ПУТИ ПОСТРОЕНИЯ МНОГОАГЕНТНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Язов Ю.К.[1], Авсентьев А.О.[2]

Цель статьи: *показать перспективность создания и рассмотреть пути построения многоагентной системы защиты информации на объекте информатизации с реализацией децентрализованного и смешанного (централизованно-децентрализованного) принципа ее построения и функционирования в интересах исключения добывания различных видов информации, сведений о характеристиках объекта информатизации и взаимосвязях между его структурными элементами.*

Метод исследования: *применен метод функционально-структурного анализа технических каналов утечки сведений, циркулирующих в виде речевой информации на объектах информатизации органов внутренних дел в ходе их повседневной деятельности или при проведении служебных мероприятий, а также путей построения системы защиты информации от утечки по техническим каналам.*

Полученный результат: *определены факторы, учет которых необходим при обосновании состава и функций агентов многоагентной системы защиты информации в зависимости от условий, характеризующих динамику выполнения нарушителем действий по добыванию защищаемых сведений, динамику применения мер и средств защиты. Показано, что в состав многоагентной системы защиты могут входить два класса агентов – простые и интеллектуальные, а сама система должна представлять собой многослойную структуру, каждый слой которой привязан к определенному виду технических каналов утечки информации, и содержать один или несколько агентов (мета-агентов), обеспечивающих решение задач поддержки принятия решений по защите информации в каждом слое и в системе защиты в целом и управление другими агентами. Приведены примеры состава и структуры многоагентной системы защиты от утечки по техническим каналам, а также примеры структуры простого и интеллектуального агента для такой системы.*

Научная новизна *статьи состоит в том, что идея создания многоагентной системы впервые рассмотрена применительно к решению проблемы защиты информации от утечки по техническим каналам, определены состав, структура и функции таких систем, а также направления развития методического обеспечения их создания и функционирования.*

Ключевые слова: *машинное обучение, объект информатизации, техническое средство приема, технический канал утечки информации, интеллектуальный агент, средство защиты, база знаний.*

DOI:10.21681/2311-3456-2022-5-2-13

Введение

Различные объекты информатизации (ОИ) отличаются составом используемых информационных ресурсов, технических средств и систем обработки информации, используемыми информационными технологиями и средствами их обеспечения, архитектурными характеристиками зданий, сооружений и помещений, в которых эти средства и системы установлены, а также помещений и объектов, предназначенных для ведения конфиденциальных переговоров. При этом на ОИ осуществляется обработка информации в различных формах ее представления (речевой, видовой, буквенно-цифровой, графической и др.) с использованием материальных носителей различного вида (бумажных, электронных, сигнальных). Форма представления обрабатываемой информации и ее материальные носители могут меняться при переходе от этапа к этапу жизненного цикла ОИ и даже в пределах одного этапа, а время, в течение которого

1 Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник управления ФАУ «ГНИИИ ПТЗИ ФСТЭК России», г. Воронеж, Российская Федерация. E-mail: Yazoff_1946@mail.ru.

2 Авсентьев Александр Олегович, кандидат технических наук, доцент кафедры компьютерной безопасности и технической экспертизы ФГКОУ ВО «Воронежский институт Министерства внутренних дел Российской Федерации», г. Воронеж, Российская Федерация. E-mail: aoaao8787@mail.ru.

информация содержится в ОИ, ограничено и является случайным [1]. Указанные обстоятельства, с одной стороны, характеризуют динамику реализации информационных процессов на различных этапах существования ОИ, а с другой стороны, – определяют условия реализации угроз безопасности информации (УБИ), в том числе угроз утечки информации по техническим каналам [1, 2].

В связи с изложенным защита информации (ЗИ) на ОИ на каждом этапе его существования должна обеспечиваться с учетом динамики реализации информационных процессов, характеристик ОИ и изменяющихся во времени условий реализации нарушителем актуальных УБИ [1, 2].

