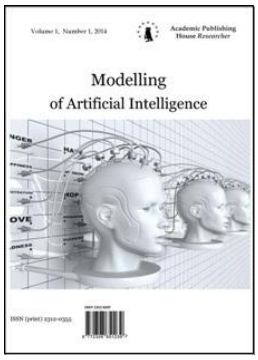

Published in the Russian Federation
Modeling of Artificial Intelligence
Has been issued since 2014.
ISSN: 2312-0355
E-ISSN: 2413-7200
Vol. 11, Is. 3, pp. 166-176, 2016

DOI: 10.13187/mai.2016.11.166
www.ejournal11.com

UDC 681.3

Creating the Conditions for the Theoretical and Practical Solution of the Problem of Automated Intelligent Search for the Attacker's Image in ADPS

Simon Zh. Simavoryan [a, *], Arsen R. Simonyan [a], Elena I. Ulitina [a], Irina L. Makarova [a], Rafik A. Simonyan [b]

[a] Sochi State University, Russian Federation
[b] Kuban State University, Russian Federation

Abstract

The work is devoted to developing methods for the automated processing of information based on specialized knowledge of the malicious actions (templates) and a knowledge base of regular situations and values their allowable characteristics, in order to detect intruders and malicious acts of automated data processing systems (ASPS).

Keywords: malicious antagonism mechanisms and data protection services, signature methods, methods of detection of anomalies.

1. Введение

В соответствии с Доктриной информационной безопасности Российской Федерации, важнейшими составляющими технологий информационной безопасности являются средства противодействия компьютерным атакам на автоматизированные системы различного класса и назначения (Российская газета. 2000. 28 сентября). Разработке средств и методов противодействия компьютерным атакам уделяется большое внимание (Симаворян, Симонян и др., 2014; Васильев, 2013; Марков, Фадин, 2013). В работах (Симаворян, Симонян и др., 2014, Васильев, 2013) исследованы актуальные направления научных исследований в области обеспечения информационной безопасности – разработка методов и моделей

обнаружения атак злоумышленников на АСОД. В работе (Симаворян, Симонян и др., 2014) использован системный подход к проектированию интеллектуальных систем защиты информации, а также проведен обзор возможностей применения таких методов как: многоагентный подход, генетические алгоритмы, нейронные сети и иммунные системы. В связи с тем, что злоумышленник постоянно совершенствует методы вторжения, и как следствие получения, извлечения и модификации информации, проблема противоборства злоумышленников и службы защиты информации может быть решена при условии достаточности информации о намерении совершения злоумышленных действий. Следует задать вопрос: сколько надо информации службе защиты информации для предотвращения потенциально возможных угроз? Чтобы целенаправленно подойти к решению поставленного вопрос воспользуемся классическим понятием информационного кадастра в работе (Герасименко, 1996). Поиск нечеткого образа злоумышленника является неотъемлемой частью интеллектуальной деятельности службы защиты информации.

Поэтому разработка, автоматизированного поиска образа интеллектуального злоумышленника в сетях АСОД является актуальной и насущной задачей.

2. Обсуждение

Чтобы практически верно подойти к решению рассматриваемого вопроса, необходимо ввести такие понятия как: информационные потребности злоумышленника и информационные потребности службы защиты информации. Под информационными потребностями злоумышленника будем понимать совокупность тех сведений (данных), которые необходимы для несанкционированного вторжения, получения и модификации информации в АСОД. Под информационными потребностями службы защиты информации будем понимать совокупность тех сведений (данных), которые необходимы для регулярного обеспечения безопасного функционирования системы защиты информации.

Приведем следующее определение (Герасименко, 1996): под информационным кадастром будем понимать полную и хорошо структурированную совокупность данных, необходимых и достаточных для эффективного функционирования системы защиты информации с целью организации эффективного противоборства. Информационный кадастр объекта удобно представлять в виде упорядоченной совокупности так называемых объективно-характеристических таблиц (ОХТ). ОХТ в информационной безопасности представляет собой таблицу в строках которой находятся наименования тех элементов (предметов, событий, явлений), которые относятся как полю злоумышленников, так и к полю деятельности службы защиты, а по столбцам – наименования тех характеристик учитываемых элементов, значения которых необходимы для информационного обеспечения деятельности злоумышленников и службы защиты информации.

На рис. 1 приводится предложенная структура ОХТ информационной безопасности, включающая в себя следующие блоки: классификационный словарь понятий, специализированную базу знаний о злоумышленных действиях (шаблоны), базу знаний о штатных ситуациях и значений их допустимых характеристик и базу сообщений.

