Воронежский институт МВД России

Методика анализа обеспечения информационной безопасности на объекте информатизации

Методические рекомендации

Воронеж 2019

ББК 32.973

Рассмотрены и одобрены на заседании кафедры информационной безопасности. Протокол № 11 от 11 июня 2019 г.

Рассмотрены и одобрены на заседании методического совета института. Протокол № 7 от 18 марта 2019 г.

Рассмотрены и рекомендованы на заседании редакционно-издательского совета института. Протокол № 3 от 26 марта 2019 г.

Киселев В.В., Нестеровский О.И., Лиходедеов Д.Ю. и др. Методика анализа обеспечения информационной безопасности на объекте информатизации: методические рекомендации. – Воронеж: Воронежский институт МВД России, 2019. – 77 с.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Возросшие требования к оперативности информационных процессов в различных областях деятельности современного общества, а также расширение возможностей сетевого построения информационных систем и внедрение методов распределенной обработки данных за счет реализации теледоступа к вычислительным средствам привели к интегрированию систем обработки информации и систем ее обмена. Угрозы информационной безопасности инфокоммуникационных систем [1, 2] являются фактором существенного снижения эффективности их применения в тех сферах общественной жизни, которые целевым образом ориентированы на обработку конфиденциальной информации. Это обстоятельство имеет особую актуальность для МВД России, требования к информационной безопасности работы которого за последнее время существенно ужесточились.

Особую остроту проблема защиты инфокоммуникационной среды приобретает в деятельности территориальных органов внутренних дел (ОВД) – министерств внутренних дел, главных управлений внутренних дел и управлений внутренних дел субъектов Российской Федерации. Инфокоммуникационные системы территориальных органов аккумулируют значительный объем конфиденциальной информации о криминальной обстановке.

Значительная ценность хранимых и обрабатываемых территориальными инфокоммуникационными системами ОВД данных обусловливает значительный интерес к ним со стороны как отдельных лиц, совершивших преступления, их группировок, так и организаций антиконституционной направленности, спецслужб иностранных государств, а также партий, общественно-политических движений и средств массовой информации, стремящихся использовать для своих целей оперативно-служебную информацию ОВД. Эти интересы служат мотивами противоправных действий в отношении информационных ресурсов инфокоммуникационных систем ОВД. Реализация данных интересов является главным фактором совершенствования методов и средств несанкционированного доступа к информации инфокоммуникационных систем ОВД, прежде всего с целью противоправного копирования конфиденциальных данных.

Необходимость совершенствования организации противодействия нарушению безопасности информации в деятельности территориальных ОВД в этих условиях очевидна.

Методика оценки угрозы и связанная с ней методика анализа обеспечения информационной безопасности на объекте информатизации является основой для реализации алгоритмов распознавания противоправных действий как источника угроз и оценки уровня данных угроз информационной безопасности объекта информатизации, позволяющих не только выявлять признаки подобных действий, но и предложить способы и средства их идентификации [3], а как следствие и противодействия.

1. Информационные ресурсы систем органов внутренних дел как объект угроз нарушения информационной безопасности

1.1. Угрозы нарушения информационной безопасности как негативный фактор влияния на информационные ресурсы на объекте информатизации

Так как технологическую основу территориальных на объекте информатизации составляют ИВС, факторы нарушения информационной безопасности их информационных ресурсов аналогичны уязвимостям информационной безопасности любой распределенной вычислительной сети независимо от области ее применения. Такими уязвимостями могут являться:

- использование широковещательной среды передачи;
- применение нестойких алгоритмов идентификации удаленных субъектов и объектов ИВС;
- использование протоколов динамического изменения маршрутизации с нестойкими алгоритмами идентификации;
- применение алгоритмов удаленного поиска с использованием широковещательных и направленных поисковых запросов;
- возможность анонимного захвата одним субъектом ИВС множества физических или логических каналов связи.

Систематизация основных причин нарушения информационной безопасности информационных ресурсов ИКС позволила ввести понятие угрозы нарушения данного состояния информации в этой системе, инвариантной к типу ИВС.

Исходя из этого, под угрозой нарушения информационной безопасности информационных ресурсов ИВС понимается несанкционированное получение защищаемой информации лицами или программами (процессами), не имеющими на это специальных полномочий, и под удаленной атакой по нарушению информационной безопасности информационных ресурсов ИВС

будем понимать реализацию такого рода угрозы.

При систематизации оснований для классификации угроз нарушения информационной безопасности информационных ресурсов ИВС будем исходить из того, что любая классификация предполагает выявление таких отличительных признаков, используя которые, можно наиболее точно описать характеризуемые явления или объекты [1, 2].

С этой целью используем стандартное описание признаков, характеризующие возможные пути нарушения информационной безопасности информационных ресурсов на объекте информатизации.

1.2. Механизмы реализации угроз нарушения информационной безопасности информационных ресурсов на объекте информатизации

Как показывают результаты исследований процессов функционирования различных сетей и систем независимо от их топологии и инфраструктуры, механизмы реализации угроз нарушения информационной безопасности информационных ресурсов их ИВС инвариантны по отношению к особенностям конкретного сегмента. Это объясняется тем, что ИВС, как технологическая основа сегментов ИКС, проектируются на основе одних и тех же принципов, а, следовательно, имеют практически одинаковые проблемы информационной безопасности.

Классификация удаленных атак по нарушению информационной безопасности информационных ресурсов ИВС описана в литературе достаточно подробно.

- Анализ сетевого трафика.
- Подмена доверенного объекта или субъекта ИВС.
- Ложный объект ИВС.
- Использование ложного объекта для организации удаленной атаки на ИВС.

Существующая практика применения информационно-телекоммуникационных систем класса аналогичных ИМТС ОВД дает основания полагать, что наиболее часто в качестве ложного объекта, при реализации противоправных действий в отношении их информационных ресурсов, используются вредоносные программы. Подобного рода программы имеют широкий диапазон особенностей, что делает их основным инструментом такого рода действий.

1.3. Принципы распознавания угроз нарушения информационной безопасности информационных ресурсов на объекте информатизации

Исследования известных методов анализа влияния негативных факторов на процессы функционирования сложных автоматизированных систем позволили установить, что при решении подобных задач ограничиваются преимущественно эвристическими правилами формирования аналитических, логических и смысловых соотношений между анализируемыми параметрами и интуитивными (экспертными) оценками изменения эффективности этих систем. Это обусловливает необходимость сформулировать принципы распознавания угроз нарушения информационной безопасности информационных ресурсов на объекте информатизации.

Принцип достоверности отражения информационных процессов в ИВС предполагает в качестве основы для реализации алгоритмов распознавания угроз нарушения информационной безопасности информационных ресурсов ИВС непрерывный анализ информационного пространства сети с целью обнаружения признаков угроз данного типа и их систематизации.

Логически вытекающий из данного принципа принцип полноты анализа угроз нарушения информационной безопасности информационных ресурсов ИВС приводит к необходимости использования методов и средств мониторинга информационного пространства ИВС.

В соответствии с принципом поэтапной обобщаемости результатов распознавания угроз нарушения информационной безопасности информационных ресурсов ИВС оценка уровня проявления угрозы должна осуществляться с учетом многоэтапности стратегий несанкционированного доступа к информации ИВС.

Принцип многоуровневости функционального анализа данных мониторинга информационного пространства ИВС предполагает наличие нескольких уровней функционального представления противоправных действий по реализации угроз нарушения информационной безопасности информационных ресурсов ИВС.

2. Теория синтеза систем распознавания угроз нарушения информационной безопасности на объекте информатизации

Совокупность признаков распознавания угроз нарушения информационной безопасности должна быть структурированной, что базируется на известном положении системного анализа [4], в соответствии с которым энтропия структурированной системы элементов, связанных одной целью, ниже энтропии совокупности несвязанных элементов. Это обусловливает необходимость выявления взаимосвязей между признаками распознавания, позволяющими представлять их не простой совокупностью, а в виде системы определенным образом связанных элементов оценки угроз нарушения информационной безопасности информации. Установим соответствия между закономерностями функционирования ИКС объекта информатизации, 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 сегмента ИКС, в качестве

области прибытия соответствия – множество **{*Y*}** закономерностей возникновения угроз, их возможностей по воздействию на информацию, циркулирующую в сегменте.

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

Доказательство утверждения предлагается осуществлять на основе определения способа сопоставления элементов этих множеств. Таким образом, выявляются и представляются в виде композиции соответствия ***q***, областей интересов нарушителя к сегменту ИКС 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 нарушения безопасности информационных ресурсов сегмента 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 нарушения безопасности информационных ресурсов ИКС объекта информатизации.

Любой сегмент ИКС в силу своего исключительного предназначения, разнообразия используемых технических средств и решаемых задач является

объектом угроз нарушения безопасности информационных ресурсов 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, перехвату и выделению содержащейся в них информации, x_4;

- наличие узлов концентрации технических средств обработки и передачи информации, объективно отражающих архитектуру и топологию сегмента, способствующее вскрытию и определению механизмов сбора, обработки и обмена информацией, x_5;

- наличие объективных демаскирующих признаков, обеспечивающих реализацию угроз нарушения безопасности информации, x_6;

- наличие стандартных данных в массивах защищаемой информации, способствующих получению нарушителем достоверной информации, x_7.

Основными объективными закономерностями проявления угроз нарушения безопасности информации являются:

- отсутствие защитных механизмов в реализации правил пакетообразования, y_1, проявляющихся при передаче данных;

- 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 сегмента 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 сегмента различных видов информации, что позволяет вести прямой ее перехват с использованием недокументированных возможностей программно-аппаратных средств, y_8.

Аналогичным образом угрозы нарушения конфиденциальности информационных ресурсов территориальных сегментов ИМТС являются объектом противодействия в силу возможности выявления действий нарушителей, связанных с попытками:

- анализа защищенности информационных ресурсов сегмента, z_1;

- вскрытия механизмов обеспечения защищенности, z_2;

- внедрения ложного доверенного субъекта* доступа к информационным ресурсам сегмента, z_3;

- анализа информации, проходящей через внедренный доверенный объект, z_4;

- перехвата информации, z_5;

- сокрытия следов противоправных действий, z_6.

Рассмотренные основные закономерности свойств и признаков территориального сегмента и угроз нарушения безопасности его информационных ресурсов можно представить соответственными областями отправления (2.1.1), (2.1.2) и прибытия (2.1.2), (2.1.3):

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7\}; \quad (2.1.1)$$

$$Y = \{y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8\}; \quad (2.1.2)$$

$$Z = \{z_1, z_2, z_3, z_4, z_5, z_6\}. \quad (2.1.3)$$

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

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

$$X \,\&\, Y = \{(x_i, y_j) |\, x_i \in X, y_j \in Y, i = 1, 2, \ldots, 7, j = 1, 2, \ldots, 8\}. \quad (2.1.4)$$

$$Y \,\&\, Z = \{(y_j, z_k) |\, y_j \in Y, z_k \in Z, j = 1, 2, \ldots, 8, k = 1, 2, \ldots, 6\}. \quad (2.1.5)$$

Эти множества дают возможность получить ряд известных соответствий $q = (X, Y, Q)$ и $s = (Y, Z, S)$, подтверждающих, что ИКС ОВД объективно являются как объектом угроз нарушения безопасности информационных ресурсов, так и объектом защиты от их проявления.

К таким соответствиям относятся:

$$q_1 = (x_1, y_1);\ R_{11}q_1 = \{x_1\};\ R_{21}q_1 = \{y_1\}, \quad (2.1.6)$$
$$q_2 = (x_1, y_2);\ R_{12}q_2 = \{x_1\};\ R_{22}q_2 = \{y_2\}, \quad (2.1.7)$$
$$q_3 = (x_1, y_4);\ R_{13}q_3 = \{x_1\};\ R_{23}q_3 = \{y_1\}, \quad (2.1.8)$$
$$q_4 = (x_2, y_3);\ R_{14}q_4 = \{x_2\};\ R_{24}q_4 = \{y_3\}, \quad (2.1.9)$$
$$q_5 = (x_2, y_4);\ R_{15}q_5 = \{x_2\};\ R_{25}q_5 = \{y_4\}, \quad (2.1.10)$$
$$q_6 = (x_2, y_5);\ R_{16}q_6 = \{x_2\};\ R_{26}q_6 = \{y_5\}, \quad (2.1.11)$$
$$q_7 = (x_3, y_5);\ R_{17}q_7 = \{x_3\};\ R_{27}q_7 = \{y_5\}, \quad (2.1.12)$$
$$q_8 = (x_3, y_7);\ R_{18}q_8 = \{x_3\};\ R_{28}q_8 = \{y_7\}, \quad (2.1.13)$$
$$q_9 = (x_3, y_8);\ R_{19}q_9 = \{x_3\};\ R_{29}q_9 = \{y_8\}, \quad (2.1.14)$$
$$q_{10} = (x_4, y_3);\ R_{110}q_{10} = \{x_4\};\ R_{210}q_{10} = \{y_3\}, \quad (2.1.15)$$
$$q_{11} = (x_4, y_4);\ R_{111}q_{11} = \{x_4\};\ R_{211}q_{11} = \{y_4\}, \quad (2.1.16)$$
$$q_{12} = (x_4, y_8);\ R_{112}q_{12} = \{x_4\};\ R_{212}q_{12} = \{y_8\}, \quad (2.1.17)$$
$$q_{13} = (x_5, y_2);\ R_{113}q_{13} = \{x_5\};\ R_{213}q_{13} = \{y_2\}, \quad (2.1.18)$$
$$q_{14} = (x_5, y_3);\ R_{114}q_{14} = \{x_5\};\ R_{214}q_{14} = \{y_3\}, \quad (2.1.19)$$
$$q_{15} = (x_5, y_6);\ R_{115}q_{15} = \{x_5\};\ R_{215}q_{15} = \{y_6\}; \quad (2.1.20)$$
$$q_{16} = (x_6, y_3);\ R_{116}q_{16} = \{x_6\};\ R_{216}q_{16} = \{y_3\}, \quad (2.1.21)$$
$$q_{17} = (x_6, y_4);\ R_{117}q_{17} = \{x_6\};\ R_{217}q_{17} = \{y_4\}, \quad (2.1.22)$$
$$q_{18} = (x_6, y_6);\ R_{118}q_{18} = \{x_6\};\ R_{218}q_{18} = \{y_6\}, \quad (2.1.23)$$
$$q_{19} = (x_6, y_7);\ R_{119}q_{19} = \{x_6\};\ R_{219}q_{19} = \{y_7\}, \quad (2.1.24)$$
$$q_{20} = (x_7, y_5);\ R_{120}q_{20} = \{x_7\};\ R_{220}q_{20} = \{y_5\}, \quad (2.1.25)$$
$$s_1 = (y_3, z_1);\ R_{31}s_1 = \{y_3\};\ R_{41}s_1 = \{z_1\}, \quad (2.1.26)$$
$$s_2 = (y_5, z_1);\ R_{32}s_2 = \{y_5\};\ R_{42}s_2 = \{z_1\}, \quad (2.1.27)$$
$$s_3 = (y_8, z_1);\ R_{33}s_3 = \{y_8\};\ R_{43}s_3 = \{z_1\}, \quad (2.1.28)$$
$$s_4 = (y_4, z_2);\ R_{34}s_4 = \{y_4\};\ R_{44}s_4 = \{z_2\}, \quad (2.1.29)$$
$$s_5 = (y_6, z_2);\ R_{35}s_5 = \{y_6\};\ R_{45}s_5 = \{z_2\}, \quad (2.1.30)$$

$$s_6 = (y_2, z_3);\ R_{36}s_6 = \{y_2\};\ R_{46}s_6 = \{z_3\}, \quad (2.1.31)$$
$$s_7 = (y_6, z_3);\ R_{37}s_7 = \{y_6\};\ R_{47}s_7 = \{z_3\}, \quad (2.1.32)$$
$$s_8 = (y_7, z_3);\ R_{38}s_8 = \{y_7\};\ R_{48}s_8 = \{z_3\}, \quad (2.1.33)$$
$$s_9 = (y_1, z_4);\ R_{39}s_9 = \{y_1\};\ R_{49}s_9 = \{z_4\}, \quad (2.1.34)$$
$$s_{10} = (y_5, z_4);\ R_{310}s_{10} = \{y_5\};\ R_{410}s_{10} = \{z_4\}, \quad (2.1.35)$$
$$s_{11} = (y_4, z_5);\ R_{311}s_{11} = \{y_4\};\ R_{411}s_{11} = \{z_5\}, \quad (2.1.36)$$
$$s_{12} = (y_6, z_5);\ R_{312}s_{12} = \{y_6\};\ R_{412}s_{12} = \{z_5\}, \quad (2.1.37)$$
$$s_{13} = (y_6, z_6);\ R_{313}s_{13} = \{y_6\};\ R_{413}s_{13} = \{z_6\}, \quad (2.1.38)$$

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

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

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

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

Таким образом существуют причинно-следственные связи, как при реализации угроз нарушения безопасности информационных ресурсов, так и при выполнении функций защиты информации. Это предполагает реализацию элементов множеств соответствия $\{Y\}$ и $\{Z\}$ лишь в определенной последовательности. С целью доказательства утверждения рассмотрим соответствия (2.1.6) – (2.1.38). Как видно из их содержания, имеют место последовательности:

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

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

в которых выражения $y_m \to y_n$ $(z_g \to z_h)$ означают, 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*}**.

