УДК 004.056

МИРОШНИК М.А., доктор технических наук, профессор (Украинский государственный университет железнодорожного транспорта),
КРЫЛОВА В.А., кандидат технических наук (Национальный технический университет «Харьковский политехнический институт»),
ДЕМИЧЕВ А.И., аспирант кафедры специализированных компьютерных систем (Украинский государственный университет железнодорожного транспорта)

Применение интеллектуальной диагностической инфраструктуры для управления кибербезопасностью. Часть 1. Интеллектуализация механизмов защиты

Кибербезопасность в условиях глобальной информатизации общества рассматривается сегодня как одна из основных компонент национальной безопасности. В работе рассматривается подход к разработке и использованию систем киберзащиты, основанный на выделении интеллектуальной надстройки над традиционными механизмами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты. Представляются отдельные механизмы управления кибербезопасностью.
***Ключевые слова**: распределенные сети, сеть, доступ, аутентификация, шифрование, защита информации, базы данных, модели безопасности.*

Постановка проблемы в общем виде и ее связь с важными научными или практическими задачами

В связи с беспрецедентно быстрым развитием компьютерных и телекоммуникационных технологий, в том числе появлением сети Интернет, объединяющей огромное количество разнородных сетей (от локальных до транснациональных), и переходом к информационному обществу проблема обеспечения кибербезопасности и построения информационно-безопасных распределенных вычислительных систем стала одной из наиболее актуальных проблем [1].

В соответствии с современными представлениями перспективная система киберзащиты (СКЗ) должна представлять собой взаимоувязанную, многоэшелонированную и непрерывно контролируемую систему, способную оперативно реагировать на удаленные и локальные кибератаки и несанкционированные действия (НСД), накапливать знания о способах противодействия, обнаружения и реагирования на атаки и НСД и использовать их для усиления защиты.

Такая СКЗ должна предоставлять, по крайней мере, три уровня защиты [2]. Первый уровень защиты составляют «традиционные» средства защиты, реализующие функции идентификации и аутентификации, криптографической защиты, разграничения доступа, контроля целостности, регистрации и учета, межсетевого экранирования. Второй уровень включает средства проактивной защиты, обеспечивающие сбор необходимой информации, анализ защищенности, мониторинг состояния сети, обнаружение атак, противодействие их реализации, введение злоумышленника в заблуждение и т. п. Третий уровень соответствует средствам управления защитой, которые осуществляют интегральную оценку состояния сети, управление защитой и адаптацию политик безопасности и компонентов СКЗ.

Первый уровень достаточно широко представлен в существующих исследованиях. Разработка механизмов киберзащиты, относящихся ко второму и особенно третьему уровню, реализующих по существу интеллектуальную надстройку над традиционными механизмами защиты (для управления ими), составляет в настоящее время приоритетную задачу в области теоретических и прикладных исследований по построению информационно - безопасных распределенных вычислительных систем.

В статье рассматривается подход к разработке и использованию СКЗ, основанный на выделении такой интеллектуальной надстройки над традиционными механизмами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем киберзащиты.

Формулирование целей статьи (постановка задачи)

В рамках решения задачи киберзащиты авторами исследуется комплекс формальных методов, моделей, алгоритмов и построенных на их основе программных прототипов, реализующих различные интеллектуальные механизмы защиты:

– сбор информации о состоянии информационной системы и ее анализ за счет механизмов обработки и слияния информации из различных источников;

– проактивное предупреждение атак и препятствование их выполнению;

– обнаружение аномальной активности и явных атак, а также нелегитимных действий и отклонений работы пользователей от политики безопасности, предсказание намерений и возможных действий нарушителей;

– активное реагирование на попытки реализации действий нарушителей путем автоматической реконфигурации компонентов защиты для отражения действий нарушителей в реальном масштабе времени;

– дезинформацию злоумышленника, сокрытие и камуфляж важных ресурсов и процессов, «заманивание» злоумышленника на ложные (обманные) компоненты с целью раскрытия и уточнения его целей, рефлексивное управление поведением злоумышленника;

– мониторинг функционирования сети и контроль корректности текущей политики безопасности и конфигурации сети;

– поддержку принятия решений по управлению политиками безопасности, в том числе по адаптации к последующим вторжениям и усилению критических механизмов защиты.

