УДК 681.3.053:681.32:007.5

Исследование интеллектуального противоборства злоумышленников и службы защиты информации в АСОД

[1] Симон Жоржевич Симаворян
[2] Арсен Рафикович Симонян
[3] Елена Ивановна Улитина
[4] Рафик Арсенович Симонян

[1-3] Сочинский государственный университет, Российская Федерация
354000, г. Сочи, Краснодарский край, ул. Советская, 26 а
[1] Кандидат технических наук, доцент
E-mail: simsim58@mail.ru
[2] Кандидат физико-математических наук, доцент
E-mail: oppm@mail.ru
[3] Кандидат физико-математических наук, доцент
E-mail: ulitinaelena@mail.ru
[4] Кубанский государственный университет, Российская Федерация
350040, г. Краснодар, ул. Ставропольская, 149
Аспирант
E-mail: raf55@list.ru

*Работа выполнена при поддержке гранта РФФИ 13-01-00544.

Аннотация. В статье разработана классификация подсистем противоборства злоумышленников и службы защиты информации автоматизированных систем обработки данных (АСОД), проведен анализ возможностей использования многоагентного подхода, генетических алгоритмов, нейронных сетей, иммунных систем.

Ключевые слова: механизмы противоборства злоумышленников и службы защиты информации; многоагентный подход; генетические алгоритмы; нейронные сети; иммунные системы.

Введение. В настоящее время, одним из наиболее актуальных направлений научных исследований в области обеспечения информационной безопасности является разработка методов и моделей обнаружения атак злоумышленников и защиты от этих атак на АСОД. В связи с возросшей активностью злоумышленных действий, следствием которых является несанкционированное получение защищаемой информации злоумышленником, при этом следует учесть тот фат, что злоумышленник постоянно совершенствует методы несанкционированного получения и извлечения информации, проблема противоборства злоумышленников и службы защиты информации вышла на новые рубежи интеллектуального противоборства. Все это обуславливает чрезвычайную актуальность вопросов защиты информации в АСОД. Практически любая АСОД представляет интерес для злоумышленника.

Материалы и методы. Основными источниками для написания данной статьи стали работы ведущих ученых в области информационной безопасности автоматизированных систем обработки информации. Первичная информация о противоборстве злоумышленников и службы защиты информации собиралась в открытых ресурсах, а именно на научных сайтах и журнальных публикациях. В работе использован системный подход к проектированию интеллектуальных систем защиты информации, а также проведен обзор возможности применения таких методов как: многоагентный подход, генетические алгоритмы, нейронные сети и иммунные системы.

Обсуждение. К настоящему времени проблеме исследования механизмов противоборства злоумышленников и службы защиты информации автоматизированной системы обработки информации (АСОД) уделяется большое внимание [9-11,17,28,29,31,32,34,35]. Это противоборство перешло на уровень решения

интеллектуальных задач противоборства злоумышленника с системой защиты информации в АСОД. С методологической точки зрения при решении данной проблемы необходимо исходить из двух следующих посылок: 1) современный злоумышленник постоянно совершенствует свои методы вторжения в АСОД, при этом следует говорить об интеллектуальном злоумышленнике; 2) служба защиты постоянно совершенствует механизмы противодействия угрозам несанкционированного получения информации злоумышленником. При разработке моделей интеллектуального злоумышленника необходимо учитывать:

1. Какие классы злоумышленников существуют?
2. Какая модель защиты информации в АСОД (количество зон защиты информации, рубежей)?
3. Какова вероятность проявления каналов НПИ в соответствующих зонах защиты информации?
4. Какова вероятность доступа злоумышленников в зоны защиты информации?
5. Какова вероятность наличия защищаемой информации в момент доступа злоумышленника к каналу НПИ?
6. Какова вероятность локализации НПИ?
7. Какова вероятность ликвидации последствий НПИ?
8. Какие модели (схемы) существуют у службы защиты АСОД о потенциально возможных НПИ в АСОД и схемы противодействия?

В работе [1] предложен системный подход к проектированию интеллектуальных систем защиты информации. Исходной основой концепции построения интеллектуальных систем защиты информации в АСОД являются: концепции построения интеллектуальных АСОД, концепции построения интеллектуальных баз данных, технологии обработки информации в АСОД, а также условия функционирования АСОД. Постоянно происходящие изменения в перечисленных областях приводят к появлению новых каналов несанкционированного получения информации (КНПИ). Служба защиты информации регулярно разрабатывает и реализует средства, методы и мероприятия по обеспечению и управлению защитой информации в АСОД. Злоумышленник также регулярно разрабатывает и реализует ряд стратегий по эффективному проведению атак на АСОД по потенциально возможным КНПИ.