Следствием является требование к структуре системы распознавания, которая в этих условиях должна быть многоуровневой иерархической. Уровни иерархии структуры системы распознавания определяются исходя из того, что каждому уровню структуры соответствует определенная степень обобщения признаков угроз нарушения информационной безопасности информации, причем признаки нижнего уровня имеют самую низкую степень обобщения, а признак верхнего уровня является результирующим.

Следует заметить, что термин «многоуровневая структура» относится к структурам с тремя и более уровнями. Это предположение основано на восприятии неструктурированной системы распознавания как двухуровневой системы простейшего анализа неупорядоченной совокупности признаков, в которой первый уровень составляют анализируемые признаки, второй – сам анализатор.

Рассматриваемое требование иерархичности структуры системы распознавания базируется на очевидном предположении, в соответствии с которым обобщение признаков распознавания представляет собой процесс поэтапного обобщения характера проявления угроз нарушения информационной безопасности информации, начиная с множества признаков, отражающих лишь отдельные проявления и заканчивая одним, результирующим признаком.

С целью разработки методологии синтеза систем распознавания угроз нарушения информационной безопасности информационных ресурсов на объекте информатизации воспользуемся положениями методологии концептуального проектирования защищенных информационных систем.

В настоящее время создание, развитие и совершенствование систем распознавания угроз информационной безопасности в целом и систем распознавания угроз нарушения информационной безопасности

информационных ресурсов в частности возможно на путях обеспечения эффективности применения соответствующих способов, средств и мероприятий по направлениям:

- идентификации средств, потенциально решающих задачи систем распознавания угроз;

- повышения эффективности управления системой распознавания и ее информационным обеспечением;

- совершенствования контроля и оценки эффективности средств, используемых в системе;

- повышения эффективности традиционных, внедрения новых и разработки перспективных мер, способов и технологий распознавания угроз и др.

Особенностью совершенствования систем распознавания угроз информационной безопасности по рассмотренным направлениям является то, что некорректная постановка или игнорирование какого-либо из направлений полностью или в значительной степени снизит эффективность остальных. Это требует принятия единой системы принципов синтеза систем распознавания угроз нарушения информационной безопасности информационных ресурсов на объекте информатизации. К таким принципам следует отнести:

- принцип системного подхода, обеспечивающего учет использования всего комплекса способов, средств, методов, мероприятий по распознаванию такого рода угроз и учитывающего требования по обнаружению угроз при построении систем защиты информации;

- принцип максимальной эффективности, учитывающей максимальный выигрыш качества распознавания к стоимости системы или затратам ресурса;

- принцип централизации и управляемости процесса распознавания, при которых управление системой распознавания угроз нарушения информационной безопасности информационных ресурсов должно быть сосредоточено в соответствующей подсистеме;

- принцип непрерывности, предполагающей обеспечение процесса распознавания угроз на всех этапах жизненного цикла систем обработки информации;

- принцип дифференцированности применяемых способов распознавания, отражающих различные стратегии противоправных действий в отношении информационных ресурсов ИКС;

- принцип модульности, заключающейся в дискретности структуры процесса распознавания, обеспечивающей гибкое формирование из унифицированных модулей, узлов, блоков системы защиты распознавания;

- принцип динамичности, позволяющей гибко изменять и дополнять принятые в системе способы распознавания.

Рассмотренные принципы имеют конкретное содержание и могут быть положены в основу разработки методологии синтеза систем распознавания угроз нарушения информационной безопасности информационных ресурсов на объекте информатизации.

Реализованный на основе данных принципов механизм распознавания реализует многоуровневую аналитическую структуру, нижний уровень которой представляется первичными признаками, получаемыми в результате контроля информационного пространства сегмента ИКС, а остальные – в процессе аналитической обработки признаков распознавания. При этом правила формирования иерархических уровней такого механизма являются, в определенной степени, стандартными для иерархических систем [5], а именно, признаки, полученные в результате обработки нижнего уровня структуры являются исходными данными для формирования признаков последующих уровней. Верхний уровень такой структуры формирует результирующий признак, позволяющий оценить степень угрозы информационной безопасности информационных ресурсов территориального сегмента ИМТС.

3. Функциональное моделирование распознавания угроз нарушения информационной безопасности на объекте информатизации

3.1. Моделирование как методологическая основа оптимального синтеза систем распознавания угроз информационной безопасности на объекте информатизации

Система распознавания угроз нарушения информационной безопасности информационных ресурсов на объекте информатизации является важнейшей компонентой ее системы защиты информации (СЗИ), что приводит к необходимости использования одних и тех же закономерностей при создании такого рода систем.

Модели такой системы можно построить путем изучения общей картины информационной деятельности и исследованием содержания внутренних связей во внешней по отношению к защищенной информационной системе среде. В этих целях возможно использование известных структурных методологий [6].

Структурным анализом принято называть метод исследования системы, который начинается с ее общего обзора и затем детализируется, приобретая иерархическую структуру со все большим числом уровней [6]. В настоящее время преобладают структурные методологии, основанные на системном анализе объекта исследования. Структурирование по отношению к формальным методам описания архитектуры сложных систем и процессов их функционирования является методологией, которая позволяет понизить сложность описания.

Вместе с тем формальные методы структурирования, которые уже достаточно хорошо разработаны для формализованных структур, для таких трудно формализуемых процессов, как угрозы информационной безопасности информационных ресурсов ИКС, как правило имеют эвристическую форму.

Принимая во внимание целевую направленность угроз информационной безопасности информационных ресурсов на объекте информатизации, при их исследовании структурными методами структуризации подлежит предметная целевая функция. Это приводит к необходимости выделять функционально специализированные элементы. При этом специфицируемые в результате структуризации функции и логические связи исследуемой системы формируют описание ее функциональной структуры, что, в свою очередь, является функциональной моделью данной системы.

Следует заметить, что в процессе декомпозиции описания компонентов моделируемой системы, в случае представления ее функционирования в терминах «вход-выход», появляется ряд новых (внутренних) переменных, необходимых не только для реализации функций этих компонентов, но и для выражения основной функции системы. Формируемый в результате список допустимых функциональных компонентов, в терминах которого может в результате декомпозиции представляться структура исследуемой системы, представляет собой ее структурный базис.

Структурированное описание угроз информационной безопасности информационных ресурсов на объекте информатизации в интересах их распознавания должно обеспечивать:

- полноту и адекватность отображения всех существенных элементов и атрибутов таких действий и их взаимосвязей;

- возможность воспроизведения в процессе моделирования всех значимых характеристик противоправных действий;

- унифицированность описания структуры и взаимосвязей между элементами на любом уровне ее детализации;

- гибкость, позволяющую объединять элементы в структуры и заменять эти элементы и их совокупности.

Функциональная модель представляет собой описание с требуемой степенью подробности системы выполняемых предметных функций и отражает

процедурные знания об исследуемом объекте.

Информационная модель представляет собой подробное описание информационных потоков в исследуемом объекте и отражает декларативные знания о нем.

Приемлемым вариантом функциональной декомпозиции целевой функции угроз информационной безопасности информационных ресурсов на объекте информатизации является тот уровень ее детализации, при котором в описании порядка выполнения определенных функций появляются альтернативы. Это является показателем приемлемого уровня детализации исследуемого процесса и возможности перехода к методам математического формализма в его описании.

3.2. Функциональная модель распознавания угроз информационной безопасности на объекте информатизации

В результате анализа элементов множества $\{Y\}$ закономерностей возникновения угроз их трансформации в угрозу информационной безопасности информационных ресурсов ИКС установлено, что подобного рода воздействия реализуются в рамках определенных стратегий. Такая стратегия реализуется в рамках следующих этапов противоправных действий:

$f_1^{(1)}$ – физический доступ;

$f_2^{(1)}$ – вскрытие механизмов защиты информации;

$f_3^{(1)}$ – внедрение ложного доверенного объекта доступа;

$f_4^{(1)}$ – контроль над проходящим информационным потоком;

$f_5^{(1)}$ – несанкционированное воздействие на информацию;

$f_6^{(1)}$ – создание условий для последующего легального доступа.

Рассмотренные функциональные модели декомпозиции описания угрозы информационной безопасности информационных ресурсов на объекте информатизации служат основой для формирования набора первичных

признаков их распознавания.

Каждый из первичных признаков распознавания $\alpha_i^{(V)}$ из их множества $A^{(V)}$:

$$A^{(V)} = \{\alpha_i^{(V)}\},\ i = 1, 2, \ldots, |\{\alpha_i^{(V)}\}| \qquad (3.3.1)$$

в общем случае* описывается параметрическим списком вида

$$B_i(f^{(V)}_{l1,\, l2,\, l3,\, l4,\, l5}) = (\beta_{i,\,1}, \beta_{i,\,2}, \ldots, \beta_{i,\,j}, \ldots, \beta_{i,\,Ji}),$$

где $\beta_{i,\,j}$ – j - й параметр (список параметров) первичного признака $\alpha_i^{(VI)}$;

J_i – число параметров, описывающих признак $\alpha_i^{(VI)}$;

$f^{(V)}_{l1,\ l2,\ l3,\ l4,\ l5}$ – соответствующая первичному признаку $\alpha_i^{(VI)}$ идентифицируемая функция угрозы;

$l1, l2, l3, l4, l5$ – индекс идентифицируемой функции, характеризующий ее структурную взаимосвязь со вторичными функциями.

Параметры первичных признаков распознавания угрозы информационной безопасности информационных ресурсов на объекте информатизации могут быть представлены в качественном или количественном виде.

Качественные признаки представляют собой суждения качественного характера. Качественные признаки подразделяются на логические и лингвистические.

Логические признаки угроз можно рассматривать как элементарные высказывания, принимающие два значения истинности вида «истина» или «ложь» с полной определённостью.

Лингвистические признаки рассматриваются как элементарные высказывания, принимающие одно из нескольких лингвистических значений, характеризующих качество распознаваемого объекта.

Количественные признаки – это признаки, имеющие количественное выражение. Количественные признаки подразделяются на детерминированные и вероятностные.

Детерминированные признаки – признаки, количественная величина

* В частном случае признак $\alpha_i^{(V)}$ описывается одним параметром $B_i(f^{(V)}_{l1,\, l2,\, l3,\, l4,\, l5})$.

которых носит детерминированный характер.

Вероятностные (статистические) признаки – признаки, случайные значения которых распределены по различным классам угроз. При этом решение о принадлежности распознаваемого проявления угроз к тому или иному их классу может приниматься только на основании конкретных значений признаков данного проявления, определенного в результате проведения соответствующих мероприятий мониторинга информационного пространства сегмента ИМТС.

Для привязки к топологии системы вводится *идентифицирующий список* следующего вида:

$$\vec{\beta}_{i,j} = \left(\gamma_{i,j,1}, \delta_{i,j,1}, \gamma_{i,j,2}, \delta_{i,j,2}, ..., \gamma_{i,j,k}, \delta_{i,j,k}, ..., \gamma_{i,j,K}, \delta_{i,j,K}\right), \quad (3.3.2)$$

где $\gamma_{i,\,j,\,k}$ – идентификатор элемента топологии сегмента, представляемая в лингвистической форме;

$\delta_{i,\,j,\,k}$ – характеристика вскрытия сегмента по данному элементу, представляемая в вероятностной форме.

Например, $\gamma_{i,\,j,\,k}$ = «маршрутизатор №12577», $\delta_{i,\,j,\,k}$ = 0.8.

Для привязки к персоналу системы вводится *информативный список* следующего вида:

$$\vec{\beta}_{i,j} = \left(\varepsilon_{i,j,1}, \gamma_{i,j,1}, \delta_{i,j,1}, \varepsilon_{i,j,2}, \gamma_{i,j,2}, \delta_{i,j,2}, ..., \varepsilon_{i,j,k}, \gamma_{i,j,k}, \delta_{i,j,k}, ..., \varepsilon_{i,j,K}, \gamma_{i,j,K}, \delta_{i,j,K}\right), \quad (3.3.3)$$

где $\varepsilon_{i,\,j,\,k}$ – идентификационная характеристика сотрудника сегмента, представляемая в лингвистической форме;

$\gamma_{i,\,j,\,k}$ – идентификатор элемента топологии сегмента, представляемый в лингвистической форме;

$\delta_{i,\,j,\,k}$ – характеристика вскрытия сегмента по данному элементу, представляемая в вероятностной форме.

Например, $\varepsilon_{i,\,j,\,k}$ =«СисАдмин Иванов И. И.», $\gamma_{i,\,j,\,k}$ = «Сервер №3», $\delta_{i,\,j,\,k}$ = 0.95.

Вышеприведенные списки являются по сути реализацией так называемых

«векторов» (массивов переменной длинны) и могут быть реализованы в формате ключевых и информационных полей таблиц систем управления базами данных (СУБД).

В анализируемом сегменте ИКС примем информацию о топологии сегмента и информацию о персонале как условно неизменный набор данных ввиду того, что по сравнению с параметрами распознавания угрозы конфиденциальности информации скорость изменения этих данных значительно ниже. На основании этого представим элементы списков (3.3.2) и (3.3.3) $\varepsilon_{i,\,j,\,k}$ и $\gamma_{i,\,j,\,k}$ в качестве системы координат для определения элемента сегмента ИКС. Это позволяет считать данные элементы списка лингвистическими координатами элемента $\delta_{i,\,j,\,k}$, а элемент $\delta_{i,\,j,\,k}$ – значимым элементом параметра $\beta_{i,\,j}$ в представленных списках. Тогда (3.3.2) можно считать идентификационным списком, а (3.3.3) – информативным списком по типу значимого элемента.

Практическая реализация предложенных как списков $\varepsilon_{i,\,j,\,k}$ и $\gamma_{i,\,j,\,k}$, так их отображений при использовании в параметрах $\beta_{i,\,j}$ в рамках использования современных СУБД не представляет сложности и является элементарной задачей.

Ниже приводится сформированное в соответствии с (3.3.1) – (3.3.3) описание набора первичных признаков распознавания угроз безопасности информационных ресурсов ИКС объекта информатизации.

Сбор общедоступных сведений о ИКС в средствах массовой информации

Первичный признак распознавания $\alpha_1^{(V)}$, соответствующий функции сбора общедоступных сведений о ИКС ОВД в средствах массовой информации, описывается параметрическим списком вида:

$$B_1(f^{(V)}_{1,\,1,\,1,\,1,\,1}) = (\beta_{1,\,1}, \beta_{1,\,2}).$$

Элементами этого списка являются логические параметры, характеризующие возможность получения злоумышленником сведений о ИКС:

за счет контакта злоумышленника через официальную контактную линию – $\beta_{1,\,1}$;

путем анализа сведений о топологии сегмента, попавших в средства массовой информации – $\beta_{1,2}$.

При этом параметр $\beta_{1,1}$ является логическим, а параметр $\beta_{1,2}$ – идентифицирующим списком вида (3.3.2).

Сбор общедоступных сведений о ИКС из ресурсов сети Internet

Первичный признак распознавания $\alpha_2^{(V)}$, соответствующий функции сбора общедоступных сведений о ИКС ОВД из ресурсов сети Internet, описывается параметрическим списком вида:

$$B_2(f^{(V)}_{1,1,1,1,2}) = (\beta_{2,1}, \beta_{2,2}, \beta_{2,3}, \beta_{2,4}).$$

Элементами этого списка являются логические параметры, характеризующие возможность получения злоумышленником сведений о ИКС:

путем анализа сведений о системе, попавших в официальные Internet-ресурсы – $\beta_{2,1}$;

за счет контакта злоумышленника через электронную почту – $\beta_{2,2}$;

за счет контакта злоумышленника через Internet-пейджеры (например, ICQ, Windows Messenger и др.) – $\beta_{2,3}$;

за счет контакта злоумышленника через социальные сети (например, «Одноклассники», «ВКонтакте» и др.) – $\beta_{2,4}$.