Приведем следующие определения (Васильев, 2013):

1) под системой обнаружения атак (СОА) понимаются системы,

собирающие информацию из различных точек защищаемой АСОД и анализирующие эту информацию с целью выявления как попыток нарушения, так и реальных нарушений защиты (вторжений);

2) атака – событие, при котором злоумышленник пытается получить

несанкционированный доступ к ресурсам АСОД или нарушить её нормальное функционирование.

Рис. 1. Структура ОХТ информационной безопасности

Модель действий злоумышленника включает в себя следующие этапы:

1-ый этап – сбор информации об объекте атаки; 2-ой этап – НСД к компонентам атаки; 3-ий этап – сокрытие следов и долговременное присутствие.

Основными методами, используемыми для выявления атак являются: методы сигнатурного анализа (Васильев, 2013; Марков, Фадин, 2013; Борисов, Шабуров, 2015; Сидельников, 2010) и методы обнаружения аномалий (Васильев, 2013; Шелухин и др., 2013; Сидельников, 2010; Микова, 2015; Басараб, Строганов, 2014).

Сущность методов сигнатурного анализа заключается в следующем: в основе этих методов лежит предположение о том, что атаку можно описать с помощью определенного набора правил, или алгоритма, или некоторой формальной модели. Обнаружение атак (злоумышленных действий) сводится к сравнению текущих действий пользователя, или входящего (исходящего) трафика с заданными сигнатурами (шаблонами) атак, хранящимися в специализированной базе знаний. Сигнатурные методы описывают каждую атаку особой моделью или сигнатурой, однако эти методы имеют один недостаток – невозможность обнаружения атак, сигнатуры которых пока не определены. Так с помощью сигнатур специализированной базы знаний о злоумышленных действиях можно успешно рассчитать формулы вероятностей НПИ приведенных в работе (Симаворян, 2009), где приводится следующая формула вероятности несанкционированного получения информации НПИ одним нарушителем γ-ой категории по *i*-му КНПИ в ℓ-ой зоне *j*-го типового структурного компонента (ТСК) АСОД в условиях неопределенности:

$P_{ij\gamma\,\ell}^{\text{НПИ}}=\left(1-P_{j\gamma\,\ell}^{\text{пд}}\right)\mu_B^{\gamma\ell}\left(1-P_{ij\,\ell}^{\text{пн}}\right)\mu_A^{ij\ell}\left(1-P_{ij\,\ell}^{\text{ннпи}}\right)\left(1-P_{ij\,\ell}^{\text{лок}}\right)\left(1-P_{ij\,\ell}^{\text{лик}}\right)P_{ij\gamma\,\ell}^{\text{и}}$, где $P_{j\gamma\ell}^{\text{пд}}$ – вероятность предупреждения доступа злоумышленника γ-ой категории в ℓ-тую зону защиты *j*-го типового структурного компонента (ТСК) АСОД; $P_{ij\ell}^{\text{пн}}$ - вероятность предупреждения наличия *i*-го КНПИ в ℓ-ой зоне защиты информации *j*-го ТСК АСОД; $P_{ij\ell}^{\text{ннпи}}$ - вероятность предупреждения НПИ при -наличии *i*-го канала в ℓ-ой зоне защиты *j*-го ТСК; $P_{ij\gamma\ell}^{\text{и}}$ - вероятность наличия информации в момент доступа злоумышленника γ-ой категории к *i*-му КНПИ в ℓ-ой зоне *j*-го ТСК; $P_{ij\ell}^{\text{лок}}$ - вероятность локализации НПИ в *i*-ом канале НПИ в ℓ-ой зоне *j*-го ТСК; $P_{ij\ell}^{\text{лик}}$ - вероятность ликвидации последствий НПИ в ***i*** -ом канале в ℓ-ой зоне *j*-го ТСК, $\mu_B^{\gamma\ell}$ - степень принадлежности γ-го злоумышленника нечеткому множеству потенциально возможных злоумышленников В (в ℓ-ой зоне), $\mu_A^{ij\ell}$ - степень принадлежности ***i***-го канала нечеткому множеству потенциально возможных КНПИ (в ℓ-ой зоне **j**-го ТСК). Эта вероятность названа базовой вероятностью и обозначена как $P^{\text{б}}$. Вероятность НПИ при некоторой $\{i^*\}$ совокупности КНПИ, некоторой $\{j^*\}$ совокупности ТСК и некоторой $\{\gamma^*\}$ совокупности нарушителей определяется как

$P_{\{i^*\}\{j^*\}\{\gamma^*\}} = 1-\prod_{\{i^*\}}P_{ij\gamma}^{\text{б}}\prod_{\{j^*\}}P_{ij\gamma}^{\text{б}}\prod_{\{\gamma^*\}}P_{ij\gamma}^{\text{б}}$.