Применительно к угрозам утечки информации по техническим каналам, возникающим за счет побочных информативных сигналов (например, за счет побочных электромагнитных излучений (ПЭМИ)) радиоэлектронных устройств (РЭУ) в составе ОИ, содержание реализуемых мер ЗИ обусловлено необходимостью учета условий возникновения технического канала утечки информации (ТКУИ), включающего источник (датчик) информации (ДИ), среду распространения информативного сигнала и приемник как техническое средство перехвата (ТСП), при помощи которого осуществляется обнаружение, прием этого сигнала, извлечение сообщения и его отображение в форме, удобной для нарушителя [3].

Меры ЗИ сегодня, как правило, реализуются в составе систем защиты информации (СЗИ), развертываемых на ОИ. В настоящее время СЗИ создаются по централизованному принципу, когда управление системой защиты осуществляется из одного центра управления, создаваемого на ОИ. Однако для больших ОИ, в состав которых могут входить десятки и сотни датчиков и аппаратных или программно-аппаратных элементов средств защиты, состав и настройки которых должны изменяться в динамике изменения обстановки, централизованное управления системой из-за большого количества процедур анализа и принятия решений по управлению с высокой вероятностью может приводить к сбоям. Не помогает в этом случае и создание многоканальных систем передачи данных в центр управления от датчиков, предназначенных для мониторинга инцидентов безопасности на ОИ, так как при этом не упрощаются процессы принятия решений в центре управления СЗИ по всей совокупности передаваемых от датчиков данных, то есть по всем возможным инцидентам безопасности на ОИ. Указанные обстоятельства, во-первых, обусловливают снижение эффективности защиты, во-вторых, не позволяют адекватно оценить защищенность информации на различных этапах существования ОИ.

Выходом из создавшейся ситуации представляется переход к децентрализованному или смешанному (централизованно-децентрализованному) принципу построения СЗИ в виде многоагентной системы защиты информации (МАСЗИ) [4]. В этом случае система решений в ходе управления защитой информации на ОИ распределяется между агентами МАСЗИ, а сами агенты распределяются по территории ОИ и его элементам.

До настоящего времени принципы построения многоагентных систем (МАС) рассматривались как зарубежными [5 – 7], так и отечественными [4, 8 – 14] специалистами в интересах применения в различных приложениях (в частности, для управления электросетями в Великобритании, для управления процессами в промышленных системах, для управления ансамблями динамических объектов, например, беспилотных летательных аппаратов и др.).

Кроме того, сегодня существует несколько международных подходов к созданию МАС, наиболее известные их них — это OMG MASIF, созданный компанией Object Management Group, в основе которого лежит понятие мобильный агент. Существует целый ряд стандартов, предложенных FIPA (Foundations for Intelligent Physical Agents), а также стандарты, разработанные исследовательским подразделением Пентагона — Агентством Передовых Оборонных Научных Исследований (Defense Advanced Research Projects Agency — DARPA), а также программные продукты, поддерживающие эти стандарты, такие как AnyLogic, Java Intelligent Agent Compontentware, The SPADE Multiagent and Organizations Platform, JACK Intelligent Agents, The FipaOS agent platform, AgentService, Zeus Agent Building Toolkit, JADE и др.

Следует отметить, что структура исследований в области МАС в настоящее время очень широка и сравнима с широтой исследований в области искусственного интеллекта.

В частности, в исследованиях, посвященных теории агентов, рассматриваются формализмы и математические методы для описания желаемых свойств агентов, архитектуры построения агентов и МАС в целом, методы, языки и средства коммуникации агентов, методы и программные средства поддержки миграции агентов и др. При этом в перспективных исследованиях значительное внимание уделяется динамической реорганизации МАС (изменения структуры и

поведения МАС с учетом внутренних и внешних условий), что является основным направлением развития адаптивных МАС.

Применительно к решению задач защиты информации также проводились исследования, но в основном в интересах защиты информации в компьютерных системах.

Так, в [8, 12] рассматривалась архитектура многоагентной системы обнаружения вторжений в компьютерную сеть, в [13] исследовались вопросы применения многоагентных технологий для индустриальных приложений и т.д. Однако, при этом вопросы построения МАСЗИ применительно к решению задач защиты информации от утечки по техническим каналам даже не упоминались.

Данная статья посвящена вопросам построения такого рода многоагентных систем, предназначенных для защиты информации на ОИ от утечки по техническим каналам.