Исследованиям интеллектуального противоборства злоумышленников и службы безопасности АСОД уделяется большое внимание. Для разработки систем обнаружения злоумышленных действий предлагаются различные инновационные подходы, например, многоагентный подход [3,4,15,20,23,33,39-41], генетические алгоритмы [8,42-45], нейронные сети [5,6,7,12,14,16,18,24-27,30,32], иммунные системы [13,18, 21,36,37].

Анализ этих работ показывает, что в них не прослеживается единая методология классификации уровней интеллектуального противоборства злоумышленников и службы защиты информации. Поэтому, с методологической точки зрения при разработке единой методологии механизмов противоборства злоумышленников и службы защиты информации необходимо учитывать такие параметры как: уровень интеллектуальной подготовки злоумышленника, уровень интеллектуальной подготовки службы защиты информации, уровень интеллектуальности средств защиты информации. В этом плане особый интерес представляет работа [2].

В работе [2] классификация уровней интеллектуальности систем защиты информации производится по трем признакам: по множеству потенциально возможных КНПИ, по множеству решаемых задач защиты информации и по множеству средств защиты информации. Каждое из этих множеств может быть как заданным, так и интеллектуальным. В результате такого подхода в работе [2] было получено 8 уровней интеллектуальности систем защиты информации:

- уровень 0 - определяется с помощью тройки $\{К_з, З_з, С_з\}$, где К - заданное множество потенциально возможных КНПИ, $З_з$ - заданное множество задач защиты информации, $С_з$ - заданное множество средств защиты информации;

- уровень 1- определяется тройкой {$К_з$, $З_з$, $С_и$}, где $К_з$ - заданное множество потенциально возможных КНПИ, $З_з$ - заданное множество задач защиты информации, $С_и$ - интеллектуальное множество средств защиты информации;

- уровень 2 определяется тройкой {$К_з$, $З_и$, $С_з$}, где $К_з$ - заданное множество потенциально возможных КНПИ, $З_и$ - интеллектуальное множество задач защиты информации, $С_з$ - заданное множество средств защиты информации;

- уровень 3 определяется тройкой {$К_з$, $З_и$, $С_и$} - где $К_з$ - заданное множество потенциально возможных КНПИ, $З_и$ - интеллектуальное множество задач защиты информации, $С_и$ - интеллектуальное множество средств защиты информации;

- уровень 4 определяется тройкой {$К_и$, $З_з$, $С_з$}, где $К_и$ - интеллектуальное множество потенциально возможных КНПИ, $З_з$ – заданное множество задач защиты информации, $С_з$ - заданное множество средств защиты информации;

- уровень 5 определяется тройкой {$К_и$, $З_з$, $С_и$}, где $К_и$ - интеллектуальное множество потенциально возможных КНПИ, $З_з$ - заданное множество задач защиты информации, $С_и$ - интеллектуальное множество средств защиты информации;

- уровень 6 определяется тройкой {$К_и$, $З_и$, $С_з$}, где $К_и$ - интеллектуальное множество КНПИ, $З_и$ - интеллектуальное множество задач защиты информации, $С_з$ - заданное множество средств защиты информации;

- уровень 7 (высший уровень) определяется тройкой {$К_и$, $З_и$, $С_и$}, где $К_и$ - интеллектуальное множество потенциально возможных КНПИ, $З_и$ -интеллектуальное множество задач защиты информации, $С_и$ - интеллектуальное множество средств защиты информации.

Таким образом, в результате такого подхода исследование противоборства службы защиты информации и множества потенциально возможных злоумышленников выходит на новый уровень исследования. Исходя из принятой классификации следует рассматривать задачи уровней 4, 5, 6 и 7.