Однако с помощью шаблонов не всегда достоверно удается обнаружить злоумышленника, поскольку злоумышленник постоянно совершенствует свои методы скрытого несанкционированного получения информации. Поэтому необходимо использовать методы обнаружения аномалий сетевого трафика (Васильев, 2013; Шелухин и др., 2013; Сидельников, 2010; Микова, 2015; Басараб, Строганов, 2014). Следует отметить, что для организации системной защиты информации необходимо методы обнаружения аномалий расширить на все подсистемы защиты информации, приведенные в работе (Симаворян, Симонян и др., 2014) (таблица 1).

Таблица 1. Классификация подсистем противодействия злоумышленнику

Признаки классификации		Зоны защиты				
		Внешняя	Территории	Помещений	Ресурсов	Базы данных
Подсистемы противодействия злоумышленнику	Предупреждения доступа в зону	Блок ПД-1/1	Блок ПД-1/2	Блок ПД1/3	Блок ПД-1/4	Блок ПД-1/5
	Предупреждения наличия канала в зоне	Блок ПН-2/1	Блок ПН-2/2	Блок ПН-2/3	Блок ПН-2/4	Блок ПН-2/5
	Предупреждения наличия информации в канале в момент доступа к нему злоумышленника	Блок ПНИ-3/1	Блок ПНИ-3/2	Блок ПНИ-3/3	Блок ПНИ-3/4	Блок ПНИ-3/5
	Локализации НПИ	Блок Л-4/1	Блок Л-4/2	Блок Л-4/3	Блок Л-4/4	Блок Л-4/5
	Ликвидации последствий НПИ	Блок ЛП-5/1	Блок ЛП-5/2	Блок ЛП-5/3	Блок ЛП-5/4	Блок ЛП-5/5

Из таблицы видно, что:

- подсистемы противодействия злоумышленным действиям удобно делить по зонам защиты информации на блоки. При этом следует в каждом блоке учитывать модели противодействия относительно одного или нескольких злоумышленников одного определенного класса, нескольких злоумышленников в совокупности различных классов и всего множества злоумышленников;
- структура ОХТ должна быть разработана в соответствии с блоками защиты информации, приведенными в таблице 1;
- методы сигнатурного анализа и методы обнаружения аномалий должны быть привязаны к блокам информационной безопасности.

Сущность методов обнаружения аномалий заключается в том, что СОА обладает некоторым набором знаний о нормальном (штатном) поведении злоумышленника или характере сетевых подключений. Любые отклонения от этого профиля расцениваются как аномальное поведение пользователя. После обнаружения этой аномалии и оценки степени ее опасности принимается решение о том, что это атака, или данное отклонение допустимо.

В настоящее время, ведутся работы по совместному использованию методов сигнатурного анализа и методов обнаружения аномалий сетевого трафика или действий пользователя (Васильев, 2013).

В рамках данной статьи рассмотрим некоторые практические аспекты автоматизированного поиска нечеткого образа злоумышленного действия. Вопросам разработки программных комплексов обнаружения атак уделяется большое внимание

(Тищенко, 2013; Чурилина, 2012). В этом направлении выделим следующие методы и модели практической реализации поиска нечеткого (размытого) образа злоумышленника (злоумышленного действия): 1) модель представления данных о злоумышленных действиях, построенная с использованием специализированной базы знаний о злоумышленных действиях (шаблонов); 2) алгоритмы первоначального поиска нечеткого злоумышленника; 3) алгоритм итеративного повышения функциональной эффективности поиска; 4) эвристический метод разработки оперативного оптимального плана исследования множества злоумышленных действий, основанный на анализе нечеткого образа злоумышленных действий на базе знаний о штатных ситуациях и значений их допустимых характеристик.

В данной статье исследованы первые два аспекта.

Модель представления данных о злоумышленных действиях, построенная с использованием специализированной базы знаний о злоумышленных действиях (шаблонов).

Наиболее приемлемый и естественный способ представления данных о злоумышленных действиях является способ представления данных в виде информационного кадастра. Нетрудно видеть, что разработка структуры информационного кадастра должна осуществляться в следующей последовательности: 1) на основе анализа целей злоумышленника составляется наиболее точный список всех возможных злоумышленных действий по каждому из каналов несанкционированного получения информации; 2) составленный список классифицируется на однородные группы для каждого класса из злоумышленников в отдельности, причем основным критерием однородности должны быть идентичность характеристик злоумышленных действий; 3) для каждой группы злоумышленников составляется перечень характеристик, по которым должны собираться сведения о них; 4) для всех групп устанавливаются их взаимосвязи, на основе чего и строится упорядоченная структура всех ОХТ. При таком представлении информационного кадастра обеспечиваются хорошие условия для автоматизированного поиска нечеткого образа злоумышленных действий. Эти таблицы составляют основу как специализированной базы знаний о злоумышленных действиях (шаблоны), включая знания о штатных ситуациях, и значения их допустимых характеристик. Таблицы строятся по принципу объект-признак.