Интеллектуализация механизмов защиты

Перспективным подходом к построению интеллектуальных механизмов киберзащиты является *технология интеллектуальных многоагентных систем*. Этот подход позволяет по сравнению с традиционными методами существенно повысить эффективность защиты информации, в том числе ее адекватность, отказоустойчивость, устойчивость к деструктивным действиям, универсальность, гибкость и т. д.

В соответствии с данным подходом предполагается, что компоненты систем киберзащиты, специализированные по типам решаемых задач, тесно взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений, адаптируются к изменению трафика, реконфигурации аппаратного и программного обеспечения, новым видам кибератак [3 - 6].

В рамках предлагаемого подхода компоненты многоагентной системы киберзащиты представляют собой интеллектуальные автономные программы (агенты защиты), реализующие определенные функции защиты с целью обеспечения требуемого класса защищенности. Они позволяют реализовать комплексную надстройку над механизмами безопасности используемых сетевых программных средств, операционных систем и приложений, повышая защищенность системы до требуемого уровня.

В рамках данного направления исследований разработаны архитектуры, модели и программные прототипы нескольких многоагентных систем, в том числе агентно-ориентированная система моделирования атак, многоагентная система обнаружения вторжений, многоагентная система обучения обнаружению вторжений и др.

Согласно разработанной технологии процесс создания многоагентных систем для любой предметной области, в том числе киберзащиты, предполагает решение двух высокоуровневых задач [5, 7]:

– создание «Системного ядра» многоагентной системы;

– клонирование программных агентов и отделение сгенерированной многоагентной системы от «Системного ядра».

Для спецификации «Системного ядра» используются два компонента программного инструментария создания многоагентных систем MASDK («Multi-agent System Development Kit») [7]. Первый из них — это так называемый «Типовой агент» («Generik Agent») который предназначен для создания высокоуровневой спецификации класса агента. Второй компонент служит для формирования проблемно-ориентированной архитектуры приложения, заполнения данных, знаний, а также определения коммуникационного компонента.

Сформированные агенты имеют аналогичную архитектуру (рис. 1). Различия отражаются в содержании данных и баз знаний агентов. Каждый агент взаимодействует с другими агентами, средой, которая воспринимается и, возможно, изменяется агентами, а также пользователем, общающимся с агентами через пользовательский интерфейс.

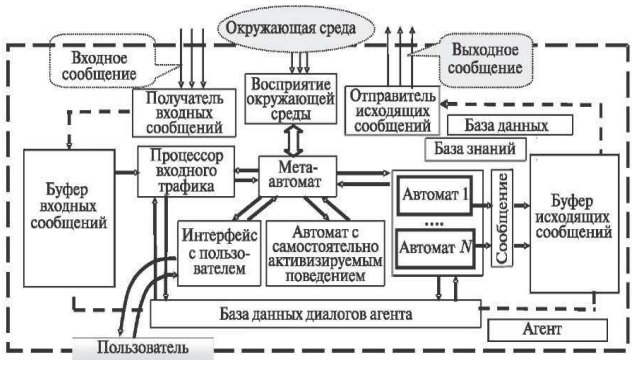

Рис. 1. Архитектура типового агента

В предложенной формальной модели и прототипе *агентно-ориентированной системы моделирования атак* (АСМА) распределенные скоординированные атаки на компьютерную сеть рассматриваются в виде последовательности совместных действий агентов-хакеров, которые выполняются с различных хостов [4, 8]. Предполагается, что хакеры координируют свои действия согласно некоторому общему сценарию. На каждом шаге сценария атаки они пытаются реализовать некоторую частную подцель. АСМА построена на основе предложенной формальной модели реализации атак.