При этом параметр $\beta_{2,1}$ является логическим идентифицирующим списком вида (3.3.2), а параметры $\beta_{2,2}$, $\beta_{2,3}$, $\beta_{2,4}$ – логическими информативными списками.

Сбор сведений из материалов приглашений к сотрудничеству

Первичный признак распознавания $\alpha_3^{(V)}$, соответствующий возможности получения злоумышленником сведений о ИКС из материалов приглашений к сотрудничеству, описывается параметром:

$$B_3(f^{(V)}_{1,1,1,3,1}) = \beta_{3,1},$$

характеризующим возможность получения злоумышленником сведений о ИКС путем анализа такого рода информации.

Параметр $\beta_{3,1}$ является вероятностным.

Сбор сведений о взаимодействующих организациях

Первичный признак распознавания $\alpha_4^{(V)}$, соответствующий возможности получения злоумышленником сведений об организациях, сотрудничающих с сегментом ИКС, описывается параметрами:

$$B_4(f^{(V)}_{1,1,1,4,1}) = (\beta_{4,1}, \beta_{4,2}, \beta_{4,3}),$$

характеризующими возможность получения злоумышленником сведений о сегменте ИКС путем анализа информации о взаимодействующих (смежных) организациях:

за счет контакта злоумышленника через официальную контактную линию смежной организации – $\beta_{4,1}$;

путем анализа сведений о смежной организации, попавших в официальные Internet-ресурсы – $\beta_{4,2}$;

за счет контакта злоумышленника через электронную почту, Internet-пейджеры, социальные сети с персоналом смежной организации – $\beta_{4,3}$.

При этом параметр $\beta_{4,1}$ является логическим идентифицирующим списком вида (3.3.2), а параметры $\beta_{4,2}$, $\beta_{4,3}$ – логическими информативными списками.

Сбор сведений с помощью физического наблюдения

Первичный признак распознавания $\alpha_5^{(V)}$, соответствующий возможности получения злоумышленником сведений о сегменте ИКС, описывается параметрами:

$$B_5(f^{(V)}_{1,1,2,1,1}) = (\beta_{5,1}, \beta_{5,2}),$$

характеризующими возможность получения злоумышленником таких сведений путем наблюдения:

за персоналом сегмента ИКС – $\beta_{5,1}$;

за его топологией – $\beta_{5,2}$.

Здесь параметр $\beta_{5,1}$ является вероятностным информативным списком, а параметр $\beta_{5,2}$ – вероятностным идентифицирующим списком.

Сбор сведений с помощью оперативного воздействия на персонал

Первичный признак распознавания $\alpha_6^{(V)}$, соответствующий возможности получения злоумышленником сведений о сегменте ИКС, описывается параметрами:

$$B_6(f^{(V)}_{1,1,2,2,1}) = (\beta_{6,1}, \beta_{6,2}),$$

характеризующими возможность получения злоумышленником таких сведений путем:

вовлечения персонала сегмента ИКС в различные сторонние организации – $\beta_{6,1}$;

воздействия на персонал сегмента ИКС с помощью личных контактов – $\beta_{6,2}$.

Параметры $\beta_{6,1}$ и $\beta_{6,2}$ являются логическими информативными списками.

Подкуп ответственного сотрудника

Первичный признак распознавания $\alpha_7^{(V)}$, соответствующий возможности получения злоумышленником предпосылок к физическому доступу к элементам сегмента ИКС, описывается параметром:

$$B_7(f^{(V)}{}_{1,2,1,1,1}) = \beta_{7,1},$$

характеризующим возможность получения злоумышленником доступа в результате подкупа ответственного сотрудника сегмента ИКС. Это вероятностный информативный список.

Принуждение (шантаж) ответственного сотрудника

Первичный признак распознавания $\alpha_8^{(V)}$, соответствующий возможности получения злоумышленником предпосылок к физическому доступу к элементам сегмента ИКС, описывается параметрами:

$$B_8(f^{(V)}{}_{1,2,1,2,1}) = (\beta_{8,1}, \beta_{8,2}),$$

характеризующими возможность получения злоумышленником доступа в результате:

использования компрометирующих сотрудника материалов – $\beta_{8,1}$;

использования угрозы физического воздействия (в том числе по отношению к близким) – $\beta_{8,2}$.

Аналогично параметры $\beta_{8,1}$ и $\beta_{8,2}$ являются вероятностными информативными списками.

Изучение возможности доступа к каналам связи ИКС ОВД вне помещений этой системы

Первичный признак распознавания $\alpha_9^{(V)}$, соответствующий возможности получения злоумышленником предпосылок к физическому доступу к элементам сегмента ИКС, описывается параметром:

$$B_9(f^{(V)}{}_{1,2,2,1,1}) = \beta_{9,1},$$

характеризующим возможность получения злоумышленником доступа к каналам связи сегмента ИКС вне контролируемых зон, а именно наличием линий связи вне контролируемых помещений.

Параметр $\beta_{9,1}$ является логическим идентифицирующим списком.

Изучение возможности доступа к каналам связи сегмента ИКС внутри помещений этой системы

Первичный признак распознавания $\alpha_{10}^{(V)}$, соответствующий возможности

получения злоумышленником предпосылок к физическому доступу к элементам сегмента ИКС, описывается параметрами:

$$B_{10}(f^{(V)}{}_{1,2,2,2,1}) = (\beta_{10,1}, \beta_{10,2}, \beta_{10,3}).$$

характеризующими возможность получения злоумышленником доступа к каналам связи сегмента ИКС внутри контролируемых помещений, а именно:

наличие свободных точек доступа – $\beta_{10,1}$, $\beta_{10,2}$;

наличие неконтролируемых концентраторов и(или) маршрутизаторов сегмента ИКС – $\beta_{10,3}$.

Параметры $\beta_{10,1}$, $\beta_{10,2}$, $\beta_{10,3}$, являются логическими идентифицирующими списками.

Регистрация пользователя

Первичный признак распознавания $\alpha_{11}^{(V)}$, соответствующий возможности получения злоумышленником учетной записи пользователя сегмента ИКС, описывается параметрами:

$$B_{11}(f^{(V)}{}_{1,2,3,1,1}) = (\beta_{11,1}, \beta_{11,2}),$$

характеризующими возможность получения злоумышленником доступа к сегменту ИКС в качестве пользователя, а именно:

возможность получения «гостевого» доступа – $\beta_{11,1}$;

получение учетных данных пользователя сегмента ИКС (в том числе неполных) – $\beta_{11,2}$.

Здесь параметр $\beta_{11,1}$ является логическим, а параметр $\beta_{11,2}$ – вероятностным.

Получение пользовательских данных для удаленного доступа

Первичный признак распознавания $\alpha_{12}^{(V)}$, соответствующий возможности получения злоумышленником учетной записи пользователя сегмента ИКС, описывается параметрами:

$$B_{12}(f^{(V)}{}_{1,2,3,2,1}) = (\beta_{12,1}, \beta_{12,2}),$$

характеризующими возможность получения злоумышленником доступа к сегменту ИКС в качестве пользователя, а именно:

возможность осуществления удаленного доступа – $\beta_{12,1}$;

актуализация учетных данных пользователя сегмента ИКС – $\beta_{12,2}$.

При этом параметр $\beta_{12,1}$, является логическим, а параметр $\beta_{12,2}$ вероятностным.

Открытое сканирование портов

Первичный признак распознавания $\alpha_{13}^{(V)}$, соответствующий возможности получения злоумышленником информации о сетевых портах, применяемых в сегменте ИКС, и описывается параметрами:

$$B_{13}(f^{(V)}{}_{1,3,1,1,1}) = (\beta_{13,1}, \beta_{13,2}, \beta_{13,3}, \beta_{13,4}),$$

характеризующими возможность получения злоумышленником информации различными способами, а именно:

осуществление посылки TCP SYN-запросов на создание соединения на различные порты – $\beta_{13,1}$;

реализация особенности протокола TCP в различных сетевых ОС (за исключением ОС Microsoft): на передаваемый TCP FIN-запрос закрытые порты отвечают пакетом с флагом RST, а открытые порты данное сообщение игнорируют – $\beta_{13,2}$;

используя разбиение TCP SYN- или TCP FIN-запроса на несколько маленьких IP-фрагментов для сканирования портов элемента системы – $\beta_{13,3}$;

для UNIX-систем с использованием TAP IDENT сервиса запрос на 113-й порт, задача которого заключается в предоставлении удаленным пользователям информации о существующих на сервере в данный момент соединениях – $\beta_{13,4}$.

Параметры $\beta_{13,1}$, $\beta_{13,2}$, $\beta_{13,3}$, $\beta_{13,4}$ являются логическими идентифицирующими списками.

Анонимное сканирование портов

Первичный признак распознавания $\alpha_{14}^{(V)}$, соответствующий возможности получения злоумышленником информации о сетевых портах, применяемых в сегменте ИКС, описывается параметрами:

$$B_{14}(f^{(V)}{}_{1,3,1,2,1}) = (\beta_{14,1}, \beta_{14,2}, \beta_{14,3}),$$

характеризующими возможность получения злоумышленником информации различными способами сканирования портов, а именно:

путем скрытой атаки по FTP для– $\beta_{14,1}$;

путем использования метода Dumb host scan – $\beta_{14,2}$;

с использованием промежуточного хоста (или цепочки хостов) – $\beta_{14,3}$.

Параметры $\beta_{14,1}$, $\beta_{14,2}$, $\beta_{14,3}$ являются логическими идентифицирующими списками.

Анализ служб использующихся абонентами распределенной вычислительной сети объекта информатизации

Первичный признак распознавания $\alpha_{15}^{(V)}$, соответствующий возможности

анализа злоумышленником служб абонентов сегмента ИКС, описывается параметрами:

$$B_{15}(f^{(V)}{}_{1,3,2,1,1}) = (\beta_{15,1}, \beta_{15,2}),$$

характеризующими возможность получения злоумышленником информации о службах сегмента ИКС, а именно:

информация о доступных службах – $\beta_{15,1}$;

информация о нестандартных службах сегмента ИКС – $\beta_{15,2}$.

Здесь параметры $\beta_{15,1}$ и $\beta_{15,2}$ являются лингвистическими идентифицирующими списками.

Анализ служб, использующихся на серверах сегмента ИКС

Первичный признак распознавания $\alpha_{16}^{(V)}$, соответствующий возможности анализа злоумышленником служб серверов сегмента ИКС, описывается параметрами:

$$B_{16}(f^{(V)}{}_{1,3,2,2,1}) = (\beta_{16,1}, \beta_{16,2}),$$

характеризующими возможность получения злоумышленником информации о службах сегмента ИКС, а именно:

получение информации о доступных сервисах – $\beta_{16,1}$;

получение отказа в обслуживании сервиса – $\beta_{16,2}$.

Параметры $\beta_{16,1}$, $\beta_{16,2}$ являются лингвистическими идентифицирующими списками.

Проникновение в помещения сегмента ИКС

Первичный признак распознавания $\alpha_{17}^{(V)}$, соответствующий факту проникновения злоумышленника в помещение с элементами сегмента ИКС, описывается параметрами:

$$B_{17}(f^{(V)}{}_{2,1,1,1,1}) = (\beta_{17,1}, \beta_{17,2}),$$

характеризующими критичность проникновения к элементам сегмента ИКС, а именно:

проникновение к каналам связи сегмента ИКС – $\beta_{17,1}$;

проникновение к узлам, маршрутизаторам, серверам сегмента ИКС – $\beta_{17,2}$.

Все параметры описывает логический идентифицирующий список.

Внедрение закладки в канал связи сегмента ИКС

Первичный признак распознавания $\alpha_{18}^{(V)}$ соответствует возможности внедрения злоумышленником закладки в канал связи сегмента ИКС и

описывается параметрами:

$$B_{18}(f^{(V)}{}_{2,1,2,1,1}) = (\beta_{18,1}, \beta_{18,2}),$$

характеризующими возможность получения злоумышленником информации из канала связи сегмента ИКС, а именно:

внедрение закладки в проводной канал связи – $\beta_{18,1}$;

внедрение закладки в беспроводной канал связи – $\beta_{18,2}$.

Все параметры описывает логический идентифицирующий список.

Внедрение закладки в маршрутизатор, роутер, сервер сегмента ИКС

Первичный признак распознавания $\alpha_{19}^{(V)}$ соответствует возможности внедрения злоумышленником закладки в узел связи сегмента ИКС и описывается параметрами:

$$B_{19}(f^{(V)}{}_{2,1,2,2,1}) = (\beta_{19,1}, \beta_{19,2}),$$

характеризующими возможность получения злоумышленником информации из узла сегмента ИКС, а именно:

внедрение закладки в маршрутизатор (роутер) – $\beta_{19,1}$;

внедрение закладки в сервер сегмента ИКС – $\beta_{19,2}$.

Все параметры описывает логический идентифицирующий список.

Получение удаленного доступа внутри сегмента ИКС

Первичный признак распознавания $\alpha_{20}^{(V)}$ соответствует возможности получения удаленного доступа злоумышленником внутри сегменте ИКС и описывается параметрами:

$$B_{20}(f^{(V)}{}_{2,1,3,1,1}) = (\beta_{20,1}, \beta_{20,2}),$$

характеризующими возможность получения злоумышленником информации из узла сегмента ИКС, а именно:

получение доступа к точке доступа сегмента ИКС – $\beta_{20,1}$;

получение доступа к службам сегмента ИКС – $\beta_{21,2}$.

Все параметры – логические информативные списки.

Получение удаленного доступа из вне сегмента ИКС

Первичный признак распознавания $\alpha_{21}^{(V)}$, соответствующий возможности получения удаленного доступа злоумышленником извне сегмента ИКС, описывается параметрами:

$$B_{21}(f^{(V)}{}_{2,1,3,2,1}) = (\beta_{21,1}, \beta_{21,2}),$$

характеризующими возможность получения злоумышленником информации из узла сегмента ИКС, а именно:

получение удаленного доступа к точке входа в сегмент ИКС – $\beta_{21,1}$;

получение удаленного доступа к службам сегмента ИКС – $\beta_{21,2}$.

Все параметры – логические информативные списки.

Преодоление автономной охраны

Первичный признак распознавания $\alpha_{22}^{(V)}$, соответствующий факту преодоления злоумышленником системы охраны сегмента ИКС, описывается параметром:

$$B_{22}(f^{(V)}{}_{2,2,1,1,1}) = \beta_{22,1},$$

характеризующим наличие проникновения злоумышленника через систему охраны сегмента ИКС. Параметр логический.

Преодоление физической охраны

Первичный признак распознавания $\alpha_{23}^{(V)}$, соответствующий факту преодоления злоумышленником средств физической охраны сегмента ИКС, описывается параметром:

$$B_{23}(f^{(V)}{}_{2,2,1,2,1}) = \beta_{23,1},$$

характеризующим наличие проникновения злоумышленника через систему физической охраны сегмента ИКС. Параметр логический.

Преодоление инженерных преград

Первичный признак распознавания $\alpha_{24}^{(V)}$, соответствующий факту преодоления злоумышленником инженерных сооружений сегмента ИКС, описывается параметрами:

$$B_{24}(f^{(V)}{}_{2,2,2,1,1}) = (\beta_{24,1}, \beta_{24,2}),$$

характеризующими нарушение инженерных преград воздействием, а именно:

преодоление периметральных заграждений – $\beta_{24,1}$.

преодоление инженерных преград между различными элементами сегмента ИКС – $\beta_{24,2}$.

Параметры логические.

Съем информации с клавиатуры точки доступа сегмента ИКС

Первичный признак распознавания $\alpha_{25}^{(V)}$, соответствующий факту наличия программных средств съема информации с клавиатуры точки доступа сегмента ИКС, описывается параметром

$$B_{25}(f^{(V)}{}_{2,3,1,1,1}) = \beta_{25,1},$$

характеризующим данный факт. Параметр – логический идентифицирующий список.