Под признаком f_i понимается некоторое отображение множества объектов U в F_i , ставящее в соответствие каждому объекту u_j значение $f_i(u_j)$, принадлежащее множеству значений признака f_i. Признаки могут выражать различные типы данных об объектах злоумышленных действий. Признаки принято классифицировать на следующие типы: количественные (численные), качественные (лингвистические) и ранговые.

Количественные признаки могут принимать непрерывные или дискретные действительные значения, например, количество КНПИ в зоне защиты информации, количество используемых средств защиты при закрытии канала, стоимость средства защиты и т.д.

Качественные (лингвистические) признаки позволяют разбивать злоумышленные действия на неподдающиеся упорядочению группы злоумышленных действий по каждому из значений признаков. Так, например, признак выражающий вероятность злоумышленных действий, может принимать значения «невероятно», «маловероятно», «вероятно», «весьма вероятно», «несомненно», признак характеризующий надежность функционирования средств защиты информации, может принимать значения «не надежный», «мало надежный», «надежный», «весьма надежный», «несомненно надежный». Качественные признаки могут быть альтернативными и неальтернативными. Признак называется альтернативным, если всякому конкретному злоумышленному действию может соответствовать либо одно значение признака, либо отсутствовать информация о значении признака. Неальтернативные признаки могут принимать одновременно несколько значений из множества значений F. Любые неальтернативные признаки можно преобразовать в альтернативные путем соответствующего расширения множества значений F. Специфическим видом качественных признаков являются дихотомичесие (иначе булевые или бинарные) признаки, множество значений которых состоит из 2-х значений, например,

0 и 1. Каждый качественный признак f_i , имеющий m_i значений, можно с помощью процедуры дихотомизации заменить m_i дихотомическими признаками f_i^j, j=1,2,..., m_i , где f_i^j=1, если f_i принимает j-тое значение из множества F_i и f_i^j=0 – в противном случае. Для альтернативных качественных признаков f_i справедливо, что для любого i, l существует j , для которого $f_i^j(u_l)$=1 , где $f_i^j(u_l)$- значение, которое принимает дихотомический признакf_i^j у объекта u_l .

Дихотомическое деление признаков, характеризующих объекты информационной безопасности привлекательно тем, что мы всегда имеем дело лишь с двумя классами, которые исчерпывают объём делимого понятия. Таким образом, дихотомическое деление всегда соразмерно; члены деления исключают друг друга, так как каждый объект делимого множества попадает только в один из определенных классов злоумышленных действий ***Q*** или *не* ***Q***; деление проводится по одному основанию - наличие или отсутствие некоторого признака. Обозначив делимое понятие буквой ***Q*** и выделив в его объёме некоторый подвид, скажем, ***R***, можно разделить объём ***Q*** на две части – ***R*** и *не* ***R***.

Дихотомическое деление имеет недостаток, например, если разделить специалистов АСОД на не злоумышленников и *злоумышленников*, то вторая группа оказывается весьма неопределенной. Кроме того, если в начале дихотомического деления обычно довольно легко установить наличие противоречащего понятия, то по мере удаления от первой пары понятий найти его становится всё труднее.

Ранговые (иначе порядковые) признаки позволяют упорядочивать объекты по степени появления какого-либо качества, не фиксируя более глубоких соотношений между значениями признаков. В таком понимании ранговые признаки понимаются как лингвистические переменные. Авторы придерживаются того мнения, что при анализе данных, связанных со злоумышленными действиями целесообразно оперировать ранговыми признаками как качественными (лингвистическими).

В задачах противодействия злоумышленников и службы защиты информации чаще всего приходится сталкиваться с ситуациями, когда исследуемые объекты заданы наборами разнородных признаков, часть которых может быть выражена численно, а часть носит лингвистический или ранговый характер. В дальнейшем изложении мы буде предполагать, что признаки описывающие объекты, предварительно преобразуются в лингвистические переменные, и только после этого производится дихотомизация полученных качественных признаков.

Таким образом, в задачах противоборства злоумышленников и службы защиты информации согласно предполагаемой модели исходные эмпирические данные ОХТ представляются в виде блочной матрицы

$X=(X_1, X_2, \dots, X_k)$

размерности n*m, которая состоит из k субматриц X_j размерности n*m_j, где

n – общее число образов объектов в базе знаний о злоумышленных действиях;

m_j - число значений, получаемых качественным признаком (с учетом значения «нет информации о злоумышленных действиях»);

m - общее число дихотомических признаков описываемых объектов;

k - число дихотомизированных качественных признаков, описывающих объект.