Отличительные черты реализованного в АСМА подхода к моделированию атак: моделирование атак базируется на спецификации задач хакеров и иерархии их намерений; многоуровневое описание атаки представляется в последовательности «общий сценарий распределенной атаки → намерения хакеров → простые атаки → входной трафик или данные аудита»; разработка планов действий хакеров и моделей отдельных атак основывается на задании онтологии предметной области «Атаки на компьютерные сети»; формальное описание сценариев взаимодействия агентов и реализации распределенных атак выполнено на базе семейства стохастических атрибутных грамматик, связанных операциями подстановки; в алгоритмической интерпретации процедур генерации атак каждой из грамматик ставится в соответствие автомат; генерация действий (атак) хакеров происходит в зависимости от реакции атакуемой сети в реальном масштабе времени.

Разработанный к настоящему времени программный прототип АСМА состоит из следующих компонентов (агентов): множества агентов хакеров, каждый из которых реализует модель атакующего, агента — модели атакуемой компьютерной сети и генератора фонового «нормального» трафика. В процессе атаки агенты обмениваются сообщениями с целью координации своих действий.

Данные о реализуемой атаке разбиты на четыре группы:

– элементы спецификации задачи атакующего;

– дерево генерации атаки;

– строки генерируемых действий злоумышленника;

– для каждого действия злоумышленника отображаются признак успеха (неуспеха) в виде квадрата зеленого (черного) цвета и данные, полученные от атакуемого хоста (реакция хоста).

Компоненты *многоагентной системы обнаружения вторжений* (МСОВ) – это взаимодействующие между собой агенты, совместно решающие общую задачу обнаружения вторжений в компьютерную сеть [3, 7, 9]. Архитектура МСОВ включает один или несколько экземпляров агентов разных типов, специализированных для решения подзадачи обнаружения вторжений. Агенты распределены по хостам защищаемой сети, специализированы по типам решаемых задач и взаимодействуют друг с другом с целью обмена информацией и принятия согласованных решений. В принятой архитектуре исследуемого прототипа МСОВ в явном виде отсутствует «центр управления» семейством агентов — в зависимости от сложившейся ситуации ведущим может становиться любой из агентов, инициирующий и (или) реализующий функции кооперации и управления. В случае необходимости агенты могут как клонироваться (образовывать новые сущности), так и прекращать свое функционирование. В зависимости от ситуации (вида и количества атак на компьютерные сети, наличия вычислительных ресурсов для выполнения функций защиты) может потребоваться генерация нескольких экземпляров агентов каждого класса. Предполагается, что архитектура МСОВ может адаптироваться к реконфигурации сети, изменению трафика и новым видам атак, используя накопленный опыт.

Представляется, что наиболее действенный путь обнаружения распределенных многофазных атак, направленных на компьютерные сети, состоит в кооперации множества агентов защиты, распределенных по хостам сети. Поэтому основное достоинство МСОВ заключается в возможности относительно «легких» компонентов системы сотрудничать и совместно решать сложную задачу обнаружения таких атак. Базовые черты подхода, реализованного в МСОВ, таковы:

– расширяемая и адаптивная многоагентная архитектура;

– центральное внимание уделяется обнаружению многофазных распределенных атак;

– обеспечение безопасности и робастности (обработка сетевых событий, важных с точки зрения защиты информации, и функции управления распределены среди множества агентов различных хостов).

Базовые типы компонентов МСОВ, размещаемые на каждом из хостов защищаемой компьютерной сети, представлены ниже.

Агент-демон AD-E (AD-Events) осуществляет предварительную обработку поступающих на хост сообщений, фиксируя значимые для защиты информации события, и переадресует выделенные сообщения соответствующим специализированным агентам. *Агент-демон идентификации и аутентификации* AIA ответствен за идентификацию источников сообщений и подтверждение их подлинности. *Агент-демон разграничения доступа* АСА регламентирует доступ пользователей к ресурсам сети в соответствии с их правами и метками конфиденциальности объектов защиты. Агенты AIA и АСА обнаруживают несанкционированные действия

по доступу к информационным ресурсам хоста, прерывают соединения и процессы обработки событий, отнесенные к числу несанкционированных, а также посылают сообщения агентам обнаружения вторжений. *Агенты-демоны* IDA1 и IDA2 (AD-Patterns) отвечают за обнаружение отдельных «подозрительных» событий или очевидных фактов вторжения и принятие решений относительно реакции на данные события (факты). *Интеллектуальные агенты обнаружения вторжений* IDA1 и IDA2 реализуют более высокий уровень обработки и обобщения обнаруженных фактов. Они принимают решения на основе сообщений об обнаруженном подозрительном поведении и явных атаках как от агентов-демонов своего хоста, так и от агентов других хостов.