Съем информации с экрана точки доступа сегмента ИКС

Первичный признак распознавания $\alpha_{26}^{(V)}$, соответствующий факту наличия устройств для съема информации с экрана точки доступа сегмента ИКС, описывается параметрами:

$$B_{26}(f^{(V)}_{2,3,1,1,2}) = (\beta_{26,1}, \beta_{26,2}),$$

характеризующими такие факты, а именно:

съем информации оптическим способом – $\beta_{26,1}$;

съем сигнала кабеля экрана – $\beta_{26,2}$.

Все параметры – логические идентифицирующие списки.

Съем информации с сетевых устройств сегмента ИКС

Первичный признак распознавания $\alpha_{27}^{(V)}$, соответствующий факту наличия устройств для съема информации с сетевого устройства сегмента ИКС, описывается параметрами:

$$B_{27}(f^{(V)}_{2,3,1,1,3}) = (\beta_{27,1}, \beta_{27,2}, \beta_{27,3}, \beta_{27,4}),$$

характеризующими такие факты, а именно:

съем информации с линии связи – $\beta_{27,1}$;

съем информации с маршрутизатора (роутера) сети – $\beta_{27,2}$;

съем информации с точки доступа сети – $\beta_{27,3}$;

съем информации с сервера сети – $\beta_{27,4}$.

Параметры описываются логическим идентифицирующим списком.

Внедрение сетевых червей

Первичный признак распознавания $\alpha_{28}^{(V)}$, соответствующий факту внедрения сетевого червя в сегмент ИКС, описывается параметром:

$$B_{28}(f^{(V)}_{2,3,1,2,1}) = \beta_{28,1},$$

характеризующим такие факты. Параметр – логический идентифицирующий список.

Внедрение троянских программ

Первичный признак распознавания $\alpha_{29}^{(V)}$, соответствующий факту внедрения троянской программы в сегмент ИКС, описывается параметром:

$$B_{29}(f^{(V)}_{2,3,1,2,2}) = \beta_{29,1},$$

характеризующим такие факты. Параметр – логический идентифицирующий список.

Внедрение программ, использующих уязвимость системы

Первичный признак распознавания $\alpha_{30}^{(V)}$, соответствующий факту применения программы, использующей уязвимость в сегменте ИКС, описывается параметрами:

$$B_{30}(f^{(V)}{}_{2,3,1,2,3}) = (\beta_{30,1}, \beta_{30,2}, \beta_{30,3}),$$

характеризующими такие факты, а именно:

программы инициирующие уязвимости механизмов защиты, аутентификации и идентификации – $\beta_{30,1}$;

программы инициирующие уязвимости файлового (информационного) обмена – $\beta_{30,2}$;

программы инициирующие уязвимости систем управления базами данных – $\beta_{30,3}$.

Все параметры – логический идентифицирующий список.

Внедрение программ, использующихся для скачивания информации (downloader)

Первичный признак распознавания $\alpha_{31}^{(V)}$, соответствующий факту использования программы для закачивания информации в сегмент ИКС, описывается параметрами:

$$B_{31}(f^{(V)}{}_{2,3,1,3,1}) = (\beta_{31,1}, \beta_{31,2}, \beta_{31,3}),$$

характеризующими:

увеличение внешнего трафика системы без объективных предпосылок – $\beta_{31,1}$;

наличие в системе нестандартных (для системы) запросов на передачу информации – $\beta_{31,2}$;

факт обнаружения подобной программы – $\beta_{31,3}$.

Здесь параметр $\beta_{31,1}$ является количественным идентифицирующим списком, а параметры $\beta_{31,2}$, $\beta_{31,3}$ –логическими идентифицирующими списками.

Внедрение программ использующих возможность получения привилегированных полномочий (rootkit)

Первичный признак распознавания $\alpha_{32}^{(V)}$, соответствующий факту использования программ-rootkit для получения привилегированного доступа к ресурсам в сегменте ИКС, описывается параметрами:

$$B_{32}(f^{(V)}{}_{2,3,1,3,2}) = (\beta_{32,1}, \beta_{32,2}).$$

характеризующими:

манипуляции с точки доступа системы с превышением выданных

полномочий – $\beta_{32,1}$; параметр – логический идентифицирующий список;

факт обнаружения программы повышения полномочий пользователя – $\beta_{31,2}$. параметр – логический информативный список.

Внедрение программ, использующих недокументированные возможности (backdoor)

Первичный признак распознавания $\alpha_{33}^{(V)}$, соответствующий факту, использования программ-backdoor для получения доступа к ресурсам в сегменте ИКС, описывается параметром:

$$B_{33}(f^{(V)}{}_{2,3,1,3,3}) = \beta_{33,1},$$

характеризующим факт обнаружения подобных программ. Параметр – логический идентифицирующий список.

Внедрение вирусных программ

Первичный признак распознавания $\alpha_{34}^{(V)}$, соответствующий факту внедрения в сегмент ИКС вирусных программ , описывается параметром:

$$B_{34}(f^{(V)}{}_{2,3,1,4,1}) = \beta_{33,1},$$

характеризующим факт обнаружения подобных программ. Параметр – логический идентифицирующий список.

Внедрение программ преодоления криптографической защиты

Первичный признак распознавания $\alpha_{35}^{(V)}$, соответствующий факту использования программ преодоления криптографической защиты в сегменте ИКС, описывается параметрами:

$$B_{35}(f^{(V)}{}_{2,3,1,4,2}) = (\beta_{35,1}, \beta_{35,2}),$$

характеризующими:

преодоление путем перебора вариантов пароля – $\beta_{35,1}$;

преодоление путем изменения функционирования сегмента – $\beta_{35,2}$.

Все параметры – логические идентифицирующие списки.

Установка системного программного обеспечения

Первичный признак распознавания $\alpha_{36}^{(V)}$, соответствующий факту установки системного программного обеспечения (ПО) в сегменте ИКС, описывается параметрами:

$$B_{36}(f^{(V)}{}_{2,3,2,1,1}) = (\beta_{36,1}, \beta_{36,2}),$$

характеризующими:

установку нового системного ПО – $\beta_{36,1}$;

замену существующего системного ПО (в том числе без изменения

версии ПО) – $\beta_{36,\,2}$.

Все параметры – логические идентифицирующие списки.

Модификация транспортного программного обеспечения

Первичный признак распознавания $\alpha_{37}^{(V)}$, соответствующий модификации транспортного программного обеспечения в сегменте ИКС, описывается параметрами:

$$B_{37}(f^{(V)}{}_{2,\,3,\,2,\,2,\,1}) = (\beta_{37,\,1}, \beta_{37,\,2}),$$

характеризующими:

установку нового транспортного ПО – $\beta_{37,\,1}$;

подмену существующего транспортного ПО (в том числе изменение параметров подобного ПО) – $\beta_{37,\,2}$;

Все параметры – логические идентифицирующие списки.

Установка прикладного программного обеспечения

Первичный признак распознавания $\alpha_{38}^{(V)}$, соответствующий установке транспортного программного обеспечения в сегменте ИКС, описывается параметрами:

$$B_{38}(f^{(V)}{}_{2,\,3,\,2,\,3,\,1}) = (\beta_{38,\,1}, \beta_{38,\,2}),$$

характеризующими:

установку нового прикладного ПО (в том числе скрытую от пользователя сегмента ИКС) – $\beta_{38,\,1}$;

подмену существующего прикладного ПО – $\beta_{38,\,2}$;

Все параметры – логические идентифицирующие списки.

Иные изменения программной среды

Первичный признак распознавания $\alpha_{39}^{(V)}$, соответствующий изменениям в программном обеспечении сегмента ИКС, описывается параметром:

$$B_{39}(f^{(V)}{}_{2,\,3,\,3,\,1,\,1}) = \beta_{39,\,1},$$

характеризующим факты подобного изменения. Данный признак используется для оценки изменений и дополнений программной среды в сегменте ИКС, не подходящей под признаки $\alpha_{26}^{(V)}$ - $\alpha_{38}^{(V)}$. Параметр – логический идентифицирующий список.

Внедрение закладки в канал связи сегмента ИКС

Первичный признак распознавания $\alpha_{40}^{(V)}$, соответствующий внедрению закладки в канал связи сегмента ИКС, описывается параметром:

$$B_{40}(f^{(V)}{}_{2,4,1,1,1}) = \beta_{40,1},$$

характеризующим факт обнаружения подобной закладки. Параметр – логический идентифицирующий список.

Нарушение работоспособности канала связи

Первичный признак распознавания $\alpha_{41}^{(V)}$, соответствующий нарушению работоспособности канала связи сегмента ИКС, описывается параметрами:

$$B_{41}(f^{(V)}{}_{2,4,1,2,1}) = (\beta_{41,1}, \beta_{41,2}),$$

характеризующими:

отказ работоспособности – $\beta_{41,1}$;

задержки при передаче данных – $\beta_{41,2}$;.

Все параметры – логические идентифицирующие списки.

Внедрение закладки в маршрутизатор сегмента ИКС

Первичный признак распознавания $\alpha_{42}^{(V)}$, соответствующий внедрению закладки в маршрутизатор сегмента ИКС, описывается параметром:

$$B_{42}(f^{(V)}{}_{2,4,2,1,1}) = \beta_{42,1},$$

характеризующим факт обнаружения подобной закладки. Параметр – логический идентифицирующий список.

Нарушение работоспособности маршрутизатора

Первичный признак распознавания $\alpha_{43}^{(V)}$, соответствующий нарушению работоспособности канала связи сегмента ИКС, описывается параметрами:

$$B_{43}(f^{(V)}{}_{2,4,2,0,2}) = (\beta_{43,1}, \beta_{43,2}, \beta_{43,3}),$$

характеризующими:

отказ работоспособности – $\beta_{43,1}$;

ошибки адресации пакетов – $\beta_{43,2}$;

изменение параметров ретрансляции пакетов – $\beta_{43,3}$.

Все параметры – логические идентифицирующие списки.

Внедрение закладки в сервер сегмента ИКС

Первичный признак распознавания $\alpha_{44}^{(V)}$, соответствующий внедрению закладки в сервер сегмента ИКС, описывается параметром:

$$B_{44}(f^{(V)}{}_{2,4,3,1,1}) = \beta_{44,1},$$

характеризующим факт обнаружения подобной закладки. Параметр – логический идентифицирующий список.

Нарушение работоспособности сервера

Первичный признак распознавания $\alpha_{45}^{(V)}$, соответствующий нарушению работоспособности сервера сегмента ИКС, описывается параметрами:

$$B_{45}(f^{(V)}{}_{2,4,3,2,1}) = (\beta_{45,1}, \beta_{45,2}, \beta_{45,3}),$$

характеризующим:

отказ работоспособности сервера – $\beta_{45,1}$;

отказ работоспособности служб сервера – $\beta_{45,2}$;

модификацию служб сервера – $\beta_{45,3}$.

Все параметры – логические идентифицирующие списки.

Внедрение закладки в абонентский пункт сегмента ИКС

Первичный признак распознавания $\alpha_{46}^{(V)}$, соответствующий внедрению закладки в абонентский пункт сегмента ИКС, описывается параметром:

$$B_{46}(f^{(V)}{}_{2,4,4,1,1}) = \beta_{46,1},$$

характеризующим факт обнаружения подобной закладки. Параметр – логический идентифицирующий список.

Нарушение работоспособности абонентского пункта

Первичный признак распознавания $\alpha_{47}^{(V)}$, соответствующий нарушению работоспособности абонентского пункта сегмента ИКС, описывается параметрами:

$$B_{47}(f^{(V)}{}_{2,4,4,2,1}) = (\beta_{47,1}, \beta_{47,2}).$$

характеризующими:

отключение абонентского пункта – $\beta_{47,1}$;

отказ службы абонентского пункта – $\beta_{47,2}$;

Все параметры – логические идентифицирующие списки.

Подмена абонентского пункта сегмента ИКС

Первичный признак распознавания $\alpha_{48}^{(V)}$, соответствующий подмене абонентского пункта сегмента ИМТС, описывается параметром:

$$B_{48}(f^{(V)}{}_{2,4,4,3,1}) = \beta_{48,1},$$

характеризующим факт обнаружения подобной подмены. Параметр – логический идентифицирующий список.

Атака на абонента сегмента ИКС перехватом запроса DNS

Первичный признак распознавания $\alpha_{49}^{(V)}$, соответствующий атаке на абонента сегмента ИКС перехватом запроса DNS, описывается параметрами:

$$B_{49}(f^{(V)}_{3,1,1,1,1}) = (\beta_{49,1}, \beta_{49,2}, \beta_{49,3}),$$

характеризующими:

перехват UDP пакета запроса службы DNS – $\beta_{49,1}$;

наличие «лишних» ответов службы DNS – $\beta_{49,2}$;

увеличение времени передачи информации от абонента к серверу – $\beta_{49,3}$.

Все параметры – логические идентифицирующие списки.

Атака на абонента сегмента ИКС «штормом» ложных сообщений DNS службы

Первичный признак распознавания $\alpha_{50}^{(V)}$, соответствующий атаке на абонента сегмента ИКС с помощью «шторма» ложных сообщений службы DNS, описывается параметром:

$$B_{50}(f^{(V)}_{3,1,1,1,2}) = \beta_{50,1},$$

характеризующим наличие сообщений службы DNS в канале связи с сервером. Параметр – логический идентифицирующий список.

Атака на DNS сервер сегмента ИКС перехватом запроса DNS

Первичный признак распознавания $\alpha_{51}^{(V)}$, соответствующий атаке на DNS сервер сегмента ИКС перехватом запроса DNS, описывается параметрами:

$$B_{51}(f^{(V)}_{3,1,1,1,1}) = (\beta_{51,1}, \beta_{51,2}, \beta_{51,3}),$$

характеризующими:

перехват UDP пакета запроса службы DNS – $\beta_{51,1}$; параметр – логический идентифицирующий список;

наличие «лишних» ответов службы DNS – $\beta_{51,2}$; параметр – логический идентифицирующий список;

увеличение времени передачи информации от сервера к абоненту – $\beta_{51,3}$; параметр – количественный идентифицирующий список.

Атака на DNS сервер сегмента ИКС «штормом» ложных сообщений DNS службы

Первичный признак распознавания $\alpha_{52}^{(V)}$, соответствующий атаке на абонента сегмента ИКС с помощью «шторма» ложных сообщений службы DNS, описывается параметром:

$$B_{52}(f^{(V)}_{3,1,1,2,2}) = \beta_{52,1},$$

характеризующим наличие дублирующихся сообщений службы DNS в канале связи с сервером. Параметр – логический идентифицирующий список.

Организация подмены ARP внутри сегмента ИКС

Первичный признак распознавания $\alpha_{53}^{(V)}$, соответствующий атаке на абонента сегмента ИКС с помощью организации подмены ARP сервиса, описывается параметрами:

$$B_{53}(f^{(V)}{}_{3,1,2,1,1}) = (\beta_{53,1}, \beta_{53,2}),$$

характеризующими наличие широковещательного запроса ARP на стороне абонента – $\beta_{53,1}$, и на стороне сервера – $\beta_{53,2}$.

Все параметры описываются логическим идентифицирующим списком.

Организация подмены сервера извне сегмента ИКС

Первичный признак распознавания $\alpha_{54}^{(V)}$, соответствующий атаке на абонента сегмента ИКС путем подмены сервера ARP сервиса из-за пределов сегмента, описывается параметром:

$$B_{54}(f^{(V)}{}_{3,1,2,2,1}) = \beta_{54,1},$$

характеризующим наличие широковещательного запроса ARP на стороне абонента извне пределов сегмента – $\beta_{54,1}$.

Параметр – логический идентифицирующий список.

Организация подмены абонентского пункта извне сегмента ИКС

Первичный признак распознавания $\alpha_{55}^{(V)}$, соответствующий атаке на абонента сегмента ИКС с помощью организации подмены абонента на сервере ARP сервиса из-за пределов сегмента, описывается параметром:

$$B_{55}(f^{(V)}{}_{3,1,2,2,2}) = \beta_{55,1},$$

характеризующим наличие широковещательного запроса ARP на стороне сервера извне пределов сегмента - $\beta_{55,1}$. Параметр логический идентифици-рующий список.

Использование IP сегмента как источник угроз

Первичный признак распознавания $\alpha_{56}^{(V)}$, соответствующий атаке на абонента сегмента ИМТС при использовании IP сегмента ИКС, описывается параметром:

$$B_{56}(f^{(V)}{}_{3,2,1,1,1}) = \beta_{56,1},$$

характеризующим наличие пакетов внутри сегмента от IP – $\beta_{56,1}$. Параметр – логический идентифицирующий список.