Исходя из структурированной схемы потенциально возможных злоумышленных действий в АСОД [22], следует сделать вывод об особенностях противоборства в каждой зоне защиты информации в АСОД, а именно: 1) во внешней неконтролируемой зоне - территории вокруг АСОД, на которой персоналом и средствами АСОД не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации; 2) в зоне контролируемой территории - территории вокруг помещений АСОД, которая непрерывно контролируется персоналом или средствами АСОД; 3) в зоне помещений АСОД - внутреннее пространство тех помещений, в которых расположены средства системы; 4) в зоне ресурсов АСОД - в той части помещений, откуда возможен непосредственный доступ к ресурсам системы; 5) в зоне баз данных - в той части информационных ресурсов системы, к которым возможен непосредственный доступ.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. Поэтому, учитывая сформулированные в [22] функции защиты информации, архитектурно система защиты информации должна включать в себя следующие подсистемы: 1) подсистему предупреждения доступа злоумышленника в зону защиты; 2) подсистему обнаружения и контроля наличия канала НПИ в зоне защиты информации; 3) подсистему контроля наличия защищаемой информации в канале и доступа к нему злоумышленника; 4) подсистему локализации НПИ и 5) подсистему ликвидации последствий НПИ. В табл. 1 приводится общая модель подсистем противодействия злоумышленникам в АСОД.

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.

Анализ вышеупомянутых подходов к моделированию противоборства злоумышленников и службы защиты показывает, что комбинированное применение многоагентного подхода, в сочетании с генетическими алгоритмами, нейронными сетями и иммунными системами даёт хороший результат. Основная цель любой службы защиты информации - перекрытие утечки информации по потенциально возможным КНПИ. Механизм закрытия КНПИ выглядит следующим образом: {{КНПИ}-{Задача}-{Средство}}.

Так, например, многоагентная модель очень удобна для описания таких агентов как: злоумышленник, знания злоумышленника, служба защиты информации, знания службы защиты информации.

Многоагентный подход

В работах [3, 4, 15, 20, 23, 33, 39-41] приводятся исследования по противоборству службы защиты информации и потенциально возможных злоумышленников; а также исследования по разработке архитектуры автоматизированной системы управления информационной безопасностью предприятия с помощью интеллектуальных многоагентных моделей. Рассмотрим наиболее значимые положения этого подхода применительно к нашему механизму закрытия КНПИ. Модель включает множество агентов-злоумышленников и агентов-службы безопасности, которые являются интеллектуальными агентами, и агентов работников АСОД. Интеллектуальные агенты способны выбирать наиболее рациональные стратегии НПИ и защиты от НПИ в зависимости от располагаемых знаний об АСОД и совершенствоваться (обучаться) в процессе выполнения своих действий.

Так, например, в [3] агенты описываются с помощью различных кортежей, например,

$A = (K, B, T, З, И, C, П)$,

где К – класс злоумышленника; В – вид злоумышленника; Т – время жизни злоумышленника; З - совокупность знаний; И - множество инструментальных средств; С - множество стратегий; П - пользовательский идентификатор.

Таким образом, можно выделить следующие классы агентов: агенты службы защиты информации; агенты АСОД; агенты злоумышленники. Злоумышленники подразделяются на следующие делятся на следующие группы: пользователи АСОД, операторы АСОД, программисты АСОД, инженерно-технические работники АСОД, администрация АСОД, служба защиты информации АСОД. Время доступа злоумышленников к КНПИ ограничено, если злоумышленник не имеет свободного неограниченного доступа к ресурсам АСОД.

Полный набор знаний обозначим как $З=\{З_1,...,З_n\}$, где это знания о наличии КНПИ в АСОД, о зонах их проявления, о задачах защиты информации, о средствах защиты информации. Это могут быть знания как злоумышленника, так и сотрудника службы защиты информации. Их онтологии как злоумышленник, так и сотрудник службы безопасности АСОД размещает в своей базе знаний. На основе этих знаний злоумышленник синтезирует дерево НПИ. Сотрудник службы защиты информации, исходя из конкретных задач защиты и средств защиты информации, на основе своей базы знаний синтезирует своё дерево НПИ по каждому канал. Аналогично агент злоумышленник синтезирует дерево уязвимостей АСОД. Каждому ребру дерева приписывается кортеж с указанием вероятности успешной атаки, времени реализации атаки, возможностей её локализации и ликвидации последствий НПИ. Более детально о возможностях многоагентного подхода можно узнать в последующих публикациях. Многоагентная модель может быть успешно реализована применительно к каждому блоку системы защиты информации, приведенным в таблице 1.