1. Состав и функции агентов многоагентной системы защиты информации от утечки по техническим каналам

Перехват конфиденциальной информации по ТКУИ характеризуется энергетическими и частотными характеристиками физических полей, по которым осуществляется перехват, пространственным расположением средств перехвата и источников излучений, чувствительностью приемных устройств и др., а также динамикой передачи перехватываемых сообщений и действий нарушителя, составом и характеристиками мер и средств защиты и т.д. [15].

При выявлении состава агентов МАСЗИ и их функций следует учитывать необходимость [1, 3, 4, 15, 16]:

- обнаружения по демаскирующим признакам на территории, прилегающей к ОИ (к границам контролируемой зоны (КЗ) объекта) нарушителя, выполняющего действия, связанные с применением приемника в составе ТСП, в интересах формирования ТКУИ;
- блокирования действий нарушителя (внутреннего и внешнего) как непосредственно на территории ОИ (или в пределах КЗ объекта), так и на территории, прилегающей к объекту, выполняемых им в интересах формирования ТКУИ;
- локализации (на основе пассивных мер защиты) побочных информативных сигналов структурных элементов ОИ различного состава и назначения, как ДИ различной физической природы в структуре формируемых нарушителем ТКУИ;
- получение агентами данных о характеристиках информативных физических полей, как сред распространения побочных информативных сигналов различной физической природы (вид поля, протяженность, направленность и др.), а также о результатах измерения энергетических параметров побочных информативных сигналов различной физической природы (агентами-датчиками);
- оценку защищенности информации по результатам, полученным от агентов-датчиков, и принятие решения на применение мер и средств защиты;
- оценки необходимых параметров активных средств защиты, в частности параметров их излучений (пространственных и линейных), выбора мест размещения этих средств, как в пределах ОИ, так и с РЭУ бытового назначения за пределами объекта;
- реализации процедур выбора мер и соответствующих им средств защиты в зависимости от обстановки на ОИ – выявленных угроз возникновения (в связи с наличием побочных информативных сигналов) или формирования нарушителем ТКУИ (по признакам применения ТСП);
- активации и выключения средств защиты (в том числе превентивно установленных на ОИ), включенных в состав МАСЗИ;
- поиска в пределах ОИ (в пределах КЗ объекта) портативных закладочных устройств, установленных нарушителем на ОИ;
- наблюдения за оперативной обстановкой как в пределах ОИ, так и на территории, прилегающей к объекту (к границе КЗ), в интересах контроля и разграничения доступа (обеспечения КЗ);
- обеспечения взаимодействия агентов в условиях изменения оперативной обстановки как в пределах ОИ, так и на территории, прилегающей к объекту (к границам КЗ);
- реализации алгоритмов обучения агентов, например, по результатам анализа ранее измеренных энергетических параметров побочных информативных сигналов различной физической природы, характеристик пассивных и активных мер защиты информации, а также выявленных демаскирующих признаков закладочных устройств и действий нарушителя, применяющего ТСП.

Необходимость решения указанных задач и учет изложенных факторов обусловливает то, что перспек-

тивные МАСЗИ, во-первых, должны представлять собой многослойную структуру, каждый слой которой привязан к определенному виду ТКУИ, и содержать один или несколько агентов, обеспечивающих решения задач поддержки принятия решений по защите информации в интересах МАСЗИ в каждом слое и системы в целом и управление другими агентами. Во-вторых, МАСЗИ со смешанным принципом построения, как правило, будет иметь место зональная структура (кампусная, если ОИ находится в нескольких зданиях, зонально-территориальная или секторная ее структура, если в состав объекта включается определенная территория и рассматривается прилегающая к контролируемой зоне ОИ территория. При этом на нижних уровнях системы, как правило, будет иметь место смешанный принцип построения и управления агентами, а на верхних уровнях (для кампуса, зоны или сектора в целом) – централизованный принцип. Это обусловлено тем, что на ОИ, во-первых, применяются не только технические, но и организационные меры, выбор и управление которыми осуществляется только централизованно руководством организации (предприятия). Во-вторых, некоторые технические меры (касающиеся, например, корреляции моментов включения и выключения средств защиты в зависимости от сроков проведения мероприятия на ОИ, на котором обсуждается конфиденциальная информация, подлежащая защите) также могут выбираться централизованно.