Возможными высокоуровневыми сценариями, обнаруживаемыми IDA2, являются:

– разведка – разведывательные действия атакующего (действия по определению конфигурации сети, обнаружению хостов, функционирующих на хосте сервисов, определению операционной системы, приложений и т. п.);

– внедрение в систему – действия злоумышленника по взлому хоста и внедрению в систему;

– повышение прав – попытки атакующего, направленные на получение повышенных прав по доступу к объектам хоста;

– распространение поражения на хосте – нелигитимное распространение злоумышленника по объектам хоста (каталогам, файлам, программам);

– распространение поражения по сети – распространение атакующего по защищаемой компьютерной сети и др.

Многоагентная система обучения обнаружению вторжений в компьютерные сети (МСООВ) является мультисенсорной системой объединения данных. Она формирует решения на основе многоуровневой модели обработки входных данных (входного трафика сети и данных аудита). На нижнем уровне решения принимаются так называемыми *«базовыми»* классификаторами. Их может быть несколько для одного и того же подмножества атак, но они должны обучаться на различных наборах обучающих и тестовых данных. На более высоком уровне решения базовых классификаторов используются для принятия итогового решения на основе объединения решений базовых классификаторов. Это выполняется мета-классификаторами. Применительно к такому взгляду на обучаемую систему предложена архитектура многоагентной системы обучения обнаружению вторжений [5, 6]. Эта система имеет многоагентную архитектуру, реализующую многоуровневое обучение на основе имеющихся интерпретированных данных из тех же источников и представленных в тех же структурах, которые используются МСОВ. Типовыми классами агентов МСООВ являются: класс агентов управления данными обучения; класс агентов тестирования классификаторов; класс агентов подготовки мета-данных; класс обучающих агентов. В качестве методов (алгоритмов) обучения, которые позволяют решать рассматриваемую задачу обучения, используются методы ID3, C4.5, бустинг, мета-классификации, FP-growth, метод визуальной классификации, GK2, INFORMи др.

Исследование возможностей агентских технологий и проведенные эксперименты с разработанными программными прототипами показали несомненные преимущества применения интеллектуальных систем ки- берзащиты и использования многоагентного подхода к построению СКЗ. В пользу этого тезиса можно выдвинуть следующие обстоятельства [5].

Распределение объектов и средств защиты как в границах хоста, так и в рамках компьютерной сети диктует необходимость использовать распределенную интегрированную систему защиты, к классу которых относятся многоагентные СКЗ.

Большинство атак реализуются по предварительно заданным сценариям. Каждый сценарий состоит из последовательных стадий, предназначенных для преодоления различных уровней защиты. Сложные атаки на компьютерные сети могут затрагивать сразу несколько хостов сети и иметь целью поражение множества хостов. Они могут реализовываться посредством кооперации большой группы злоумышленников и использования множества хостов для инициирования отдельных фаз атаки из нескольких источников в сети. Реализованная в АСМА агентно-ориентированная технология позволяет адекватно моделировать распределенные скоординированные атаки. Кооперация распределенных агентов обнаружения вторжений может обеспечивать обнаружение атак, реализующих такие сложные сценарии.

Многоагентный подход обеспечивает повышение оперативности выполнения задач защиты в силу распараллеливания и автоматического выполнения решаемых задач. В разработанном прототипе МСОВ агенты IDA1 и IDA2 осуществляют обобщенный анализ обнаруженных фактов вторжения в рамках всей защищаемой сети. Это позволяет использовать режим автоматического обнаружения сложных координированных атак и минимизировать количество ложных срабатываний и пропусков атак.

Для больших распределенных систем крайне важна способность продолжать функционировать, когда ее компоненты разрушены или изолированы. СКЗ, имеющие централизованную архитектуру, могут легко поражаться злоумышленником, например, путем атаки «отказ в обслуживании» на хосты управления СКЗ. Как в АСМА, так и в МСОВ совокупность агентов, соответственно выполняющих атаку или

реализующих задачу обнаружения, на каждом из хостов может взять на себя необходимые функции генерации или обнаружения распределенной атаки.