Каждая субматрица X_j соответствует дихотомизированному качественному признаку f_j и является булевой матрицей с m_j ортогональными столбцами, причем сумма этих столбцов дает столбец, все компоненты которого равны единице; каждый столбец отвечает отдельному значению признака, так что элемент (i,l) субматрицы X_j равен единице в том и только в том случае, когда признак j у объекта u_i принимает l -ое значение, и равен 0 в противном случае. В каждой строке субматрицы X_j содержится одна и только одна единица, т.е. признак f_j задает разбиение на множестве объектов.

Алгоритм автоматизированного весового поиска нечеткого образа злоумышленника

Сущность весового поиска заключается в том, что запрос на поиск нечеткого образа злоумышленника, ассоциирующимся со злоумышленными действиями в виде атаки на АСОД, задается в виде описания значений признаков некоторого объекта с известными

шаблонами (сигнатурами) атак, хранящимися в специализированной базе знаний. При весовом поиске каждому образу, далее будем подразумевать или атаки, или злоумышленному действию, из архива на основе анализа совпадения значений описываемых его признаков и значений признаков в запросе ставится в соответствие некоторое действительное число, выражающее степень формальной релевантности этого образа, или шаблона, запросу. Этот метод поиска нечеткого образа злоумышленных действий называется весовым, так как он учитывает так называемые «веса», отражающие значимость (информативность) признаков и их значений. Заметим, что уже сам выбор признаков службой защиты информации, описывающих шаблоны (сигнатуры), есть не что иное как субъективное взвешивание, при котором признаки, не нашедшие отражение в образах объектов, был приписан маленький вес. Для весового поиска образа атаки необходимо решение следующих задач: задачи вычисления весов признаков и их значений и задачи определения степени соответствия образов объектов запросу по известным весам.

Анализ методов вычисления весов показывает, что можно выделить следующие основные пути вычисления весовых оценок значимости: а) экспертный опрос; б) на основе средней информации, даваемой признаком или его значением о некоторых группах объектов; в) на основе средней информации, даваемой признаком или его значением о всей совокупности признаков, описывающих объекты; г) на основе средней информации, даваемой признаком или его значением о значениях некоторых других, так называемых выходных признаках (частный случай б), поскольку каждой комбинации значений выходных признаков можно поставить в соответствие группу объектов, описываемых этой комбинацией). Мы будем пользоваться вторым путем, т.е. будем подразумевать, что исходное множество образов злоумышленных действий может быть разбито на несколько групп по правилам составления информационного кадастра злоумышленных действий. Группы могут быть непересекающимися и однородными.

Как уже отмечалось, группы могут быть получены также, если некоторые признаки будут помечены пользователем как выходные признаки. В этом случае каждой комбинации значений выходных признаков ставится в соответствие одна группа злоумышленников.

Далее при изложении методов вычисления весов будем предполагать, что архив разбит на q групп $G_1, G_2, \dots, G_q$, причем $G_1 \vee G_2 \vee \dots \vee G_2 =$ U, а $G_i \wedge G_j \neq \emptyset$, при i≠j, т.е. предполагаем, что не обязательно является пустым. Тогда для каждого лингвистического(качественного) признака f_i можно построить таблицу соответствия (рис.), строки которой соответствуют m_i значениям лингвистического признака f_i, а столбцы группам G_j, j=1,2,...,q. Элемент таблицы соответствия лежащий на пересечении -той строки и j-го столбца $a_i^{l,j}$, выражает число образов объектов, относящихся к классу G_j и описываемых l-тым значением качественного признака f_i.

Обозначим $\sum_{j=1}^{q} \alpha_i^{\ell,j}$ через $\alpha_i^{\ell,0}$, а $\sum_{l=1}^{m_i} \alpha_i^{\ell,j}$ через $\alpha_i^{0,j}$, индекс i опущен, так как $\alpha^{0,j}$ выражает число образов в классе G_j и не зависит от i).

Вес ℓ-го значения i-го признака будем обозначать через λ_i^{ℓ} , а вес i-го признака через λ_i.

Элементы сопряжения	G_1	G_2	…	G_j	…	G_q	$\sum$
f_i^1							
f_i^2							
…	…		…				
f_i^l				$\alpha_i^{l,j}$			$\alpha_i^{l,0}$
…							
$f_i^{m_i}$							
$\sum$				$\alpha_i^{0,j}$			

Рис. 2. Таблица сопряженности групп G_1, G_2,..., G_q и значений лингвистических значений признака f_i

Рассмотрим несколько методов вычисления весов значений признаков λ_i^j.