Смена маршрута(-ов) между хостами внутри сегмента

Первичный признак распознавания $\alpha_{57}^{(V)}$, соответствующий атаке на абонента сегмента ИКС при помощи смены маршрутов между абонентскими станциями внутри сегмента ИМТС, описывается параметром:

$$B_{57}(f^{(V)}_{3,\,2,\,1,\,1,\,2}) = \beta_{57,\,1},$$

характеризующим наличие такой смены – $\beta_{57,\,1}$. Параметр – логический идентифицирующий список.

Нарушение работоспособности сегмента ИКС

Первичный признак распознавания $\alpha_{58}^{(V)}$, соответствующий нарушению работоспособности сегмента ИКС, описывается параметрами:

$$B_{58}(f^{(V)}_{3,\,2,\,1,\,2,\,1}) = (\beta_{58,\,1}, \beta_{58,\,2}),$$

характеризующими:

отключение связи абонентских пунктов в сегменте – $\beta_{58,\,1}$;

отказ служб сегмента – $\beta_{58,\,2}$.

Все параметры – логические идентифицирующие списки.

Использование IP внутри сегмента ИКС как источник угроз

Первичный признак распознавания $\alpha_{59}^{(V)}$, соответствующий нарушению работоспособности сегмента ИКС, описывается параметром:

$$B_{59}(f^{(V)}_{3,\,2,\,1,\,2,\,2}) = \beta_{59,\,1},$$

характеризующим наличие угрозы от IP внутри сегмента – $\beta_{59,\,1}$. Параметр – логический идентифицирующий список.

Подмена анализом значения идентификатора соединения (TCP)

Первичный признак распознавания $\alpha_{60}^{(V)}$, соответствующий нарушению работоспособности сегмента ИКС, описывается параметром:

$$B_{60}(f^{(V)}_{3,\,2,\,2,\,1,\,1}) = \beta_{60,\,1},$$

характеризующим наличие факта дубляжа пакетов с идентичным идентификатором внутри сегмента – $\beta_{60,\,1}$. Параметр – логический идентифицирующий список.

«Шторм» ложных запросов, направленных на сервер, «Шторм» ложных запросов на соединение, направленных на объект воздействия

Первичный признак распознавания $\alpha_{61}^{(V)}$, соответствующий нарушению работоспособности сегмента ИКС, описывается параметром:

$$B_{61}(f^{(V)}_{3,2,2,1,2}) = \beta_{61,1},$$

характеризующим наличие факта шторма пакетов на сервер или абонент сегмента – $\beta_{61,1}$. Параметр – логический идентифицирующий список.

Land атака,
Атака через неправильную сегментацию пакетов,
Атака через широковещательный запрос

Первичный признак распознавания $\alpha_{62}^{(V)}$, соответствующий нарушению работоспособности сегмента ИКС, описывается параметром:

$$B_{62}(f^{(V)}_{3,2,2,2,1}) = \beta_{62,1},$$

характеризующим наличие пакетов внутри сегмента с признаками сетевых атак – $\beta_{62,1}$. Параметр – логический идентифицирующий список.

Сбор открытых данных

Первичный признак распознавания $\alpha_{63}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{63}(f^{(V)}_{4,1,1,1,1}) = \beta_{63,1},$$

характеризующим количество трафика через элемент сегмента – $\beta_{63,1}$. Параметр – количественный информативный список.

Сбор зашифрованных данных

Первичный признак распознавания $\alpha_{64}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{64}(f^{(V)}_{4,1,1,1,2}) = \beta_{64,1},$$

характеризующим количество зашифрованного трафика через элемент сегмента – $\beta_{64,1}$. Параметр – количественный информативный список.

Сбор односторонне преобразованных данных (CRC и т.п.)

Первичный признак распознавания $\alpha_{65}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{65}(f^{(V)}_{4,1,1,1,3}) = \beta_{65,1},$$

характеризующим количество односторонне преобразованного трафика через элемент сегмента – $\beta_{65,1}$. Параметр – количественный информативный список.

Сбор информации о стандартных портах

Первичный признак распознавания $\alpha_{66}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{66}(f^{(V)}_{4,1,1,2,1}) = \beta_{66,1},$$

характеризующим используемые стандартные порты в элементе сегмента – $\beta_{66,1}$. Параметр – лингвистический информативный список.

Сбор информации об индивидуально использующихся портах в сегменте ИМТС

Первичный признак распознавания $\alpha_{67}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{67}(f^{(V)}_{4,1,1,2,2}) = \beta_{67,1},$$

характеризующим используемые индивидуальные порты в элементе сегмента – $\beta_{67,1}$. Параметр – лингвистический информативный список.

Криптоалгоритмы

Первичный признак распознавания $\alpha_{68}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{68}(f^{(V)}_{4,1,1,3,1}) = \beta_{68,1},$$

характеризующим наличие криптопакетов при обмене информацией внутри сегмента – $\beta_{68,1}$. Параметр представляется логическим идентифицирующим списком.

Накопление информативных данных

Первичный признак распознавания $\alpha_{69}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{69}(f^{(V)}_{4,1,2,1,1}) = \beta_{69,1},$$

характеризующим количество трафика через элемент сегмента – $\beta_{69,1}$. Параметр – количественный информативный список.

Идентификация активных служб, выполняемых на серверах

Первичный признак распознавания $\alpha_{70}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{70}(f^{(V)}_{4,1,2,2,1}) = \beta_{70,1},$$

характеризующим активные службы в элементах сегмента – $\beta_{70,1}$. Параметр – лингвистический идентифицирующий список.

Анализ перехваченных данных

Первичный признак распознавания $\alpha_{71}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{71}(f^{(V)}_{5,1,1,1,1}) = \beta_{71,1},$$

характеризующим спад производительности элемента сегмента – $\beta_{71,1}$. Параметр – количественный идентифицирующий список.

Прямой поиск через точку доступа

Первичный признак распознавания $\alpha_{72}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{72}(f^{(V)}_{5,1,2,1,1}) = \beta_{72,1},$$

характеризующим поиск информации абонентом элемента сегмента – $\beta_{72,1}$. Параметр – логический информативный список.

Формирование поискового запроса (для СУБД)

Первичный признак распознавания $\alpha_{73}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{73}(f^{(V)}_{5,1,3,1,1}) = \beta_{73,1},$$

характеризующим количеством запросов к СУБД абонентом элемента сегмента – $\beta_{73,1}$. Параметр – количественный информативный список.

Передача команды на копирование

Первичный признак распознавания $\alpha_{74}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{74}(f^{(V)}_{5,2,1,1,1}) = \beta_{74,1}, \beta_{74,2},$$

характеризующим количество запросов на копирование информации абонентом элемента сегмента – $\beta_{74,1}$. и объем трафика – $\beta_{74,2}$. Параметры – количественные информативные списки.

Передача данных

Первичный признак распознавания $\alpha_{75}^{(V)}$, соответствующий сбору данных внутри сегмента ИКС, описывается параметром:

$$B_{75}(f^{(V)}_{5,2,2,1,1}) = \beta_{75,1},$$

характеризующими объем трафика копированной информации абонентом элемента сегмента – $\beta_{75,1}$. Параметр – количественный информативный список.

Вход в систему

Первичный признак распознавания $\alpha_{76}^{(V)}$, соответствующий модификации данных внутри сегмента ИКС, описывается параметром:

$$B_{76}(f^{(V)}_{5,3,1,1,1}) = \beta_{76,1}$$

характеризующим вход абонента элемента сегмента в систему – $\beta_{76,1}$. Параметр – логический информативный список.

Формирование запроса на поиск (либо команда перехода)

Первичный признак распознавания $\alpha_{77}^{(V)}$, соответствующий модификации данных внутри сегмента ИКС, описывается параметром:

$$B_{77}(f^{(V)}_{5,3,1,2,1}) = \beta_{77,1},$$

характеризующим сетевую активность абонента элемента сегмента в системе – $\beta_{77,1}$. Параметр – логический информативный список.

Модификация информации с последующим сохранением

Первичный признак распознавания $\alpha_{78}^{(V)}$, соответствующий модификации данных внутри сегмента ИКС, описывается параметром:

$$B_{78}(f^{(V)}_{5,3,1,3,1}) = \beta_{78,1},$$

характеризующим перезапись информации абонентом элемента сегмента в системе – $\beta_{78,1}$. Параметр – логический информативный список.

Активация вредоносного ПО

Первичный признак распознавания $\alpha_{79}^{(V)}$, соответствующий модификации данных внутри сегмента ИКС, описывается параметром:

$$B_{79}(f^{(V)}_{5,3,2,1,1}) = \beta_{79,1},$$

характеризующим активацию вредоносного ПО абонентом элемента сегмента в системе – $\beta_{79,1}$. Параметр – логический информативный список.

Поиск участка данных

Первичный признак распознавания $\alpha_{80}^{(V)}$, соответствующий модификации данных внутри сегмента ИКС, описывается параметром:

$$B_{80}(f^{(V)}_{5,3,2,2,1}) = \beta_{80,1},$$

характеризующим сетевую активность вредоносного ПО в элементе сегмента – $\beta_{80,1}$. Параметр – логический информативный список.

Модификация найденного участка

Первичный признак распознавания $\alpha_{81}^{(V)}$, соответствующий модификации данных внутри сегмента ИКС, описывается параметром:

$$B_{81}(f^{(V)}_{5,3,2,3,1}) = \beta_{81,1},$$

характеризующим перезапись информации ПО в сегменте – $\beta_{81,1}$. Параметр – логический информативный список.

Запрос на замену данных с подтверждением перезаписи

Первичный признак распознавания $\alpha_{82}^{(V)}$, соответствующий модификации данных внутри сегмента ИКС, описывается параметром:

$$B_{82}(f^{(V)}_{5,\,3,\,3,\,1,\,1}) = \beta_{82,\,1},$$

характеризующим количество команд на перезапись информации абонентом в сегменте – $\beta_{82,\,1}$. Параметр – количественный информативный список.

Передача новых данных

Первичный признак распознавания $\alpha_{83}^{(V)}$, соответствующий модификации данных внутри сегмента ИКС, описывается параметром:

$$B_{83}(f^{(V)}_{5,\,3,\,3,\,2,\,1}) = \beta_{83,\,1},$$

характеризующим количество данных на перезапись информации абонентом в сегменте – $\beta_{83,\,1}$. Параметр – количественный информативный список.

Удаление вредоносного программного кода по команде злоумышленника

Первичный признак распознавания $\alpha_{84}^{(V)}$, соответствующий сокрытию следов атаки внутри сегмента ИКС, описывается параметром:

$$B_{84}(f^{(V)}_{6,\,2,\,1,\,1,\,1}) = \beta_{84,\,1},$$

характеризующим наличие команды на удаление вредоносного ПО в сегменте – $\beta_{84,\,1}$. Параметр – логический информативный список.

Удаление вредоносного программного кода автоматически

Первичный признак распознавания $\alpha_{85}^{(V)}$, соответствующий сокрытию следов атаки внутри сегмента ИКС, описывается параметром:

$$B_{85}(f^{(V)}_{6,\,2,\,2,\,1,\,1}) = \beta_{85,\,1}$$

характеризующим наличие самоудаления вредоносного ПО в сегменте – $\beta_{85,\,1}$. Параметр – логический информативный список.

Удаление несанкционированных подключений

Первичный признак распознавания $\alpha_{86}^{(V)}$, соответствующий сокрытию следов атаки внутри сегмента ИКС, описывается параметром:

$$B_{86}(f^{(V)}_{6,\,3,\,1,\,1,\,1}) = \beta_{86,\,1},$$

характеризующим факт удаления несанкционированных подключений к элементам сегмента – $\beta_{86,\,1}$. Параметр – логический идентифицирующий список.

Удаление следов непосредственного воздействия

Первичный признак распознавания $\alpha_{87}^{(V)}$, соответствующий сокрытию следов атаки внутри сегмента ИКС, описывается параметром:

$$B_{87}(f^{(V)}_{6,\,4,\,1,\,1,\,1}) = \beta_{87,\,1},$$

характеризующим факт удаления следов воздействия на элементы сегмента – $\beta_{87,\,1}$. Параметр – логический идентифицирующий список.

Сформируем на основе параметров признаков распознавания $B_1 \div B_{87}$ три списка параметров:

1) единый список A параметров:

$$A = \langle a_k \rangle,\ k = 1, 2, \ldots, 136,$$

где a_1 – характеристика состояния параметров;

$a_2 \div a_{136}$ – параметры признаков распознавания $B_1 \div B_{87}$;

2) список B простых параметров:

$$B = \langle b_l \rangle,\ l = 1, 2, \ldots, 10,$$

где $b_1 \div b_{10}$ – параметры признаков распознавания $B_1 \div B_{87}$, соответствующие следующим параметрам списка A: a_1, a_7, a_{23}, a_{24}, a_{25}, a_{26}, a_{45}, a_{46}, a_{47}, a_{48};

3) список C идентифицирующих параметров:

$$C = \langle c_{m,\,u} \rangle,\ m = 1, 2, \ldots, 83,\ u = 1, 2, \ldots, U,$$

где $c_{1,\,u} \div c_{83,\,u}$ – параметры признаков распознавания $B_1 \div B_{87}$, соответствующие следующим параметрам списка A - a_3, a_8, a_{13}, a_{19}, a_{20}, a_{21}, a_{22}, a_{27}, a_{28}, a_{29}, a_{30}, a_{31}, a_{32}, a_{33}, a_{34}, a_{35}, a_{36}, a_{37}, a_{38}, a_{39}, a_{40}, a_{49}, a_{50}, a_{51}, a_{52}, a_{53}, a_{54}, a_{55}, a_{56}, a_{57}, a_{58}, a_{59}, a_{60}, a_{62}, a_{63}, a_{64}, a_{65}, a_{66}, a_{67}, a_{68}, a_{69}, a_{70}, a_{71}, a_{72}, a_{73}, a_{74}, a_{75}, a_{76}, a_{77}, a_{78}, a_{79}, a_{80}, a_{81}, a_{82}, a_{83}, a_{84}, a_{85}, a_{87}, a_{88}, a_{91}, a_{92}, a_{93}, a_{94}, a_{95}, a_{96}, a_{97}, a_{98}, a_{99}, a_{100}, a_{101}, a_{102}, a_{103}, a_{104}, a_{105}, a_{106}, a_{112}, a_{113}, a_{114}, a_{115}, a_{117}, a_{118}, a_{134}, a_{135};

U – количество элементов топологии сегмента;

4) список D информативных параметров:

$$D = \langle d_{q,\,u,\,v} \rangle,\ q = 1, 2, \ldots, 42,\ u = 1, 2, \ldots, U,\ v = 1, 2, \ldots, V,$$

где $d_{1,\ u,\ v} \div d_{42,\ u,\ v}$ – параметры признаков распознавания $B_1 \div B_{87}$ соответствующие следующим параметрам списка A: a_2, a_4, a_5, a_6, a_9, a_{10}, a_{11}, a_{12}, a_{14}, a_{15}, a_{16}, a_{17}, a_{18}, a_{41}, a_{42}, a_{43}, a_{44}, a_{61}, a_{86}, a_{89}, a_{90}, a_{107}, a_{108}, a_{109}, a_{110}, a_{111}, a_{116}, a_{119}, a_{120}, a_{121}, a_{122}, a_{123}, a_{124}, a_{125}, a_{126}, a_{127}, a_{128}, a_{129}, a_{130}, a_{131}, a_{132}, a_{133};

V – количество активного персонала сегмента.

Состояние параметров – это набор значений первичных параметров

распознавания в текущий момент времени безотносительно к остальным параметрам. Характеристика состояния параметров введена для корректного анализа первичных признаков распознавания в условиях их взаимодействия и потокового представления.

Исходя из этого, характеристика состояния параметров представляется следующим образом:

$a_1 = 0$ – состояние признаков распознавания актуального на текущий момент;

$a_1 = 1$ – взаимосвязанное состояние признаков распознавания актуального на текущий момент;

$a_1 = 2, 3, \ldots, n + 2$, где n – число ключевых состояний признаков распознавания;

$a_1 = n + 2, n + 3, \ldots, N$, где N – граница длины стека архива взаимосвязанных состояний признаков распознавания в направлении от младшего к старшему.