Генетические алгоритмы

Ниже приведем краткий анализ возможностей применения генетических алгоритмов в моделях противоборства злоумышленников и службы защиты информации. Более детальные исследования требуют дополнительного исследования и публикаций, что в рамках проекта будет представлять большой интерес. Генетические алгоритмы относятся к неформально-эвристическим методам поиска оптимальных решений, использующих технику и терминологию, заимствованную из биологии, для нахождения оптимальных значений функции $Y=F(U)$, где U - вектор заданных параметров [8.42-45]. В методах генетических алгоритмов нет ограничений на тип функции F(U) и на независимые параметры U (непрерывные, дискретные, с неопределённостями), что делает их простыми в использовании, и которые относительно легко реализуются при параллельных расчетах, что значительно снижает расчетное время для детального анализа стратегий злоумышленников и службы защиты информации.

При реализации методов генетических алгоритмов, например, при решении задач поиска стратегий злоумышленных действий, связанных с НПИ, шаги использования метода следующие:

Шаг 1 - вначале определяется пространство поиска на основе вектора U (функция F базируется на критических значениях параметров защищённости информации). Параметрами вектора U могут быть знания о каналах НПИ, знания о применяемых средствах защиты информации, знания о механизмах защиты информации и т.д.

Шаг 2 - пространства событий U, связанных с НПИ, отображаются на вектор параметров - X (хромосомы по терминологии генетических алгоритмов).

Шаг 3 - исследуются неопределенности, связанных с НПИ, для нахождения условий, при которых нарушаются требования по защите информации в. АСОД.

Шаг 4 – разрабатываются сценарии возможных злоумышленных действий.

Шаг 5 - После нахождения наихудшей ситуации и идентификации НПИ могут быть оценены их вероятностные характеристики уязвимости информации.

Использование генетических алгоритмов позволяет исследовать различные стратегии усиления системы защиты и выбрать оптимальную стратегию при атаках одного или нескольких злоумышленников, проводящих распределенные атаки.

Нейронные сети

В настоящее время, использование нейронных систем обнаружения атак дает очень хорошие результаты в противодействии службы защиты информации злоумышленным вторжениям в сеть АСОД [5, 6, 7, 12, 14, 16, 18, 24-27, 30, 32],

Основными характеристиками нейронных сетей являются: 1) базовые элементы – искусственные нейроны, 2) количество нейронов и их местоположение в механизмах защиты от НПИ фиксированное; 3) поведение сети во многом зависит от принятых механизмов и алгоритмов функционирования системы защиты информации в АСОД; 4) взаимодействие между нейронами постоянно и задается на начальном этапе их функционирования; 5) во взаимодействии нейронов используется единый механизм настройки весовых связей между нейронами. Каждый нейрон можно считать своеобразным процессором: он суммирует с соответствующими весами сигналы, приходящие от других нейронов, выполняет нелинейную решающую функцию и передаёт результирующее значение связанным с ним нейронам. Любая НС используется в качестве самостоятельной системы представления знаний и может найти применение в решении задач противодействия службы защиты информации злоумышленникам. Из структуры таблицы 1 следует, что общая нейросеть будет состоять из подсетей(блоков) более мелких сетей. Постановка значительного количества задач моделирования блоков нейросетей, классификации и обработки сигналов между ними могут быть сведены именно к аппроксимационному представлению всей общей нейросети. Данная задача довольно трудоемкая и требует дополнительных исследований.

Имунные системы

В последние годы специалисты по защите информации проявляют большой интерес к новому направлению в области искусственного интеллекта – искусственным имунным системам. Данной тематике посвящено ряд исследований [13, 18, 21, 36, 37]. В настоящее время имунные системы нашли применение при решении таких задач как:

- обнаружение атак и аномалий на информационные системы;
- защита от спама;
- управление инцидентами информационной безопасности;
- распознавание новых видов компьютерных вирусов;
- выявление ошибок на серверах и рабочих местах пользователей ИС;
- интеллектуального анализа данных о защищенности информации; и т.д.

Основными свойствами имунных систем являются: 1) базовые элементы лимфоциты и антитела, 2) количество элементов системы меняется динамически; 3) имунным системам характерны такие свойства как самоорганизация и эволюция поведения; 4) взаимодействие между элементами может меняться динамически в зависимости от количества и постановки задач защиты информации; 5) отсутствует централизованное управление имунной системы, система действует децентрализованно, что может привести злоумышленника в панику (замешательство).