Метод 1. Предварительно производится сравнение, насколько отличаются частоты (вероятности, или другие признаки) встречаемости образов злоумышленных действий объектов групп G_j , j=1,2,...,q в специализированной базе знаний о злоумышленных действиях (шаблоны) от вероятности встречаемости образов злоумышленных действий объектов из групп G_j , j=1,2,...,q в имеющейся и динамически формируемой базе знаний о штатных ситуациях и значений их допустимых характеристик, у которых признак f_i принимает l –ое значение. Если эти вероятности не отличаются, то это значит, что l –ое значение признака f_i не информативно. Имеется ввиду, что информативность тем выше, чем больше разность между вероятностями. Тогда для вычисления веса λ_i^l можно использовать формулу среднеквадратичного отклонения q–го членного ряда величин, показывающих степень различия между рассматриваемыми вероятностями (Попов, 2010; Боровиков, 2003).

$$\lambda_i^l = \sqrt{\frac{\sum_{j=1}^{q}\left(\frac{\alpha_i^{l,j}*n}{\alpha_i^{l,0}*d^{0,j}} - \sum_{t=1}^{q}\frac{\alpha_i^{l,t}*n}{\alpha_i^{l,0}*\alpha^{0,t}*q}\right)^2}{q}}$$

Метод 2. Во втором методе вычисления λ_i^l , используется формула

$$\lambda_i^l = \sum_{j=1}^{q}\frac{\alpha_i^{l,j}}{\alpha_i^{l,0}} * \log_2\frac{\alpha_i^{l,j}*n}{\alpha_i^{l,0}*\alpha^{0,j}},$$

Эта формула отличается от предыдущего тем, что непосредственно учитывает таrже вероятность (частоту) встречаемости образов злоумышленных действий из групп G_j , j=1,2,...,q в множестве образов злоумышленных действий, для которых $f_i^l = 1$.

Метод 3. Метод конструирования агрегированных показателей (Миркин, 1980; Шашина, 1999).

Агрегированные показатели конструируются для некоторой группы злоумышленных действий и их признаков, в случаях, когда степень сходства между различными значениями одних качественных признаков достаточно высокая. Агрегированные показатели конструируются для групп объектов G_j, данные о которой представлены в виде блочной матрицы, построенной по правилам построения ОХТ:

$$X^j = \left(X_1^j, X_2^j, \dots, X_r^j\right),$$

Агрегированные показатели ищутся в виде $\alpha_i^{0,j}$-мерного единичного вектора Z (см. рис. 1), который наиболее сходен с матрицами X_t^j.

В этом случае становится целесообразным использование формулы, учитывающей значение степени сходства. В качестве примера можно привести формулу

$$\boldsymbol{\mu}(\boldsymbol{u_i}) = \sum_{j=1}^{k}\sum_{l=1}^{m_k}\left(\lambda_j^l * \sum_{s=1}^{m_k} f_j^s(u_i) * \sigma_j^{l,s}\right),$$

где $\boldsymbol{\sigma_j^{l,s}}$ выражает степень сходства между l –ым и s –ым значениями j –го качественного признака.

3. Результаты

Разработана модель представления данных о злоумышленных действиях.

Разработан алгоритм автоматизированного весового поиска нечеткого образа злоумышленника.

4. Заключение

В данной статье решение общей задачи противоборства злоумышленников и службы защиты информации рассмотрено в плане заблаговременного обнаружения злоумышленного действия – атаки. При рассмотрении общей задачи на базе системного подхода была выделена частная задача по созданию условий для теоретического и практического решения автоматизированного поиска образа интеллектуального злоумышленника в АСОД, т.е. в зоне базы данных. Основными методами, используемыми

для выявления атак являются: методы сигнатурного анализа и методы обнаружения аномалий. Для реализации этих методов необходимо построить соответствующие ОХТ. Сущность поиска нечеткого образа злоумышленника, ассоциируется со злоумышленными действиями в виде атак на АСОД, которые задаются в виде описания значений признаков злоумышленных действий виде шаблонов (сигнатур) атак. Для поиска нечеткого образа злоумышленных действий был предложен весовой подход, который дает возможность организации первоначального поиска образа злоумышленника с точки зрения определения степени соответствия этого образа шаблонам в специализированных базах знаний о злоумышленных действиях и в базах знаний о штатных ситуациях и значений их допустимых характеристик.

Благодарности
Работа поддержана грантом РФФИ 16-01-00527

Литература

Российская газета. 2000. 28 сентября – Доктрина информационной безопасности Российской Федерации [Текст] [Утверждена Указом Президента Российской Федерации от 9 сентября 2009 года №ПР-1895] // Российская газета. 2000. 28 сентября.

Симаворян, Симонян и др., 2014 – Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян А.Р. Исследование интеллектуального противоборства злоумышленников и службы защиты информации в АСОД. // Известия СГУ, 2014, № 4-1 (32). С. 15-23.