Таким образом, имеет место множество списков

$$\{A_n\} = \{\langle a_{nk} \rangle\}, \quad k = 1, 2, \ldots, 136, \quad n = 1, 2, \ldots, N.$$

$$\{B_n\} = \{\langle b_{nl} \rangle\}, \quad l = 1, 2, \ldots, 10, \quad n = 1, 2, \ldots, N.$$

$$\{C_n\} = \{\langle c_{nmu} \rangle\}, \quad m = 1, 2, \ldots, 83, \quad u = 1, 2, \ldots, U, \quad n = 1, 2, \ldots, N.$$

$$\{D_n\} = \{\langle d_{nquv} \rangle\}, \quad q = 1, 2, \ldots, 42, \quad u = 1, 2, \ldots, U, \quad v = 1, 2, \ldots, V, \quad n = 1, 2, \ldots, N.$$

Для представления параметров и их взаимосвязей в пределах одного состояния определим фиксированные множества $\{\zeta_m\}$ и $\{\kappa_m\}$, $m = 1, 2, 3$, признаков состояния, в котором:

ζ_1 – признак характера взаимосвязей;

κ_1 – коэффициент изменения взаимосвязи;

ζ_2 – признак взаимосвязей по топологии сегмента ИКС;

κ_2 – коэффициент взаимосвязи по топологии сегмента ИКС;

ζ_3 – признак взаимосвязей по персоналу сегмента ИКС;

κ_3 – коэффициент взаимосвязи по персоналу сегмента ИКС.

Проводя анализ характера взаимосвязей параметров, можно выделить их следующие типы: независимые параметры, взаимозависимые параметры, связанные параметры и исключающие параметры.

Для каждого из перечисленных типов имеют место следующие правила взаимодействия:

1) $\zeta_1 = 0$ – пара независимых параметров не влияет на значение друг друга. Взаимосвязь отсутствует и не учитывается.
2) $\zeta_1 = 1$ – пара взаимозависимых параметров должна коррелировать друг с другом.
3) $\zeta_1 = 2$ – пара связанных параметров взаимодействует по какому-либо правилу.
4) $\zeta_1 = -1$ – пара взаимоисключающих параметров.

Для формализованного представления характера взаимосвязей параметров будем использовать матричную форму:

а) для представления типов взаимосвязей:

$$s_{1,1}(\zeta_1),\ s_{1,2}(\zeta_1),\ \ldots,\ s_{1,135}(\zeta_1);$$
$$s_{2,1}(\zeta_1),\ s_{2,2}(\zeta_1),\ \ldots,\ s_{2,135}(\zeta_1);$$
$$\ldots$$
$$s_{135,1}(\zeta_1),\ s_{135,2}(\zeta_1),\ \ldots,\ s_{135,135}(\zeta_1).$$

б) для представления характера изменения взаимосвязей:

$$z_{1,1}(\kappa_1),\ z_{1,2}(\kappa_1),\ \ldots,\ z_{1,135}(\kappa_1);$$
$$z_{2,1}(\kappa_1),\ z_{2,2}(\kappa_1),\ \ldots,\ z_{2,135}(\kappa_1);$$
$$\ldots$$
$$z_{135,1}(\kappa_1),\ z_{135,2}(\kappa_1),\ \ldots,\ z_{135,135}(\kappa_1).$$

Значения элементов матрицы изменения взаимосвязей определяются в соответствии с методами теории искусственного интеллекта и будут рассмотрены далее.

В табл. 3.4.1 приводятся формальные правила оценки взаимосвязей параметров, где *i* и *j* – индексы сравниваемых признаков.

Таблица 3.4.1

$\zeta_1 = 0$	$z_{i,j}(\kappa_1) = 0,\ a_{2i} = a_{1i}$
$\zeta_1 = 1$	$a_{2,i} = a_{1,i} + z_{i,j}(\kappa_1)(a_{1i} + a_{1j})/2$
$\zeta_1 = 2$	$a_{2,i} = a_{1,i} + z_{i,j}(\kappa_1)(a_{1j})$
$\zeta_1 = -1$	$a_{2,i} = a_{1,i} + z_{i,j}(\kappa_1)(a_{1i} - a_{1j})/2$

$$a_{2,k} = a_{1,k} + \sum_{j'=1}^{135} F\left(\zeta_1, a_k, a_j\right).$$

Из списка A_2 формируем множество списков B_2, C_1, D_1.

Для элементов списка B_2 все взаимосвязи учтены на предыдущем этапе. Для элементов идентифицирующего и информативного списков, которые могут иметь взаимосвязь между различными элементами в одном списке, как топологическую, так и связанную с персоналом, установим следующие типы взаимосвязи:

1. Топологическая взаимосвязь (по элементу списка *C*):

Тип I – взаимосвязанные элементы топологии. Имеется прямая связь, количество разделяющих элементов топологии сегмента ИКС от 0 до 3.

Тип II – элементы одной подсети. Имеется взаимосвязь, организованная программным или аппаратным способом, количество разделяющих элементов топологии не ограничивается, Тип IIа – элементы расположены в одном здании, Тип IIб – элементы расположены распределенно.

Тип III – элементы взаимосвязаны топологически, однако не входят во взаимосвязь на программном уровне при работе.

Тип IV – физически развязанные элементы топологии (связи нет).

Для каждого из перечисленных типов имеют место следующие правила взаимодействия:

1) $\zeta_2 = 1$ – Тип I;
2) $\zeta_2 = 2$ – Тип IIа;
3) $\zeta_2 = 3$ – Тип IIб;
4) $\zeta_2 = 4$ – Тип III;
5) $\zeta_2 = 0$ – Тип IV.

Для формализованного представления всего множества топологических взаимосвязей параметров используем матричную форму:

а) для представления типов взаимосвязей:

$$s_{1,1}(\zeta_2),\ s_{1,2}(\zeta_2),\ \ldots,\ s_{1,83}(\zeta_2);$$
$$s_{2,1}(\zeta_2),\ s_{2,2}(\zeta_2),\ \ldots,\ s_{2,83}(\zeta_2);$$
$$\ldots$$
$$s_{U,1}(\zeta_2),\ s_{U,2}(\zeta_2),\ \ldots,\ s_{U,83}(\zeta_2),$$

где u – число элементов топологии сегмента ИКС;

б) для представления характера изменения взаимосвязей по топологии сегмента:

$$z_{1,1}(\kappa_2),\ z_{1,2}(\kappa_2),\ \ldots,\ z_{1,83}(\kappa_2);$$
$$z_{2,1}(\kappa_2),\ z_{2,2}(\kappa_2),\ \ldots,\ z_{2,83}(\kappa_2);$$
$$\ldots$$
$$z_{U,1}(\kappa_2),\ z_{U,2}(\kappa_2),\ \ldots,\ z_{U,83}(\kappa_2).$$

Значения элементов матрицы изменения взаимосвязей по топологии

определяются в соответствии с методами теории искусственного интеллекта и будут рассмотрены далее.

В табл. 3.4.2 приводятся формальные правила взаимосвязей по топологии сегмента ИКС.

Таблица 3.4.2

$\zeta_2 = 1$	$c_{2,u,m} = c_{1,u,m} + z_{u,m}(\kappa_2)(c_{1,u',m})$
$\zeta_2 = 2$	$c_{2,u,m} = c_{1,u,m} + z_{u,m}(\kappa_2)(c_{1,u',m})$
$\zeta_2 = 3$	$c_{2,u,m} = c_{1,u,m} + z_{u,m}(\kappa_2)(c_{1,u',m})$
$\zeta_2 = 4$	$c_{2,u,m} = c_{1,u,m} + z_{u,m}(\kappa_2)(c_{1,u',m})$
$\zeta_2 = 0$	$z_{u,m}(\kappa_2) = 0$ $c_{2,u,m} = c_{1,u,m}$ (в том числе при $c_{1,u,m} = c_{1,u',m}$)

В приведенных выражениях оценивается взаимосвязь топологического элемента c_{1um} с топологическим элементом $c_{1u'm}$. При этом $u' = 1, 2, \ldots, U$. Результатом является второй уровень матрицы C – уровень c_{2um}.

Исходя из этого:

$$c_{2,u,m} = c_{1,u,m} + \sum_{m=1}^{82} z_{u,m}(\kappa_2) \cdot c_{1,u',m}.$$

2. Взаимосвязь по персоналу:

Тип А – взаимозаменяющий друг друга персонал;

Тип Б – персонал, имеющий взаимный физический доступ к абонентским станциям сети;

Тип В – администрирующий персонал (программисты и системные администраторы при настройке приложений, операционных систем, аппаратной части элементов топологии);

Тип Г – несвязанный персонал.

Для каждого из перечисленных типов имеют место следующие правила взаимодействия:

1) $\zeta_3 = 1$ – Тип А;
2) $\zeta_3 = 2$ – Тип Б;
3) $\zeta_3 = 0$ – Тип В;
4) $\zeta_3 = -1$ – Тип Г.

Для формализованного представления всего множества параметров взаимосвязей по персоналу воспользуемся матричной формой:

а) для представления типов взаимосвязей:

$$s_{1,1}(\zeta_3),\ s_{1,2}(\zeta_3),\ \ldots,\ s_{1,42}(\zeta_3);$$
$$s_{2,1}(\zeta_3),\ s_{2,2}(\zeta_3),\ \ldots,\ s_{2,42}(\zeta_3);$$
$$\ldots$$
$$s_{V,1}(\zeta_3),\ s_{V,2}(\zeta_3),\ \ldots,\ s_{V,42}(\zeta_3).$$

б) для представления характера изменения взаимосвязей:

$$z_{1,1}(\kappa_3),\ z_{1,2}(\kappa_3),\ \ldots,\ z_{1,42}(\kappa_3);$$
$$z_{2,1}(\kappa_3),\ z_{2,2}(\kappa_3),\ \ldots,\ z_{2,42}(\kappa_3);$$
$$\ldots$$
$$z_{V,1}(\kappa_3),\ z_{V,2}(\kappa_3),\ \ldots,\ z_{V,42}(\kappa_3),$$

где V – количество зарегистрированного персонала сегмента.

Значения элементов матрицы изменения взаимосвязей персонала определяются в соответствии с методами теории искусственного интеллекта и будут рассмотрены далее.

В табл. 3.4.3 приводятся формальные правила взаимосвязей по персоналу сегмента ИКС

Таблица 3.4.3

$\zeta_3 = 1$	$d_{2,q,u,v} = d_{1,q,u,v} + z_{q,v}(\kappa_3)\ d_{1,q,u,v'}$
$\zeta_3 = 2$	$d_{2,q,u,v} = d_{1,q,u,v} + z_{q,v}(\kappa_3)\ d_{1,q,u,v'}$
$\zeta_3 = 0$	$d_{2,q,u,v} = d_{1,q,u,v} + z_{q,v}(\kappa_3)\ d_{1,q,u,v'}$
$\zeta_3 = -1$	$z_{i,j}(\kappa_3) = 0,\ d_{2,q,u,v} = d_{1,q,u,v'}$

Физически информация о топологических взаимосвязях и взаимосвязях по персоналу представляется в виде списка взаимосвязей, отдельного для каждого типа.

$$d_{2,q,u,v} = d_{1,q,u,v} + \sum_{m=1}^{82}\sum_{v=1}^{42}\left[\left(z_{m,u}(\kappa_2)\cdot c_{1,m,u}\right)\times\left(z_{q,v}(\kappa_3)\cdot d_{1,q,u,v}\right)\right].$$

Таким образом, сформирована описательная база для представления всего многообразия признаков распознавания угроз конфиденциальности информационных ресурсов территориальных сегментов ИКС.

Теперь возвратимся к вопросу формирования значений элементов матрицы изменения взаимосвязей – $z_{i,j}(\kappa_1)$, изменения взаимосвязей по топологии – $z_{u,m}(\kappa_2)$, изменения взаимосвязей персонала – $z_{q,v}(\kappa_3)$. Как было сказано выше, для формирования данных матриц целесообразно применять методы искусственного интеллекта. В частности, предлагаемая форма представления данных в системе практически идеально подходит к

применению так называемых нейронных сетей. В данном случае рекомендуется использование сети на основе модели нейронов Хебба, система обучения в которой формируется на основе одноименного правила (рис. 3.4.1). Данное правило обеспечивает увеличение взаимозависимости параметров при одновременной их активации.

Так как элементы матрицы изменения взаимосвязей аналогичны друг другу, то введем псевдоним F, в котором

$f_{f1,f2}$ – элемент одной из матриц изменения взаимосвязей, а $f1$ и $f2$ – соответственно одна из пар (i,j), (u,m), (q,v) соответствующая элементам взятой матрицы.

$$F= \begin{matrix} f_{1,1}, f_{1,2}, \ldots, f_{1,f1}; \\ f_{2,1}, f_{2,2}, \ldots, f_{2,f1}; \\ \ldots \\ f_{f2,1}, f_{f2,2}, \ldots, z_{f2,f1}, \end{matrix}$$

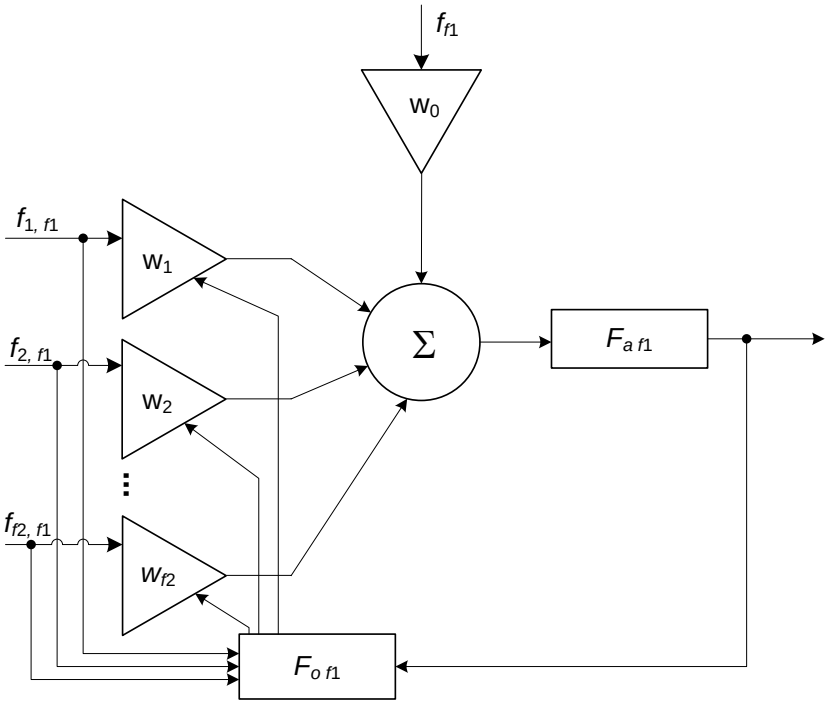

Рис. 3.4.1. Адаптированная схема нейрона Хебба

В качестве функции активации нейрона будем использовать униполярную функцию $F_a=1/(1+e^{0.5\cdot x1})$, а в качестве функции обучения – $F_{o\,f1}(t+1) = f_{f1}(t) + 0{,}1 \cdot y \cdot f_{f1}$, где y – выходное значение нейрона прошлого цикла работы, а f_{f1} – входное значение текущего цикла.

В процессе работы данного вида нейронной сети будет происходить

неподконтрольное возрастание ряда весов при наличии связи между параметрами. Поэтому необходимо предусмотреть корректирующий механизм при превышении. В качестве предельного параметра $f_{f1,f2}$ примем значение 1,0. Соответственно весовой параметр обучения не должен превышать 10 при выбранном коэффициенте обучения 0,1. В случае превышения необходимо скорректировать веса всей системы, т.е. во всех матрицах. Для коррекции можно воспользоваться выражением:

$$S = S - S^*(S_{pr} - S_{max})/ S_{pr},$$

где S – корректируемый параметр,

S_{pr} – парамер превысивший максимальное значение (S_{max}),

S_{max} – максимально допустимое значение параметра (здесь 10).

4 Обобщение признаков распознавания угроз информационной безопасности на объекте информатизации

На основе рассмотренных наборов множеств признаков для всех этапов противоправных действий на объекте информатизации определим стратегию проведения оценки угрозы информационной безопасности в привязке к каждому элементу топологии и каждому сотруднику активно работающих в контролируемом сегменте ИКС.

Для этого необходимо на конечном этапе получить множество списков

$$\{X_f\} = \{\langle x_{fuv}\rangle\},\ f = 1, 2, \ldots, 6,\ u = 1, 2, \ldots, U,\ v = 1, 2, \ldots, V,$$

где f – количество выделенных этапов противоправных действий;

U – количество элементов топологии сегмента;

V – количество активного персонала сегмента.