Исключительно важной является способность компонентов СКЗ отслеживать состояние среды функционирования и приспосабливаться к ее изменениям. В разработанных прототипах агенты могут клонироваться для охвата всех необходимых в текущей ситуации задач защиты, обеспечения требуемой избыточности и параллелизма, а также обращаться к агентам других хостов для оказания помощи. Агенты, обладающие указанными характеристиками, автономно и асинхронно выполняющие свои функции, позволяют сформировать робастную и отказоустойчивую систему защиты.

Для повышения эффективности защиты различные подсистемы СКЗ должны взаимодействовать друг с другом на разных уровнях абстракции решений, сформированных каждой из них. Такой стиль функционирования и взаимодействия подсистем СКЗ, как показало исследование реализованных прототипов, определяет требуемый способ декомпозиции функций защиты и необходимые средства взаимодействия между подсистемами СКЗ. Данный подход естественным образом реализуется с использованием парадигмы многоагентной системы и позволяет препятствовать, обнаруживать и подавлять атаки на более ранних стадиях их развития.

Многоагентная система может составлять многокомпонентную вычислительную среду, независимую от аппаратных и программных средств, на которых она базируется. Это позволяет реализовать мощную и настраиваемую среду для реализации различных механизмов защиты информации компьютерных сетях.

Для защиты информационных ресурсов компьютерных сетей необходимо не только предупреждать, блокировать, обнаруживать и реагировать на действия нарушителей, но и отвлекать их от основных целей, заманивая на ложные информационные объекты, производить сбор информации о приемах, тактике и мотивации злоумышленников, осуществлять их идентификацию и разоблачение. Для выполнения этих подзадач могут быть использованы так называемые ложные информационные системы (ЛИС), называемые системами-имитаторами, обманными системами или системами-ловушками. ЛИС являются программно-аппаратными средствами обеспечения информационной безопасности, реализующие функции сокрытия и камуфляжа защищаемых информационных ресурсов, а также дезинформации нарушителей: захват данных («прослушивание» сетевого трафика и фиксация данных для последующего анализа); сбор и объединение данных от различных программных и аппаратных компонентов компьютерной сети, в частности сенсоров, межсетевых экранов, систем обнаружения вторжений, маршрутизаторов и др.; определение «свой-чужой» и переадресация несанкционированных запросов на ложные компоненты; фильтрация событий (для автоматической отбраковки несущественных и фокусировки на значимых событиях); обнаружение действий нарушителя; выявление источника угроз, трассировка и идентификация нарушителя (определение типа, квалификации и др.); обеспечение невозможности использования скомпрометированных компонентов (ресурсов) для атаки или для нанесения вреда другим системам после проникновения нарушителя в ЛИС; распознавание плана (стратегии) действий нарушителя; контроль действий нарушителя и реагирование на них, в том числе оповещение администратора о компрометации, блокирование действий нарушителя и др.; формирование плана действий компонентов ЛИС по имитации целевой информационной системы; заманивание и обман нарушителя (привлечение внимания, сокрытие реальной структуры защищаемой системы и ресурсов, камуфляж, дезинформация) за счет эмуляции сетевых сегментов, серверов, рабочих станций, в том числе передаваемого трафика, и их уязвимостей, автоматическое реагирование на действия нарушителя, в том числе оповещение администратора; удаленное администрирование, документирование, ввод сигнатур, профилей и др. (обеспечивает централизованное управление, основанную на правилах безопасности реакцию системы, подготовку отчетов и анализ тенденций); обеспечение интерфейса с администратором безопасности.

Обобщенная функциональная структура перспективной ЛИС представлена на рис. 2. Жирным шрифтом выделены базовые компоненты.