Васильев, 2013 – Васильев В.И. Интеллектуальные системы защиты информации: учеб. пособие В.И. Васильев. 2-изд. М.: Машиностроение, 2013. 172 с.

Герасименко, 1996 – Герасименко В.А. Основы информационной грамоты. М.: Энергоатомиздат, 1996. 320 с.

Симаворян, 2009 – Симаворян С.Ж. Аналитическая модель определения показателя уязвимости информации в автоматизированных системах обработки информации (АСОД) // Обозрение прикладной и промышленной математики, том 16, выпуск 6. Ред. Ю.В. Прохоров. М.:ООО Редакция журнала «ОПиПМ», 2009.

Марков, Фадин, 2013 – Марков А.С., Фадин А.А. Статический сигнатурный анализ безопасности программ // Программная инженерия и информационная безопасность. 2013. № 1. С. 50-56.

Борисов, Шабуров, 2015 – Борисов В.И., Шабуров А.С. О применении сигнатурных методов анализа информации в siem-системах // Вестник УрФО. Безопасность в информационной сфере. 2015. № 3 (17). С. 23-27.

Шелухин и др., 2013 – Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии) / Учебное пособие для вузов / Москва, 2013.

Сидельников, 2010 – Сидельников О.В Обнаружение аномалий сетевого трафика в автоматизированных информационных системах на основе метода сигнатурно-статистического анализа // Перспективы развития информационных технологий. 2010. № 2. С. 339-343.

Микова, 2015 – Микова С.Ю., Оладько В.С., Нестеренко М.А. Подход к классификации аномалий сетевого трафика // Инновационная наука. 2015. № 11-2. С. 78-81.

Басараб, Строганов, 2014 – Басараб М.А., Строганов И.С Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4 (7). С. 30-40.

Тищенко, 2013 – Тищенко И.П., Фраленко В.П., Хачумов В.М. Программно-инструментальные средства обнаружения и распознавания сетевых атак // Прикладная физика и математика. 2013. № 4. С. 73-88.

Чурилина, 2012 – Чурилина А.Е., Никишова А.В. Программный комплекс обнаружения атак на основе анализа данных реестра // Вестник Волгоградского государственного университета. Серия 10: Инновационная деятельность. 2012. № 6. С. 152-155.

Попов, 2010 – Попов Г.А. Модель анализа эмпирических данных в системах безопасности // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2010. № 1. С. 54-61.

Боровиков, 2003 – Боровиков В. STATISTICA. Искусство анализа данных на компьютере: Для профессионалов / В. Боровиков. — СПб., Питер, 2003. 688 с.

Википедиа, 2016 – [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%85%D0%BE%D1%82%D0%BE%D0%BC%D0%B8%D1%8F#.D0.9C.D0.B5.D1.82.D0.BE.D0.B4_.D0.B4.D0.B8.D1.85.D0.BE.D1.82.D0.BE.D0.BC.D0.B8.D0.B8 (дата обращения 01.06.2016).

Миркин, 1980 – Миркин Б.Г. Анализ качественных признаков и структур. М., «Статистика», 1980. С. 319.

Шашина, 1999 – Шанина Елена Алексеевна. Статистические методы агрегирования экономических показателей : Дис. ... канд. экон. наук : 08.00.11 : Москва, 1999, 130 с. РГБ ОД, 61:99-8/1113-7.

References

Rossiiskaya gazeta. 2000. 28 sentyabrya – Doktrina informatsionnoi bezopasnosti Rossiiskoi Federatsii [Tekst] [Utverzhdena Ukazom Prezidenta Rossiiskoi Federatsii ot 9 sentyabrya 2009 goda №PR-1895] // Rossiiskaya gazeta. 2000. 28 sentyabrya.

Simavoryan, Simonyan i dr., 2014 – Simavoryan S.Zh., Simonyan A.R., Ulitina E.I., Simonyan A.R. Issledovanie intellektual'nogo protivoborstva zloumyshlennikov i sluzhby zashchity informatsii v ASOD. // Izvestiya SGU, 2014, № 4-1 (32). C. 15-23.

Vasil'ev, 2013 – Vasil'ev V.I. Intellektual'nye sistemy zashchity informatsii: ucheb. posobie V.I. Vasil'ev. 2-izd. M.: Mashinostroenie, 2013. 172 s.

Gerasimenko, 1996 – Gerasimenko V.A. Osnovy informatsionnoi gramoty. M.: Energoatomizdat, 1996. 320 s.