Создание таких МАСЗИ обусловливает разработку соответствующего программно-аппаратного комплекса (ПАК), предназначенного для решения всей совокупности задач защиты от утечки информации на ОИ по техническим каналам[3].

В состав такого ПАК должны включаться два класса агентов: интеллектуальные агенты (ИА), в которых принимаются определенные решения в интересах защиты информации от утечки, и простые агенты (ПА), в которых не принимаются какие-либо решения. ИА строятся с использованием элементов искусственного интеллекта, а ПА являются традиционными программными или программно-аппаратными модулями, исполняющими функции датчиков (обнаружения, регистрации, измерения и др.), передачи команд, сигналов и данных из заранее определенного перечня, визуализации и т.д.

С учетом изложенного пример структуры и состава такой МАСЗИ от утечки по ТКУИ на ОИ приведен на рис. 1.

Следует отметить, что совокупность ИА, предназначенных для выработки решений по защите, в каждом слое МАСЗИ вырабатывает коллективные решения раздельно на активную и пассивную защиту в пределах каждой зоны (одного вида ТКУИ), эти решения затем передаются в верхний уровень, где централизованно выделяются необходимые активные и пассивные средства, определяются места их установки средств, сроки включения и т.д. на включение. Применительно к активным средствам это обусловлено тем, что такие средства могут функционировать в интересах пресечения утечки информации по ТКУИ в нескольких зонах, а относительно пассивных средств – тем, что их установка связана с выделением личного состава и соответствующих организационных решений.

С учетом состава и функционала агентов в МАСЗИ они могут быть объединены в пять функциональных подсистем:

- агентную платформу, которую в настоящее время целесообразно формировать как веб-платформу с клиент-серверной архитектурой. На ней содержатся все агенты МАСЗИ, она предоставляет интерфейс администратору и агентам МАСЗИ для доступа к базе знаний, к агентам МАСЗИ, к командам и данным, к телекоммуникационной среде и др.;
- центральную базу знаний (или хранилище знаний, которые содержат сведения о всех агентах МАСЗИ и их настройках по умолчанию, сведения о задействованных в определенный период времени агентов и установленных на них настройках, возможные команды в системе, результаты расчетов и оценки защищенности информации, данные от агентов датчиков, в том числе о нарушителях и применяемых ими ТСП, о составе мер и средств защиты, имеющихся и применяемых на ОИ и т.д.), а также базы данных и знаний в составе простых и интеллектуальных агентов с необходимой для их функционирования информацией;
- подсистему коммуникационного взаимодействия агентов, координации их поведения и управления ими, которая может быть составной

3 В настоящее время существует достаточно обширная номенклатура ПАК, предназначенных только для оценки защищенности информации от утечки по ТКУИ, например, такие как ПАК «Легенда-20» и различные модели ПАК «Навигатор» (ПЗМ – П6М), предназначенные для оценки защищенности информации от утечки по каналам ПЭМИ. ПАК «Колибри», «Шепот», «Тритон», «Рапира», «Талис» и другие применяются для оценки защищенности речевой информации от утечки по акустическим, вибро-акустическим и акустоэлектрическим каналам и др. Однако в настоящее время они применяются раздельно, а возможности их использования в составе МАСЗИ не рассматривались.