В качестве базовых механизмов защиты используются механизмы врожденного и приобретённого иммунитета. Врождённый иммунитет обладает спецификой распознания известных механизмов и алгоритмов по НПИ, локализации и ликвидации последствий НПИ. Приобретенный иммунитет отвечает за распознавание новых ситуаций, связанных с НПИ и выработке новых механизмов локализации НПИ и ликвидации их последствий. Из известных наработок в области построения искусственных имунных систем в области информационной безопасности можно выделить сетевую имунную систему противодействия компьютерным атакам, системы обнаружения аномалий трафика, системы обнаружения необычного поведения прикладных программ, систему распознавания необычных системных вызовов, систему активного аудита информационной системы на основе интеллектуальных технологий, систему антивирусной защиты информации и т.д.

Заключение. В статье была проведена классификация моделей борьбы злоумышленников и службы защиты информации по следующим признакам: во-первых, по зонам защиты информации, а во-вторых по функциям защиты информации. Архитектурно система защиты информации была разделена на подсистемы защиты информации в соответствии с функциями защиты информации, т.е.: 1) подсистему предупреждения доступа злоумышленника в зону защиты; 2) подсистему обнаружения и контроля наличия канала НПИ в зоне защиты информации; 3) подсистему контроля наличия защищаемой информации в канале и доступа к нему злоумышленника; 4) подсистему локализации НПИ и 5) подсистему ликвидации последствий НПИ. Такая классификация дает возможность разбить механизм противоборства на блоки.

Такой подход существенно способствует структуризации механизмов защиты информации и позволяет успешно перекрывать каналы НПИ, во всех зонах защиты информации с применением различных методов и подходов. Были рассмотрены четыре метода к решению задачи противоборства злоумышленников и сотрудников службы защиты информации АСОД, а именно: многоагентный подход, генетические алгоритмы, нейронные сети, иммунные системы. Анализ показал, что применяемые новые подходы совместно с существующими позволяют получить качественно новый уровень противоборства. Само представление структуры интеллектуальной системы защиты информации через функции защиты информации, даёт блочное распределение системы с разбивкой на зоны защиты информации, и как следствие этого имеем, что злоумышленнику всё труднее и труднее будет становиться выходить победителем в противоборстве со службой защиты информации в АСОД.

Примечания:

1. Симаворян С.Ж., Симонян А.Р., Улитина Е.И., Симонян Р.А. Системный подход к проектированию интеллектуальных систем защиты информации // Известия Сочинского государственного университета. 2013, № 4-2 (28), с. 128-132.

2. Simavoryan S. Sh.,Simonyan A.R., Ulitina E.I., Simonyan R.A. About one Approach to a Question of Classification of Intellectual System of Information Security // «Modeling of Artificial Intelligence». 2014. Vol (1), № 1, p. 29-44.

3. Цыбулин А.М., Никишова А.В., Умницын М.Ю. Исследование противоборства службы безопасности и злоумышленников на многоагентной модели. // Известия Южного Федерального университета. Технические науки. 2008. Т. 85. № 8. С. 94-99

4. Бешта А.А. Многоагентная эволюционирующая система как средство контроля над внутренними злоумышленниками //Вестник Волгоградского государственного университета. Серия 10: Инновационная деятельность. 2012. № 6. С. 93-97.

5. Безкоровайный М.М., Татузов А.Л. Направления совершенствования нейросетевых методов для обнаружения вторжений // Информатизация и связь. 2010. № 2. С. 77-85.

6. Марченко А.А., Матвиенко С.В., Нестерук Ф.Г. К обнаружению атак в компьютерных системах нейросетевыми средствами //Научно-технический вестник информационных технологий, механики и оптики. 2007. № 39. С. 83-93.

7. Харченко А.Ф., Нестерук Ф.Г. Информационная безопасность и искусственные нейронные сети // Известия высших учебных заведений. Приборостроение. 2003. Т. 46. № 7. С. 47-52.

8. Crosbie M., Spafford G. Applying Genetic Programming to Intrusion Detection // Proceedings of the AAAI Fall Symposium on Genetic Programming. Cambridge, 1995. Menlo Park, CA: AAAI Press, 1995.

9. Цыбулин А.М., Шипилева А.В. Математическая модель злоумышленника в корпоративной сети // Управление большими системами: сборник трудов. 2007. № 19. С. 127-133.

10. Нестерук Ф.Г. К организации интеллектуальной защиты информации //Труды СПИИРАН. 2009. № 10. С. 148-159.

