, так и объектом защиты от их вредоносного воздействия.

К таким соответствиям относятся:

$$q_1 = (x_1, y_1);\ R_{11}q_1 = \{x_1\};\ R_{21}q_1 = \{y_1\}, \quad (6)$$
$$q_2 = (x_1, y_2);\ R_{12}q_2 = \{x_1\};\ R_{22}q_2 = \{y_2\}, \quad (7)$$
$$q_3 = (x_1, y_4);\ R_{13}q_3 = \{x_1\};\ R_{23}q_3 = \{y_1\}, \quad (8)$$
$$q_4 = (x_2, y_3);\ R_{14}q_4 = \{x_2\};\ R_{24}q_4 = \{y_3\}, \quad (9)$$
$$q_5 = (x_2, y_4);\ R_{15}q_5 = \{x_2\};\ R_{25}q_5 = \{y_4\}, \quad (10)$$
$$q_6 = (x_2, y_5);\ R_{16}q_6 = \{x_2\};\ R_{26}q_6 = \{y_5\}, \quad (11)$$
$$q_7 = (x_3, y_5);\ R_{17}q_7 = \{x_3\};\ R_{27}q_7 = \{y_5\}, \quad (12)$$
$$q_8 = (x_3, y_7);\ R_{18}q_8 = \{x_3\};\ R_{28}q_8 = \{y_7\}, \quad (13)$$
$$q_9 = (x_3, y_8);\ R_{19}q_9 = \{x_3\};\ R_{29}q_9 = \{y_8\}, \quad (14)$$
$$q_{10} = (x_4, y_3);\ R_{110}q_{10} = \{x_4\};\ R_{210}q_{10} = \{y_3\}, \quad (15)$$
$$q_{11} = (x_4, y_4);\ R_{111}q_{11} = \{x_4\};\ R_{211}q_{11} = \{y_4\}, \quad (16)$$
$$q_{12} = (x_4, y_8);\ R_{112}q_{12} = \{x_4\};\ R_{212}q_{12} = \{y_8\}, \quad (17)$$
$$q_{13} = (x_5, y_2);\ R_{113}q_{13} = \{x_5\};\ R_{213}q_{13} = \{y_2\}, \quad (18)$$
$$q_{14} = (x_5, y_3);\ R_{114}q_{14} = \{x_5\};\ R_{214}q_{14} = \{y_3\}, \quad (19)$$
$$q_{15} = (x_5, y_6);\ R_{115}q_{15} = \{x_5\};\ R_{215}q_{15} = \{y_6\}; \quad (20)$$
$$q_{16} = (x_6, y_3);\ R_{116}q_{16} = \{x_6\};\ R_{216}q_{16} = \{y_3\}, \quad (21)$$
$$q_{17} = (x_6, y_4);\ R_{117}q_{17} = \{x_6\};\ R_{217}q_{17} = \{y_4\}, \quad (22)$$
$$q_{18} = (x_6, y_6);\ R_{118}q_{18} = \{x_6\};\ R_{218}q_{18} = \{y_6\}, \quad (23)$$
$$q_{19} = (x_6, y_7);\ R_{119}q_{19} = \{x_6\};\ R_{219}q_{19} = \{y_7\}, \quad (24)$$
$$q_{20} = (x_7, y_5);\ R_{120}q_{20} = \{x_7\};\ R_{220}q_{20} = \{y_5\}, \quad (25)$$
$$s_1 = (y_3, z_1);\ R_{31}s_1 = \{y_3\};\ R_{41}s_1 = \{z_1\}, \quad (26)$$
$$s_2 = (y_5, z_1);\ R_{32}s_2 = \{y_5\};\ R_{42}s_2 = \{z_1\}, \quad (27)$$
$$s_3 = (y_8, z_1);\ R_{33}s_3 = \{y_8\};\ R_{43}s_3 = \{z_1\}, \quad (28)$$
$$s_4 = (y_4, z_2);\ R_{34}s_4 = \{y_4\};\ R_{44}s_4 = \{z_2\}, \quad (29)$$
$$s_5 = (y_6, z_2);\ R_{35}s_5 = \{y_6\};\ R_{45}s_5 = \{z_2\}, \quad (30)$$
$$s_6 = (y_2, z_3);\ R_{36}s_6 = \{y_2\};\ R_{46}s_6 = \{z_3\}, \quad (31)$$
$$s_7 = (y_6, z_3);\ R_{37}s_7 = \{y_6\};\ R_{47}s_7 = \{z_3\}, \quad (32)$$
$$s_8 = (y_7, z_3);\ R_{38}s_8 = \{y_7\};\ R_{48}s_8 = \{z_3\}, \quad (33)$$
$$s_9 = (y_1, z_4);\ R_{39}s_9 = \{y_1\};\ R_{49}s_9 = \{z_4\}, \quad (34)$$
$$s_{10} = (y_5, z_4);\ R_{310}s_{10} = \{y_5\};\ R_{410}s_{10} = \{z_4\}, \quad (35)$$
$$s_{11} = (y_4, z_5);\ R_{311}s_{11} = \{y_4\};\ R_{411}s_{11} = \{z_5\}, \quad (36)$$
$$s_{12} = (y_6, z_5);\ R_{312}s_{12} = \{y_6\};\ R_{412}s_{12} = \{z_5\}, \quad (37)$$
$$s_{13} = (y_6, z_6);\ R_{313}s_{13} = \{y_6\};\ R_{413}s_{13} = \{z_6\}, \quad (38)$$