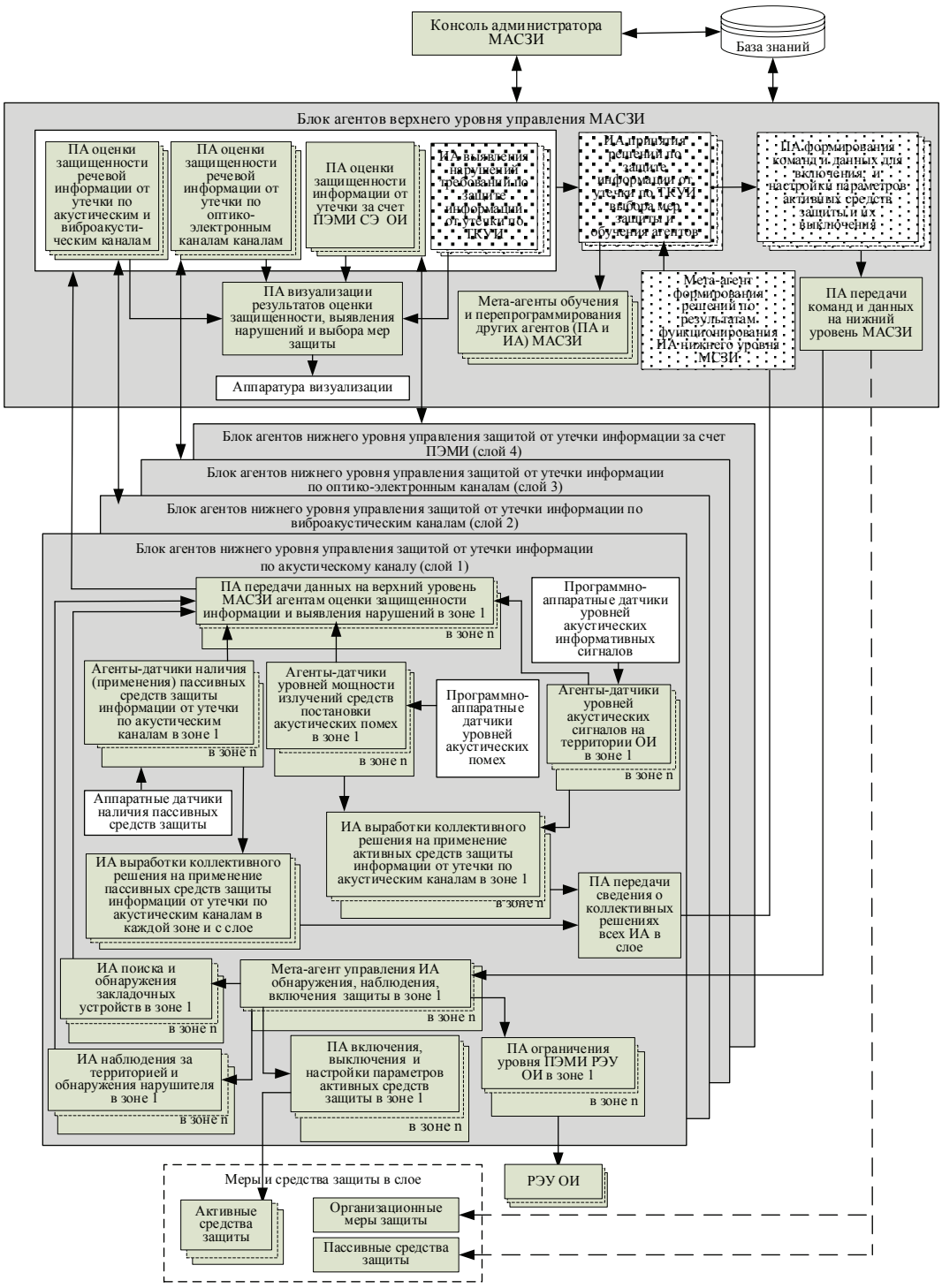

Рис. 1. Пример структуры и состава многоагентной системы защиты информации от утечки по техническим каналам на объекте информатизации

частью информационной системы предприятия (организации) или создаваться и функционировать как коммуникационной система, предназначенная для обеспечения функционирования только МАСЗИ;

— подсистему анализа и расчетов, предназначенную для оценки защищенности информации от утечки по ТКУИ, подготовки и обоснования решений по защите информации как на верхнем уровне МАСЗИ, так и при выработке решений интеллектуальными агентами на нижнем уровне;

— подсистему управляемых (подключаемых) средств защиты информации на ОИ от утечки по ТКУИ.