11. Застрожнов И.И., Коробкин Д.И., Окрачков А.А., Рогозин Е.А. Модель конфликта злоумышленника и систем защиты информации //Вестник Воронежского государственного технического университета. 2009. Т. 5. № -6. С. 142-149.

12. Булдакова Т.И. Нейросетевая защита ресурсов автоматизированных систем от несанкционированного доступа// Наука и образование, электроный научнотехнический журнал, №5, май, 2013.

13. Гладыш С.В. Имунная мультиагентная система управления инцидентами информационной безопасности// Информационная безопасность. 2008. №1, с. 114-117.

14. Васильев В.И. Применение нейтронных сетей при обнаружении атак на компьютеры в сети Интернет (на примере атаки SYNFLOOD) / В.И. Васильев, А.Ф. Хафизов // Нейрокомпьютеры: разработка, изменение // Радиотехника. 2001. № 4-5. С. 108-114.

15. Васильев В. И. Интеллектуальная многоагентная система обнаружения атак / В.И. Васильев, К.В. Сафронов: материалы конференции / V международная конференция «Проблемы управления и моделирования в сложных системах», Самара, 17-21 июня 2003 г. Самара: СНЦ РАН, 2003. С. 354-360.

16. Васильев В.И. Нейросетевые системы обнаружения атак на www-сервер / В.И. Васильев, А.Ф. Хафизов // Вестник УГАТУ. 2005. 6 т. № 1 (12). С. 116-120.

17. Васильев В.И. Комплексный подход к построению интеллектуальной системы обнаружения атак / В.И. Васильев, Т.Р. Кашаев, Л.А. Свечников // Системы управления и информационные технологии. 2007 г. № 2 . С. 76-81.

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

19. Машкина И.В. Концепция построения модели угроз в информационной среде объекта информации / И.В. Машкина, В.И. Васильев, Е.А. Рахимов // Информационные технологии. 2007 г. № 2. С. 24-32.

20. Белоусова А.И., Варламов О.О., Остроух М.Н., Краснянский М.И. Подход к формированию многоуровневой модели мультиагентной системы с использованием миваров // Перспективы науки. №5(20). 2011, С. 57-61.

21. Обухов А.В. Метод иммунного ответа на вторжения / А.В. Обухов, С.А. Петренко, А.В. Беляев // Защита информации. INSIDE. 2009. № 4. С. 44-54.

22. Герасименко В.А., Малюк А.А.. Основы защиты информации. / М: 1997. 540 с.

23. Котенко И.В., Карсаев О.И. Использование многоагентных технологий для комплексной защиты информационных ресурсов в компьютерных сетях // Известия Южного федерального университета. Технические науки. 2001. Т. 22. № 4. С. 38-50.

24. Технологии обнаружения сетевых атак [электронный ресурс]. Режим доступа: http://www.bstu.by/~opo/ru/uni/bstu/science/ids/.

25. Власов А. И. Нейросетевые методы и средства обнаружения атак на сетевом уровне / А.И. Власов, С.В. Колосков, А.Е. Пакилев: материалы конференции Ч. 1. / VIII Международная научно-техническая конференция «Нейроинформатика». М.: МИФИ, 2000. С. 30-32.

26. Лиховидов В. Н. Нейроподобные адаптивные алгоритмы обнаружения атак в компьютерных сетях. / В. Н. Лиховидов, П. Н. Коршунин: Материалы конференции. / VII Международная научно-практическая конференция «Информационная безопасность». – Таганрог: ТРТУ. 2005. № 4 (48). С. 82-87.

27. Хафизов А.Ф. Нейросетевая система обнаружения атак на www-сервер: дис. … канд. тех. наук: 05.13.11. Уфа, 2004. 172 с.

28. Абрамов Е.С. Разработка и исследование методов построения систем обнаружения атак: дис. … канд. тех. наук: 05.13.11. 142 с.

29. Костин А.А. Модель и методика проектирования адаптивной системы обнаружения компьютерных атак с использованием нейросетевых средств: дис. … канд. тех. наук: 05.13.19. СПб. 2006. 108 с.

30. Слеповичев И.И. Обнаружение DDoS атак нечеткой нейронной сетью. / И.И. Слеповичев, П.В. Ирматов, М.С. Комарова, А.А. Бежин // Известия Саратовского университета: серия «Математика. Механика. Информатика». Т. 9. 2009. Вып. 3. С. 84-89.