Списки вида $\langle x_{fuv}\rangle$ обобщают информацию об уровне угрозы конфиденциальности информационных ресурсов сегмента ИМТС.

На основе представленного множества можно сформировать следующий ряд показателей:

1) G_1 – общий для всего сегмента уровень угроз;

2) $G_2 \div G_7$ – общий для всего сегмента поэтапный уровень угроз;

3) $G_8 \div G_{8+U}$ – уровень угрозы для каждого элемента топологии сегмента;

4) $G_{9+U} \div G_{9+U+V}$ – уровень угрозы для каждого пользователя сегмента.

Формирование моделей распознавания будем осуществлять с помощью прямой и косвенной композиции параметров системы распознавания. В данном случае прямая композиция заключается в определении правил объединения наборов признаков распознавания в соответствии с рассмотренной выше схемой декомпозиции, а косвенная включит в себя взаимосвязи между элементами топологии сегмента и его персоналом в декомпозиционной схеме системы распознавания. Подобное представление позволит корректно оценить взаимозависимости параметров системы распознавания в пределах одного этапа воздействия и включить в оценку возникающие связи параметров при переходе противоправного воздействия от одного этапа к другому.

Прямая композиция параметров системы распознавания

Для обобщения ряда моделей определим следующие значения индексов элементов определенных множеств [7]:

порядковый номер элемента модели a,

список простых параметров: $B = \langle b_{la} \rangle$,

список идентифицирующих параметров $C = \langle c_{ma,\,u} \rangle$,

список информативных параметров $D = \langle d_{qa,\,u,\,v} \rangle$.

Для удобства восприятия значения индексов, аналогичные рассмотренным в пункте 3.4, не указываются.

Результирующий параметр (список параметров) имеет индекс r.

Оценка показателей первого уровня прямой композиции

Описываются модели следующих типов[7]:

– Логический параметр и логический информативный список:

$$d_{r,q,u,v} = \frac{b_{l1} + d_{n,q2,u,v}}{2},$$

Результат – $d_{r,\ q,\ u,\ v}$ представляется в виде количественного информативного списка.

– Логический идентификационный список и логический информативный список:

$$d_{r,q,u,v} = \frac{c_{n,m1,u} + d_{n,q2,u,v}}{2},$$

результат – количественный информативный список.

– Логический информативный список и логический информативный список:

$$d_{r,q,u,v} = \frac{d_{n,q1,u,v} + d_{n,q2,u,v}}{2},$$

результат – количественный информативный список.

– Вероятностный идентификационный список и вероятностный информативный список:

$$d_{r,q,u,v} = \frac{c_{n,m1,u} + d_{n,q2,u,v}}{2},$$

результат – количественный идентификационный список.

– Логический идентификационный список и логический идентификационный список:

$$c_{r,m,u} = \frac{c_{n,m1,u} + c_{n,m2,u}}{2},$$

результат – количественный идентификационный список.

– Логический и вероятностные параметры:

$$b_r = \frac{b_{l1} + b_{l2}}{2},$$

результат – количественный параметр.

– Лингвистический идентификационный список и лингвистический идентификационный список:

$$c_{r,m,u} = c_{n,m1,u} + c_{n,m2,u},$$

результат – лингвистический идентификационный список.

– Логический и логический параметры:

$$b_r = \frac{b_{l1} + b_{l2}}{2},$$

результат – количественный параметр.

– Логический идентификационный список и количественный идентификационный список:

$$c_{r,m,u} = \frac{c_{n,m1,u} + c_{n,m2,u}}{2},$$

результат – количественный идентификационный список.

– Количественный идентификационный список и количественный информативный список:

$$c_{r,m,u} = \frac{c_{n,m1,u} + c_{n,m2,u}}{2},$$

результат – количественный идентификационный список.

Оценка показателей второго уровня прямой композиции

Описываются модели следующих типов[7]:

– Логический идентификационный список, количественный идентификационный список и логический идентификационный список:

$$c_{r,m,u} = \frac{c_{n,m1,u} + c_{n,m3,u}}{2} + c_{n,m2,u},$$

результат – количественный идентификационный список.

– Количественный идентификационный список, количественный информативный список и логический идентификационный список:

$$d_{r,q,u,v} = c_{n,m1,u} + d_{n,q2,u,v} + c_{n,m3,u},$$

результат – количественный информативный список.

– Количественный информативный список и логический идентификационный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + c_{n,m2,u},$$

результат – количественный информативный список.

– Логический идентификационный список и логический идентификационный список:

$$c_{r,m,u} = c_{n,m1,u} + c_{n,m2,u},$$

результат – количественный идентификационный список.

– Количественный информативный список и количественный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – количественный информативный список.

– Лингвистический информативный список и лингвистический информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – лингвистический информативный список.

Оценка показателей третьего уровня прямой композиции

Описываются модели следующих типов [7]:

– Логический информативный список, количественный информативный список, вероятностный параметр и количественный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v} + b_{l3} + d_{n,q4,u,v},$$

результат – количественный информативный список.

– Вероятностный информативный список и количественный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – количественный информативный список.

– Вероятностный информативный список и вероятностный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – количественный информативный список.

– Логический идентификационный список и количественный идентификационный список:

$$c_{r,m,u} = c_{n,m1,u} + c_{n,m2,u},$$

результат – количественный идентификационный список.

– Количественный и количественный параметры:

$$b_r = b_{l1} + b_{l2},$$

результат – количественный параметр.

– Количественный идентификационный список и количественный идентификационный список:

$$c_{r,m,u} = c_{n,m1,u} + c_{n,m2,u},$$

результат – количественный идентификационный список.

– Лингвистический идентификационный список и лингвистический идентификационный список:

$$c_{r,m,u} = c_{n,m1,u} + c_{n,m2,u},$$

результат – лингвистический идентификационный список.

– Логический идентификационный список и логический идентификационный список:

$$c_{r,m,u} = c_{n,m1,u} + c_{n,m2,u},$$

результат – количественный идентификационный список.

– Количественный информативный список и количественный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – количественный информативный список.

– Логический и логический параметры:

$$b_r = b_{l1} + b_{l2},$$

результат – количественный параметр.

– Количественный идентификационный список, количественный информативный список и количественный идентификационный список:

$$d_{r,q,u,v} = c_{n,m1,u} + d_{n,q2,u,v} + c_{n,m3,u},$$

результат – количественный информативный список.

– Логический идентификационный список, количественный информативный список и логический идентификационный список:

$$d_{r,q,u,v} = c_{n,m1,u} + d_{n,q2,u,v} + c_{n,m3,u},$$

результат – количественный информативный список.

– Количественный информативный список и количественный идентификационный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + c_{n,m2,u},$$

результат – количественный информативный список.

– Количественный информативный список, лингвистический информативный список и количественный идентификационный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v} + c_{n,m3,u},$$

результат – количественный информативный список.

– Логический информативный список и логический информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – количественный информативный список.

Оценка показателей четвертого уровня прямой композиции

Описываются модели следующих типов [7]:

– Количественный информативный список и количественный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – количественный информативный список.

– Количественный информативный список, количественный идентификационный список, количественный параметр, количественный идентификационный список и лингвистический идентификационный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + c_{n,m2,u} + b_{l3} + c_{n,m4,u} + c_{n,m5,u},$$

результат – количественный информативный список.

– Количественный идентификационный список и лингвистический идентификационный список:

$$c_{r,m,u} = c_{n,m1,u} + c_{n,m2,u},$$

результат – количественный идентификационный список.

– Логический идентификационный список, логический идентификационный список и количественный информативный список:

$$d_{r,q,u,v} = c_{n,m1,u} + c_{n,m2,u} + d_{n,q3,u,v},$$

результат – количественный информативный список.

– Количественный параметр и количественный параметр:

$$b_r = b_{l1} + b_{l2},$$

результат – количественный параметр.

– Количественный информативный список, количественный идентификационный список и логический идентификационный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + c_{n,m2,u} + c_{n,m3,u},$$

результат – количественный информативный список.

– Количественный идентификационный список, количественный идентификационный список, количественный идентификационный список и количественный информативный список:

$$d_{r,q,u,v} = c_{n,m1,u} + c_{n,m2,u} + d_{n,q3,u,v},$$

результат – количественный информативный список.

– Количественный информативный список, количественный информативный список и лингвистический информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v} + d_{n,q3,u,v},$$

результат – количественный информативный список.

– Количественный идентификационный список, логический информативный список и количественный информативный список:

$$d_{r,q,u,v} = c_{n,m1,u} + d_{n,q2,u,v} + d_{n,q3,u,v},$$

результат – количественный информативный список.

– Количественный информативный список и количественный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – количественный информативный список.

– Логический информативный список и логический информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v},$$

результат – количественный информативный список.

Оценка показателей пятого уровня прямой композиции

Описываются модели следующих типов [7]:

– Количественный информативный список, количественный информативный список, лингвистический информативный список, количественный идентификационный список и лингвистический идентификационный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v} + d_{n,q3,u,v} + c_{n,m4,u} + c_{n,m5,u},$$

результат – количественный информативный список.

– Количественный информативный список, количественный параметр, количественный параметр, количественный информативный список и количественный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + b_{l2} + b_{l3} + d_{n,q4,u,v} + d_{n,q5,u,v},$$

результат – количественный информативный список.

– Количественный информативный список, лингвистический информативный список и лингвистический идентификационный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v} + d_{n,q3,u,v},$$

результат – количественный информативный список.

– Количественный информативный список, количественный информативный список и количественный информативный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + d_{n,q2,u,v} + d_{n,q3,u,v},$$

результат – количественный информативный список.

– Количественный информативный список, логический идентификационный список и логический идентификационный список:

$$d_{r,q,u,v} = d_{n,q1,u,v} + c_{n,m2,u} + c_{n,m3,u},$$

результат – количественный информативный список.

На основании представленных выражений сформируем матричное представление $G_{M1,\ N}$ уровня угрозы для каждого элемента и пользователя сегмента по прямой композиции параметров распознавания основу показателей, где N – этап воздействия.

Косвенная композиция параметров системы распознавания

Для формирования показателей $G_{M2,\ N}$ по косвенной композиции параметров распознавания необходимо установить все множество неявных (любых) взаимосвязей параметров в системе.

Физически информация о топологических взаимосвязях и взаимосвязях по персоналу представляется в виде отдельного для каждого типа списка взаимосвязей [7]:

$$g_{M2n,q,u,v} = g_{M1n,q,u,v} + \sum_{u=1}^{U}\sum_{v=1}^{V}\left(z_{u,v}(g)\cdot g_{M1n,q,u,v}\right),$$

где $z_{u,\ v}\ (g)$ – коэффициент, характеризующий глубину взаимосвязи рассматриваемого элемента с другими элементами топологии сегмента или с его сотрудниками.

Формирование результирующих показателей

Формирование моделей результирующих показателей G начнем со старших индексов. Для каждого из уровней реализации угроз нарушения конфиденциальности определим, соответственно, четыре типа моделей [7].

1) Модель для оценки показателя уровня угрозы для элемента топологии сегмента:

$$G_{9+U+v,N} = \sum_{u=1}^{U} G_{M1,N,n,q,u,v} \bullet$$

2) Модель для оценки показателя уровня угрозы для отдельного сотрудника сегмента:

$$G_{9+u,N} = \sum_{v=1}^{V} G_{M1,N,n,q,u,v} \bullet$$

3) Модель для оценки показателя уровня угрозы для каждого из шести этапов ее реализации:

$$G_{N+1} = \sum_{A=8}^{9+U+V} G_{A,N} \bullet$$

4) Модель для оценки обобщенного показателя уровня угрозы:

$$G_1 = \sum_{A=2}^{7} G_{A,N} \bullet$$

Оценка результирующих показателей

Оценка уровня угрозы безопасности на основе оценки обобщенного показателя уровня угрозы и показателей уровня угрозы для каждого из этапов ее реализации

Модели для оценки уровня угрозы безопасности на основе оценки обобщенного показателя уровня угрозы и показателей уровня угрозы для каждого из этапов ее реализации представлены в табл. 4.4.1. При этом колонка 2 таблицы соответствует уровню угрозы всего сегмента в целом, а колонки 3 – 8 – уровням угрозы на этапах 1 – 6, соответственно [7].

Таблица 4.4.1

№ п/п	Комбинация оценочных показателей							Оценка уровня угрозы конфиденциальности
1	2	3	4	5	6	7	8	9
1	1	1	1	1	1	1	1	$\overline{G} = \sum_{i=1}^{7} g_i$

№ п/п	Комбинация оценочных показателей							Оценка уровня угрозы конфиденциальности
1	2	3	4	5	6	7	8	9
2	1	1	0	1	1	1	1	$\overline{G} = \sum_{i=1}^{7} g_i - g_3$
3	1	1	1	1	1	1	0	$\overline{G} = \sum_{i=1}^{6} g_i$
4	1	1	0	1	1	1	0	$\overline{G} = \sum_{i=1}^{6} g_i - g_3$
5	1	1	0	1	0	0	0	$\overline{G} = M(g_1 \circ g_2 \circ g_4) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_2(y_{II} - y_I) \cdot f_4(y - y_{II}) dy_I \, dy_{II} dy$
6	1	0	1	0	1	0	0	$\overline{G} = M(g_1 \circ g_3 \circ g_5) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_3(y_{II} - y_I) \cdot f_5(y - y_{II}) dy_I \, dy_{II} dy$
7	1	0	0	1	0	1	0	$\overline{G} = M(g_1 \circ g_4 \circ g_6) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_4(y_{II} - y_I) \cdot f_6(y - y_{II}) dy_I \, dy_{II} dy$
8	1	0	0	0	1	0	1	$\overline{G} = M(g_1 \circ g_5 \circ g_7) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_5(y_{II} - y_I) \cdot f_7(y - y_{II}) dy_I \, dy_{II} dy$
9	1	1	0	0	0	1	0	$\overline{G} = M(g_1 \circ g_2 \circ g_6) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_2(y_{II} - y_I) \cdot f_6(y - y_{II}) dy_I \, dy_{II} dy$
10	1	0	1	1	0	0	0	$\overline{G} = M(g_1 \circ g_3 \circ g_4) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_3(y_{II} - y_I) \cdot f_4(y - y_{II}) dy_I \, dy_{II} dy$
11	1	0	0	1	1	0	0	$\overline{G} = M(g_1 \circ g_4 \circ g_5) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_4(y_{II} - y_I) \cdot f_5(y - y_{II}) dy_I \, dy_{II} dy$
12	1	0	0	0	1	1	0	$\overline{G} = M(g_1 \circ g_5 \circ g_6) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_5(y_{II} - y_I) \cdot f_6(y - y_{II}) dy_I \, dy_{II} dy$
13	1	0	0	0	0	1	1	$\overline{G} = M(g_1 \circ g_6 \circ g_7) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_6(y_{II} - y_I) \cdot f_7(y - y_{II}) dy_I \, dy_{II} dy$
14	1	1	0	0	0	0	1	$\overline{G} = M(g_1 \circ g_2 \circ g_7) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_2(y_{II} - y_I) \cdot f_7(y - y_{II}) dy_I \, dy_{II} dy$
15	1	1	1	0	0	0	0	$\overline{G} = M(g_1 \circ g_2 \circ g_3) = \int_0^{\infty} \int_0^{y} \int_0^{y_{II}} y \cdot f_1(y_I) \cdot f_2(y_{II} - y_I) \cdot f_3(y - y_{II}) dy_I \, dy_{II} dy$
16	1	1	0	0	0	0	0	$\overline{G} = M(g_1 \circ g_2) = \int_0^{\infty} y \int_0^{\infty} f_1(y - y_I) \cdot f_2(y_I) dy_I \, dy$

№ п/п	Комбинация оценочных показателей							Оценка уровня угрозы конфиденциальности
1	2	3	4	5	6	7	8	9
17	1	0	1	0	0	0	0	$\overline{G} = M(g_1 \circ g_3) = \int_0^\infty y \int_0^\infty f_1(y - y_{\text{I}}) \cdot f_3(y_{\text{I}}) dy_{\text{I}}\, dy$
18	1	0	0	1	0	0	0	$\overline{G} = M(g_1 \circ g_4) = \int_0^\infty y \int_0^\infty f_1(y - y_{\text{I}}) \cdot f_4(y_{\text{I}}) dy_{\text{I}}\, dy$
19	1	0	0	0	1	0	0	$\overline{G} = M(g_1 \circ g_5) = \int_0^\infty y \int_0^\infty f_1(y - y_{\text{I}}) \cdot f_5(y_{\text{I}}) dy_{\text{I}}\, dy$
20	1	0	0	0	0	1	0	$\overline{G} = M(g_1 \circ g_6) = \int_0^\infty y \int_0^\infty f_1(y - y_{\text{I}}) \cdot f_6(y_{\text{I}}) dy_{\text{I}}\, dy$
21	1	0	0	0	0	0	1	$\overline{G} = M(g_1 \circ g_7) = \int_0^\infty y \int_0^\infty f_1(y - y_{\text{I}}) \cdot f_7(y_{\text{I}}) dy_{\text{I}}\, dy$

Оценка уровня угрозы конфиденциальности на основе оценки показателя уровня угрозы для элемента топологии сегмента и показателя уровня угрозы для отдельного сотрудника сегмента

Модель для оценки уровня угрозы конфиденциальности на основе оценки показателя уровня угрозы для элемента топологии сегмента и показателя уровня угрозы для отдельного сотрудника сегмента аналитически представляется в виде:

$$\overline{G}_{ПТ} = M(G_{\text{П}} \circ G_{\text{Т}}) = \int_0^\infty y \int_0^\infty f_{\text{П}}(y - y_{\text{I}}) \cdot f_{\text{Т}}(y_{\text{I}}) dy_{\text{I}}\, dy .$$

5 Особенности реализации основных компонентов системы распознавания информационной безопасности на объекте информатизации

5.1. Структура системы распознавания угроз конфиденциальности информации сегментов ИКС

Структура разработанной в соответствии с предложенными алгоритмами и моделями распознавания угроз конфиденциальности информации сегментов ИКС системы распознавания [7] приводится на рис. 5.1.1.