Simavoryan, 2009 – Simavoryan S.Zh. Analiticheskaya model' opredeleniya pokazatelya uyazvimosti informatsii v avtomatizirovannykh sistemakh obrabotki informatsii (ASOD) // Obozrenie prikladnoi i promyshlennoi matematiki, tom 16, vypusk 6. Red. Yu.V. Prokhorov.- M.:OOO Redaktsiya zhurnala «OPiPM», 2009.

Markov, Fadin, 2013 – Markov A.S., Fadin A.A. Ctaticheskii signaturnyi analiz bezopasnosti programm // Programmnaya inzheneriya i informatsionnaya bezopasnost'. 2013. № 1. S. 50-56.

Borisov, Shaburov, 2015 – Borisov V.I., Shaburov A.S. O primenenii signaturnykh metodov analiza informatsii v siem-sistemakh // Vestnik UrFO. Bezopasnost' v informatsionnoi sfere. 2015. № 3 (17). S. 23-27.

Shelukhin i dr., 2013 – Shelukhin O.I., Sakalema D.Zh., Filinova A.S. Obnaruzhenie vtorzhenii v komp'yuternye seti (setevye anomalii) / Uchebnoe posobie dlya vuzov / Moskva, 2013.

Sidel'nikov, 2010 – Sidel'nikov O.V Obnaruzhenie anomalii setevogo trafika v avtomatizirovannykh informatsionnykh sistemakh na osnove metoda signaturno-statisticheskogo analiza // Perspektivy razvitiya informatsionnykh tekhnologii. 2010. № 2. S. 339-343.

Mikova, 2015 – Mikova S.Yu., Olad'ko V.S., Nesterenko M.A. Podkhod k klassifikatsii anomalii setevogo trafika // Innovatsionnaya nauka. 2015. № 11-2. S. 78-81.

Basarab, Stroganov, 2014 – Basarab M.A., Stroganov I.S Obnaruzhenie anomalii v informatsionnykh protsessakh na osnove mul'tifraktal'nogo analiza // Voprosy kiberbezopasnosti. 2014. № 4 (7). S. 30-40.

Tishchenko, 2013 – Tishchenko I.P., Fralenko V.P., Khachumov V.M. Programmno-instrumental'nye sredstva obnaruzheniya i raspoznavaniya setevykh atak // Prikladnaya fizika i matematika. 2013. № 4. S. 73-88.

Churilina, 2012 – Churilina A.E., Nikishova A.V. Programmnyi kompleks obnaruzheniya atak na osnove analiza dannykh reestra // Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10: Innovatsionnaya deyatel'nost'. 2012. № 6. S. 152-155.

Popov, 2010 –Popov G.A. Model' analiza empiricheskikh dannykh v sistemakh bezopasnosti // Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika. 2010. № 1. S. 54-61.

Borovikov, 2003 – Borovikov V. STATISTICA. Iskusstvo analiza dannykh na komp'yutere: Dlya professionalov / V. Borovikov. — SPb., Piter, 2003. 688 s.

Vikipedia, 2016 – [Elektronnyi resurs]. URL: https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%85%D0%BE%D1%82%D0%BE%D0%BC%D0%B8%D1%8F#.D0.9C.

D0.B5.D1.82.D0.BE.D0.B4_.D0.B4.D0.B8.D1.85.D0.BE.D1.82.D0.BE.D0.BC.D0.B8.D0.B8 (data obrashcheniya 01.06.2016).

Mirkin, 1980 – Mirkin B.G. Analiz kachestvennykh priznakov i struktur. M., «Statistika», 1980. S.319.

Shashina, 1999 – Shanina Elena Alekseevna. Statisticheskie metody agregirovaniya ekonomicheskikh pokazatelei : Dis. ... kand. ekon. nauk : 08.00.11 : Moskva, 1999, 130 c. RGB OD, 61:99-8/1113-7.

УДК 681.3

Создание условий для теоретического и практического решения задачи автоматизированного поиска образа интеллектуального злоумышленника в АСОД

Симон Жоржевич Симаворян [a, *], Арсен Рафикович Симонян [a], Елена Ивановна Улитина [a], Ирина Леонидовна Макарова [a], Рафик Арсенович Симонян [b]

[a] Сочинский государственный университет, Российская Федерация
[b] Кубанский государственный университет, Российская Федерация

Аннотация. Работа посвящена разработке методов автоматизированной обработки информации на основе специализированной базы знаний о злоумышленных действиях (шаблонах) и базы знаний о штатных ситуациях и значений их допустимых характеристик, с целью обнаружения злоумышленника и злоумышленных действий в автоматизированных системах обработки информации (АСОД).

Ключевые слова: механизмы противоборства злоумышленников и службы защиты информации, сигнатурные методы, методы обнаружения аномалий, автоматизированный поиск нечеткого образа злоумышленных действий, весовые показатели, агрегированные показатели.