где $R_{1i}q_i$ — область определения соответствия, в которое входят элементы $\{X\}$, участвующие в сопоставлении со множеством $\{Y\}$;

$R_{2i}q_j$ — область значений соответствия, в которое входят элементы множества $\{Y\}$, участвующие в сопоставлении со множеством $\{X\}$;

$R_{3j}s_j$ — область значений соответствия, в которое входят элементы множества $\{Y\}$, участвующие в сопоставлении со множеством $\{Z\}$;

$R_{4j}s_k$ — область значений соответствия, в которое входят элементы множества $\{Z\}$, участвующие в сопоставлении со множеством $\{Y\}$.

В соответствии со второй теоремой существуют причинно-следственные связи как при выполнении функций вредоносных воздействий, так и при выполнении функций защиты информации. Это

предполагает реализацию элементов множеств соответствия $\{Y\}$ и $\{Z\}$ лишь в определенной последовательности. С целью доказательства этой теоремы рассмотрим соответствия (6) – (38). Как следует из содержания этих соответствий, имеют место следующие последовательности:

$$y_1 \to y_2; \quad y_2 \to y_3; \quad \begin{matrix} y_3 \to y_4; \\ y_3 \to y_5; \\ y_3 \to y_8; \end{matrix} \quad \begin{matrix} y_4 \to y_6; \\ y_4 \to y_7; \end{matrix} \quad \begin{matrix} y_5 \to y_6; \\ y_5 \to y_7; \end{matrix} \quad y_8 \to y_5;$$

$$\begin{matrix} z_1 \to z_2; \\ z_1 \to z_3; \end{matrix} \quad \begin{matrix} z_2 \to z_3; \\ z_2 \to z_3; \end{matrix} \quad z_2 \to z_4; \quad z_3 \to z_4; \quad z_4 \to z_5; \quad z_5 \to z_6;$$

в которых выражение $y_m \to y_n\,(z_g \to z_h)$ означает, что закономерность $y_n\,(z_g)$ может быть реализована лишь при условии реализации закономерности $y_m\,(z_h)$, причем определенность последовательностей элементов множества $\{Z\}$ является следствием порядка реализации элементов множества $\{Y\}$.

Таким образом, доказаны:

- объективная доступность сведений о защищенной информационной системе для реализации вредоносного воздействия на ее информационные ресурсы;
- наличие причинно-следственных связей как при выполнении функций вредоносных воздействий, так и при выполнении функций защиты информации в такого рода системах.

Приведенные теоремы являются основой методов синтеза систем распознавания вредоносных воздействий на информационные процессы в защищенных информационных системах.

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.