В общем случае ЛИС может обеспечить три уровня введения в заблуждение нарушителя (рис. 3): уровень сегмента (основных компонентов целевой системы) — на данном уровне ЛИС имитирует защищаемую целевую систему в целом, и при обнаружении атаки злоумышленник перенаправляется с целевой системы на компоненты ЛИС; уровень хоста — данный уровень предполагает размещение компонентов ЛИС, имитирующих отдельные хосты, в компьютерной сети целевой системы; уровень сервиса/приложения — в рамках хоста целевой системы каждое приложение/сервис формируется следующим образом: целевой модуль сервиса/приложения вместе с модулем обмана «вкладывается в обертку»; в режиме санкционированного использования при вызове сервиса/приложения управление передается целевому модулю; при обнаружении несанкционированного обращения управление передается модулю обмана. Для исследования возможностей перспективных ЛИС

разработаны их прототипы и ведутся эксперименты с различными компонентами ЛИС.

Выводы

В статье предложен подход к разработке и использованию интеллектуальных адаптивных систем киберзащиты. Подход основан на реализации интеллектуальных механизмов управления защитой и построении единой унифицированной среды для создания и поддержки функционирования систем защиты на всем их жизненном цикле, включая адаптивное управление политиками безопасности.

В статье более детально охарактеризованы предложенные авторами работы интеллектуальные механизмы киберзащиты, в частности механизмы, основанные на использовании интеллектуальных агентов, механизмы дезинформации злоумышленника, сокрытия и камуфляжа важных ресурсов и процессов, «заманивания» злоумышленника на ложные (обманные) компоненты.

Представлены также механизмы создания и поддержки функционирования системы киберзащиты, в том числе механизмы определения уровня кибербезопасности и моделирования поведения системы киберзащиты.

Рис. 2. Обобщенная функциональная структура ЛИС

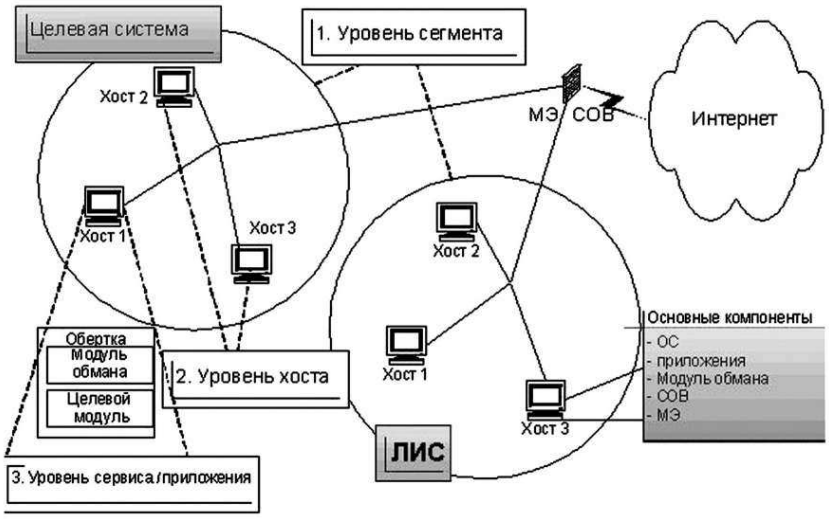

Рис. 3. Обобщенная архитектура ЛИС и реализуемые уровни введения в заблуждение

Литература

1. Miroshnik M. Uses of programmable logic integrated circuits for implementations of data encryption standard and its experimental linear cryptanalysis. / Miroshnik M., Kovalenko M. // Інформаційно-керуючі системи на залізничному транспорті. – 2013. – №6, с.36-45.
2. Мирошник М.А. Методы защиты цифровой информации в распределенных компьютерных сетях. Інформаційно-керуючі системи на залізничному транспорті. – 2014.– №5. – с. 66-70.
3. Мирошник М.А. Разработка средств защиты информации в распределенных компьютерных системах и сетях. / М.А. Мирошник // Інформаційно-керуючі системи на залізничному транспорті. – 2015. – №1. – с. 18-25.
4. Мирошник М.А. Проектирование компьютерных систем с интеллектуальной диагностической инфраструктурой. / М.А. Мирошник, В.Г. Котух, Э.Е. Герман // Радиотехника: Всеукраинский межведомственный научно-технический сборник.– Харків: ХНУРЕ, 2015. – Вип 180. – С. 64–67.
5. Miroshnik M. Implementation of cryptographic algorithms on FPGA-based digital distributed systems. / M. Miroshnik // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – Харків: УкрДУЗТ, 2015. – № 2 (111). – С. 25-30
6. Крылова В.А. Разработка методов оценки эффективности систем защиты информации в распределенных компьютерных системах / В.А. Крылова, А.Н. Мирошник // Інформаційно-керуючі системи на залізнич-ному транспорті: науково-технічний журнал. – Харків: УкрДУЗТ, 2015. – № 2 (111). – С. 43-51.
7. Мирошник М.А. Разработка интеллектуальной диагностической инфраструктуры в распределенных компьютерных системах. / М.А. Мирошник // Інформаційно-керуючі системи на залізничному транспорті: науково- технічний журнал. – Харків: УкрДУЗТ, 2015. – № 3 (112). – С. 3-9.
8. Мірошник М.А. Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах / М.А. Мірошник // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – Харків: УкрДУЗТ, 2015. – № 4 (113). – С. 39-43.
9. Мирошник М.А. Проектирование систем искусственного интеллекта с использованием нечеткой логики. / М.А. Мирошник, В.Г. Котух, Э.Е. Герман // Радиотехника: Всеукраинский межведомственный научно-технический сборник.– Харьков: ХНУРЭ, 2015. – Вып. 182. – С. 42–50.