Рис. 5.1.1. Структура системы распознавания угроз безопасности информации сегментов ИКС

Ниже приводится описание основных компонент разработанной системы.

Программная среда системы распознавания угроз

безопасности **информации сегментов ИКТС**

Программная среда системы распознавания угроз конфиденциальности информации сегментов ИКС предназначена для хранения, модификации, обработки и анализа всех данных вводимых и обрабатываемых в процессе функционирования сегмента ИКС. Данная среда является расширением существующей в сегменте среды СУБД, поддерживающей ИБД «Регион». В процессе функционирования системы распознавания угроз

конфиденциальности информации сегментов ИКС все операции с данными: их накопление, обработка, анализ производятся средствами выбранной СУБД [7]. Это позволяет избежать дополнительного внедрения в сегмент ИКС как единиц вычислительной техники для системы распознавания, так и дополнительного лицензионного программного обеспечения в серверной части сегмента ИКС.

5.3. Компонента формирования данных

Компонента формирования данных предназначена для хранения и модификации всех данных, вводимых и обрабатываемых в процессе функционирования системы распознавания [7]. Структура формируемых данной компонентой данных приводится на рис. 5.3.1.

Группа данных статических параметров системы распознавания угроз безопасности информации сегмента ИКС

Таблицы группы данных статических параметров системы распознавания угроз конфиденциальности информации сегмента ИКС содержат параметры базы данных для ее настройки и формирования непротиворечивой ключевой информации [7]. Формат такой таблицы соответствует табл. 5.3.1.

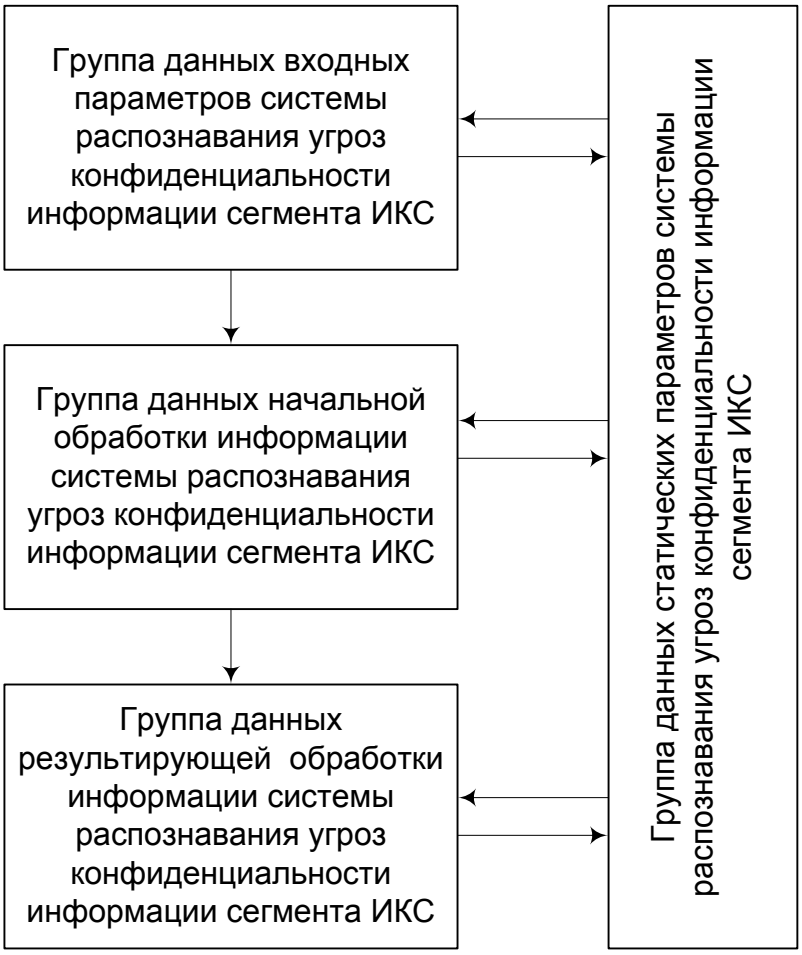

Рис. 5.3.1. Структура данных системы распознавания угроз безопасности информации сегментов ИКС

Таблица 5.3.1

Таблица параметров базы данных системы распознавания угроз безопасности информации сегмента ИКС

№ пп	Наименование параметра	Значение параметра

Формат списка ключевых параметров для информативных и идентификационных списков соответствует табл. 5.3.2 – 5.3.3.

Таблица 5.3.2

Список топологических элементов сегмента ИКС

№ пп	Наименование элемента топологии	Идентификатор топологии

Таблица 5.3.3

Список персонала сегмента ИКС

№ пп	Наименование персонала	Идентификатор персонала

Описание взаимосвязи топологии сегмента и его персонала представляется в виде таблицы взаимосвязи (табл. 5.3.4).

Таблица 5.3.4

Взаимосвязь в информативном списке

№ пп	Идентификатор топологии	Идентификатор персонала

5.3.2. Группа данных входных параметров системы распознавания угроз безопасности информации сегмента ИКС

Таблицы группы данных входных параметров системы распознавания угроз конфиденциальности информации сегмента ИКС содержат первичные параметры системы.

Имеется отдельная таблица для каждого из первичных параметров распознавания. В зависимости от вида параметра распознавания различают три

типа таблиц первичных параметров, формат которых представлен в табл. 5.3.5 - 5.3.7.

Таблица 5.3.5

Формат таблицы для параметров, определяющихся одним значением

№ пп	Время изменения	Значение параметра

Таблица 5.3.6

Формат таблицы для параметров, определяющихся идентификационным списком

№ пп	Идентификатор топологии	Время изменения	Значение параметра

Таблица 5.3.7

Формат таблицы для параметров, определяющихся информативным списком

№ пп	Идентификатор топологии	Идентификатор персонала	Время изменения	Значение параметра

5.3.3. Группа данных начальной обработки информации системы распознавания угроз безопасности информации сегмента ИКС

Группа данных начальной обработки информации системы распознавания угроз конфиденциальности информации сегмента ИКС представляется четырьмя формами: оперативных параметров, параметров их взаимосвязи, взаимосвязанных параметров и архива.

Оперативные значения первичных параметров (табл. 5.3.8) представлены актуальными показателями первичных параметров системы распознавания. В случае отсутствия одного из элементов значение соответствующего поля устанавливается в «0»

Таблица 5.3.8

Оперативная таблица первичных параметров системы

№ пп	Идентификатор топологии	Идентификатор персонала	Идентификатор параметра (таблицы параметра)	Значение параметра

Представленные, согласно, взаимосвязи первичных параметров (табл. 5.3.9) учитывают взаимосвязи между значениями оперативных первичных параметров и в совокупности с данными табл. 5.3.8 формируют массив взаимосвязанных параметров (табл. 5.3.10).

Таблица 5.3.9

Параметры взаимосвязи параметров

№ пп	Идентификатор параметра 1 (таблицы параметра)	Идентификатор параметра 2 (таблицы параметра)	Тип взаимосвязи	Коэффициент взаимосвязи

Таблица 5.3.10

Таблица взаимосвязанных параметров

№ пп	Идентификатор топологии	Идентификатор персонала	Идентификатор параметра (таблицы параметра)	Значение параметра

При внесении изменений в таблицу 5.3.8 прежде, чем изменяется информация в табл. 5.3.10, ее содержимое переносится в таблицу вида табл. 5.3.11.

Таблица 5.3.11

Информация из устаревших таблиц взаимосвязанных параметров

№ пп	Время актуальности	Идентификатор топологии	Идентификатор персонала	Идентификатор параметра (таблицы параметра)	Значение параметра

5.3.4. Группа данных результирующей обработки информации системы распознавания угроз безопасности информации сегмента ИКС

Таблицы группы данных результирующей обработки информации [7] системы распознавания угроз безопасности информации сегмента ИКС содержат список итоговых показателей системы, полученный на основе данных табл. 5.3.10 и моделей п. 4.1.1 – 4.1.5.

Таблица 5.3.12

Список итоговых показателей

№ пп	Идентификатор итогового показателя	Значение показателя

При изменении значения любого показателя из табл. 5.3.12 информация из табл. 5.3.12 переносится в таблицу вида табл. 5.3.13.

Таблица 5.3.13

Список устаревших итоговых показателей

№ пп	Время актуальности	Идентификатор итогового показателя	Значение показателя

Для контроля уровня угрозы конфиденциальности информации: от топологических элементов сегмента ИКС, от персонала сегмента, при реализации конкретного этапа противоправных действий и общего показателя угрозы определен список пороговых значений итоговых показателей распознавания такого рода угроз. Данный список представляется в формате табл. 5.3.14.

Таблица 5.3.14

Список пороговых значений итоговых показателей

№ пп	Интервал актуальности	Идентификатор итогового показателя	Значение порогового показателя

5.4. Компонента регистрации событий

Компонента регистрации событий предназначена для идентификации входящих в систему распознавания запросов к ее СУБД [7]. Ниже приводится классификация типовых запросов.

1. Добавление пользователя в систему.
2. Добавление в систему топологического элемента.
3. Изменение коэффициента взаимосвязи между параметрами.
4. Изменение значения контролируемого параметра.
5. Превышение итоговым показателем порогового значения.
6. Изменение порогового значения.

5.5. Компонента обработки событий

Компонента обработки событий реализует следующие функции [7]:

1. Добавление пользователя в систему.

В табл. 5.3.3, 5.3.4 и 5.3.8 происходит добавление записей.

2. Добавление в систему топологического элемента.

В табл. 5.3.2, 5.3.4 и 5.3.8 происходит добавление записей.

3. Изменение коэффициента взаимосвязи между параметрами.

В табл. 5.3.9 происходит изменение записей.

4. Изменение значения контролируемого параметра.

Обновляется одна из таблиц одного, изменяющегося параметра. Из табл. 5.3.1 получаем время актуальности для табл. 5.3.8. Информацию из табл. 5.3.10 переносим в табл. 5.3.11 с временем актуальности, соответствующим времени актуальности табл. 5.3.8. Вычисляем новые актуальные значения в таблице 5.3.10. Информацию из табл. 5.3.12 переносим в табл. 5.3.13 с временем актуальности табл. 5.3.8. Вычисляем новые значения табл. 5.3.12. Изменяем значение времени актуальности табл. 5.3.8 в табл. 5.3.1 в соответствии с временем изменения контролируемого параметра. Проверяем наступление

события 5 из списка событий.

5. Превышение итоговым показателем порогового значения.

Проводится сравнение полученных итоговых показателей из табл. 5.3.14 с значениями табл. 5.3.13.

6. Изменение порогового значения.

В табл. 5.3.14 происходит изменение записей.

7. Реакция системы на превышение итогового показателя.

Предоставляется информация:

– О факте превышения уровня угрозы конфиденциальности информации сегмента ИКС.

– Об элементах топологии, где подозревается превышение уровня угрозы конфиденциальности информации сегмента ИКС.

– О персонале сегмента, который показал повышение уровня угрозы конфиденциальности информации сегмента ИКС.

– О предполагаемом этапе (этапах) реализации угрозы конфиденциальности информации сегмента ИКС.

5.6. Компонента идентификации угрозы

Компонента идентификации угрозы [7] формируется на основании полученных показателей и должна учитывать циклы работы ИКС ОВД, такие как суточные, месячные, квартальные, годовые и т.п.

Для элемента топологии и персонала следует использовать пороговые значения, получаемые как результат анализа полученных результатов, в первые 2+ цикла работы системы.

При выявлении превышения пороговых уровней необходимо выявлять причины такого превышения и при их объективности принимать решение о внесении в цикл увеличенных пороговых значений для данного элемента/-ов как топологии, так и персонала.

ЗАКЛЮЧЕНИЕ

Реализация системы, предлагаемая в рекомендациях, имеет достаточно гибкие возможности. Все приведенные функции и параметры могут вводиться в систему поэтапно и даже независимо друг от друга. Соответственно при возникновении дополнительных механизмов аудита и контроля информационной безопасности они также могут войти в пул параметров системы распознавания. Единственное условие – необходимо четко представлять цель события, которое контролируется, для правильного внесения в нижний уровень декомпозиции угрозы. При выполнении этого условия необходимо и достаточно провести минимальные изменения моделей обобщения результатов путем добавления в массив обработки еще одного параметра. Это позволит предложенную типовую модель декомпозиции угрозы привести в соответствие динамически развивающемуся процессу как реализации угроз конфиденциальности, так и противодействия такой реализации.

Для минимального набора контроля информационной безопасности можно применить механизмы обработки информации на сервере СУБД на объекте информатизации, последующий этап – механизмы обработки на клиентских машинах пользователей и завершающий этап – механизмы контроля каналов связи (современные маршрутизаторы позволяют выполнять такие действия без дополнительных технических средств). Для наиболее полного охвата добавляются данные вводимые специалистами (например, по оперативной информации о нарушени информационной безопасности и т.п.).

Хочется отметить, что при достаточном вычислительном ресурсе серверов СУБД реализация системы не требует дополнительного технического обеспечения.

Все вышеизложенное определяет возможность практической реализации предлагаемой системы.

СПИСОК ИСПОЛЬЗОВАННЫХСТОЧНИКОВ

1 Об особенностях некоторых оснований при классификации угроз нарушения целостности информации в информационно-телекоммуникационных системах / С.В. Скрыль [и др.] // Информация и безопасность. – Воронеж: ВГТУ, 2010. – Вып. 2. – С. 247 – 250.

2 Классификационные основания для систематизации угроз информационной безопасности информационной сферы / В.В. Киселев [и др.] // Информация и безопасность. – Воронеж: ВГТУ, 2011. – Вып. 3. – С. 451 – 454.

3 Киселев В.В. Структурированность идентифицирующих признаков воздействий угроз информационной безопасности как фактор повышения эффективности их распознавания / В.В. Киселев // Информация и безопасность. – Воронеж: ВГТУ, 2009. – Вып. 1. – С. 155 – 156.

4. Системный анализ и его приложения: учебное пособие / под ред. В.Н. Буркова. – Воронеж: Научная книга, 2008. – 439 с.

5 Месарович М. Теория иерархических многоуровневых систем / М. Месарович, Д. Мако, И. Такахара – М.: Мир, 1973. – 344 с.

6 CASE: Структурный системный анализ (автоматизация и применение) / Г.Н. Калянов. – М.: Лори, 1996. – 242 с.

7. Киселев В.В. Распознавание и оценка угроз информационной безопасности территориальным сегментам единой информационно-телекоммуникационной системы органов внутренних дел: теоретические и организационно-методические основы: монография / В.В. Киселев. – Воронеж: Воронежский институт МВД России, 2012. — 160 с. — ISBN 975-5-88591-053-8