31. Беляев А.В. Современное состояние проблем обнаружения вторжений / А.В. Беляев, С.А. Петренко, А.В. Обухов // Защита информации, INSIDE. 2009. Вып. 143. С. 55-68.

32. Жульков Е.В. Построение модульных нейронных сетей для обнаружения классов сетевых атак: //дис. … канд. тех. наук: 05.13.19. Санкт-Петербургский политехн. ун-т. 2007. 155 с.

33. Толчеев В.О. Функциональные возможности и области применения интеллектуальных агентов и многоагентных систем // Микросистемная техника, 2002. №4. С. 10-15.

34. Корнеев В.В. Интегрированные системы обнаружения атак / В.В. Корнеев, В.В. Райх // Наукоёмкие технологии. 7 т. № 11-12. 2006. С. 62-73.

35. Свечников Л.А. Интеллектуальная система обнаружения атак на основе имитационного моделирования с использованием нечётных когнитивных карт: // дис. … канд. тех. наук: 05.13.19. Уфа, 2010. 127 с.

36. Forrest S., Hofmeyr S., Somayaji A. Computer Immunology // Communications of the ACM, 40, 10, 1997, P.86-96.

37. Somayaji A., Hofmeyr S., Forrest S. Principles of a Computer Immune System // Proceedings of the 1997 New Security Paradigms Workshop. 1998. P. 75-82.

38. Цыбулин А.М. Многоагентная модель для исследования противоборства службы безопасности и ассоциации злоумышленников // Обозрение прикладной и промышленной математики. Т. 15. № 4. 2008. С. 682-683.

39. Цыбулин А.М. Архитектура автоматизированной системы управления информационной безопасностью предприятия // Известия Южного федерального университета. Технические науки. 2011. № 12 (125). С. 58-64.

40. Цыбулин А.М. Многоагентный подход к построению автоматизированной системы управления информационной безопасностью предприятия // Известия Южного федерального университета. Технические науки. 2012. № 12 (137). С. 111-116.

41. Цыбулин А.М. Подход к построению автоматизированной системы управления информационной безопасностью предприятия //Вестник Волгоградского государственного университета. Серия 10: Инновационная деятельность. 2011. № 5. С. 86-89.

42. Воробьев Ю.Б., Кудинов П., Ельцов М., Кёоп К., Чыонг Ван К.Н. Применение информационных технологий (генетические алгоритмы, нейронные сети, параллельные вычисления) в анализе безопасности АЭС // Труды Института системного программирования РАН. 2014. Т. 26. № 2. С. 137-158.

43. Нестерук Ф.Г., Молдовян А.А., Нестерук Г.Ф., Нестерук Л.Г. Квазилогические нейронечеткие сети для решения задачи классификации в системах защиты информации //Вопросы защиты информации. 2007. № 1. С. 23-31.

44. Нестерук Г.Ф., Молдовян А.А., Грибачев В.П., Воскресенский С.И. О нейронечеткой реализации двухуровневой адаптивной системы информационной безопасности // Вопросы защиты информации. 2005. № 3. С. 6-12.

45. Бугаев С.Б. Метод формирования комплекса мер противодействия угрозам информационной безопасности на основе эволюционного подхода // Системы управления и информационные технологии. 2009. Т. 38. № 4. С. 81-85.

UDC 681.3.053:681.32:007.5

Study of Intellectual Confrontation of Perpetrators and Information Security Department in Computer Systems of Data Processing

[1] Simon Zh. Simavoryan
[2] Arsen R. Simonyan
[3] Elena I. Ulitina
[4] Rafik A. Simonyan

[1-3] Sochi State University, Russian Federation
Sovetskaya Street 26 a, Sochi city, Krasnodar krai, 354000
[1] PhD, Associate professor
E-mail: simsim58@mail.ru
[2] PhD, Associate professor
E-mail: oppm@mail.ru
[3] PhD, Associate professor
E-mail: elenaulitina@mail.ru
[4] Kuban State University, Russian Federation
Stavropolskaya St., Krasnodar, 149 350040
E-mail: raf55@list.ru
Post-graduate student

Abstract. The article develops classification of subsystems of confrontation of perpetrators and information security department of the computer systems of data processing, analyzes possibilities of the use of multi-agent approach, genetic algorithms, neural network, immune systems.

Keywords: mechanisms of confrontation of perpetrators and information security department; multi-agent approach; genetic algorithms; neural network; immune systems.