Мірошник М.А., Крилова В.А., Демічев О.І. Застосування інтелектуальної діагностичної інфраструктури для управління кібербезпекою. Частина 1. Інтелектуалізація механізмів захисту. Кібербезпека в умовах глобальної інформатизації суспільства розглядається сьогодні як один з основних компонент національної безпеки. У роботі розглядається підхід до розробки і використання систем кіберзахисту, заснований на виділенні інтелектуальної надбудови над традиційними механізмами захисту і побудові єдиної уніфікованої середовища для створення та підтримки функціонування систем захисту. Представляються окремі механізми управління кібербезпекою.

Ключові слова: кібербезпека, інтелектуальна діагностична інфраструктура, мережеві атаки, мережа, доступ, автентифікація, шифрування, захист інформації, бази даних, моделі безпеки.

Miroschnyk Maryna, Krylova V.A., Demichev A.I. Application of intelligent diagnostic infrastructure to manage cybersecurity. Part 1. Intellectualization protection mechanisms. How use of structural features in the construction of hybrid models allows supporting of models adjustment and adaptation to problem-subject environment was considered in the article. The following features were attributed to structural ones: the type of learning algorithm; kind of activation function; the number of layers of the neural network; type of neurons; way of spreading information in neural networks; method of evaluating and interpreting the results of the neural network; the format of fuzzy inference rules; fuzzification and defuzzification method; way to implement the operations of fuzzy implication and logical operations NOT, AND, OR; kind of used genetic operators and the target functions, etc.

We propose to use a neural network approach as a basis for the decision of difficulty tasks using decision-support systems. Its effectiveness can be enhanced by: prior training or adjustment of individual neural modules for solvable problem; incorporation of knowledge about the peculiarities of the domain in the hierarchical (multilayer) neural networks structure; application of basic types of hybrid models in which neural network communicates with other information technologies.

Key words: methods of diagnosis, monitoring, complex failures, computer information management systems, distributed networks, network protocols, network attacks, routed service, authentication, encryption, data protection, database security model.

Рецензент Листровой С. В., д.т.н., професcор, професcор кафедры СКС (УкрГУЖТ)

Поступила 22.10.2015г.

Мірошник М.А., *д.т.н., професор кафедри СКС, Український державний університет залізничного транспорту, Харків, Україна.*
Крилова В.А., *к.т.н., доцент кафедри автоматики і управління в технічних системах, Національний технічний університет «Харківський політехнічний інститут», Харків, Україна.*
Демичев А.И., *аспирант кафедри СКС, Український державний університет залізничного транспорту, Харків, Україна.*

Miroschnyk Maryna*, Dr. of tech. science, Ukrainian State University of Railway Transport, Kharkiv, Ukraine.*
Krylova Victoria*, Ph.D., National Technical University "Kharkiv polytechnic Institute", Kharkiv, Ukraine.*
Demichev Oleksandr*, post-graduate student, Ukrainian State University of Railway Transport, Kharkiv, Ukraine.*