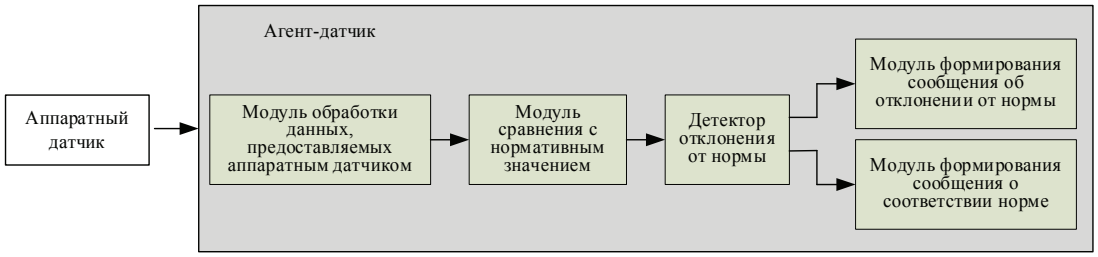

Рис. 2. Пример структуры простого агента-датчика

Наиболее сложным и наукоемким аспектом создания МАСЗИ является создание агентной платформы и, в частности, определение структуры, путей построения и алгоритмов функционирования агентов МАСЗИ.

2. Структуры и пути построения агентов для многоагентной системы защиты информации от утечки по техническим каналам

Рассматривая структуру и пути построения простых агентов, необходимо подчеркнуть, что в них не принимаются решения в интересах защиты информации, а лишь выполняются реализованные, как правило, программным путем определенные процедуры, такие как измерение, регистрация, передача данных, сведений и команд, наблюдение, поиск, распознавание ситуаций по зарегистрированным данным в соответствии с заданными признаками и критериями, включения, выключения средств защиты и управление их настройками в соответствии с заданными сценариями и др. Вместе с тем следует отметить, что некоторые из указанных процедур могут выполняться интеллектуальными агентами, такие как распознавание ситуаций, управления настройками и др. Реализуемые простым агентом функции полностью определяются его назначением, взаимосвязями с соответствующими агентами в МАСЗИ, функционирующими в интересах защиты информации от утечки по соответствующему ТКУИ (то есть в рамках одного слоя МАСЗИ). До сих пор применительно к задачам защиты информации от утечки по ТКУИ пути построения даже простых агентов для МАСЗИ не рассматривались. Функции таких агентов заранее предопределены и прописаны в базе данных (знаний) этого агента или в общей базе знаний системы, а в программе, реализующей агента, имеются программные модули, запрашивающие из базы необходимые данные и выполняющие соответствующие функции агента. Пример обобщенной структуры простого агента приведен на рис. 2.

Значительно более сложной, как правило, является структура ИА. Исследования последних десятилетий показывают, что создание ИА является весьма сложной задачей, требующей теоретического фундамента, при этом могут быть весьма разнообразные модели построения таких агентов. Наиболее известны три базовых модели ИА:

1) модель «разумного агента» (или модель «делиберативного агента»[4]). Такой агент должен содержать базу знаний, заполненную некоторыми формулами математической логики, функционировать в цикле: восприятие обстановки (обсервация) – логический вывод – действие; принятие решения о действиях на основе логического вывода. Основы строгой формализации знаний и действий делиберативного агента заложены Куртом Конолиге (Kurt Konolige)[5];

2) модель реактивного агента, обеспечивающего интеллектуальное поведение без явного символьного представления знаний и без явного абстрактного логического вывода, при этом интеллектуальное поведение возникает как результат взаимодействия агента со средой;

3) модель многослойного гибридного агента, в котором реализуются технологии предыдущих моделей агентов.

Изложенные идеи построения ИА целесообразно учесть при построении ИА для МАСЗИ от утечки по ТКУИ, однако при этом реализуемые функции должны быть увязаны с задачами защиты информации на ОИ.

Для построения ИА применяются те или иные элементы искусственного интеллекта, такие как:

- искусственные нейронные сети;
- методы машинного обучения;
- генетические алгоритмы;
- языки логико-лингвистического описания объектов и действий;

4 От англ. deliberate agent – разумный (преднамеренный, целенаправленный, заведомо определенный) агент

5 Модели интеллектуальных агентов впервые предложил Курт Конолиге (Kurt Konolige) еще в 1982 г. в своей работе: Konolige, K. A first-order formalization of knowledge find action for multi agent planning system : Machine Intelligence 10 / K. Konolige ; Ed. by J. E. Hayes, D. Michie, Y. Pao. – Chichester : Ellis Horwood, 1982. – P. 41-72.

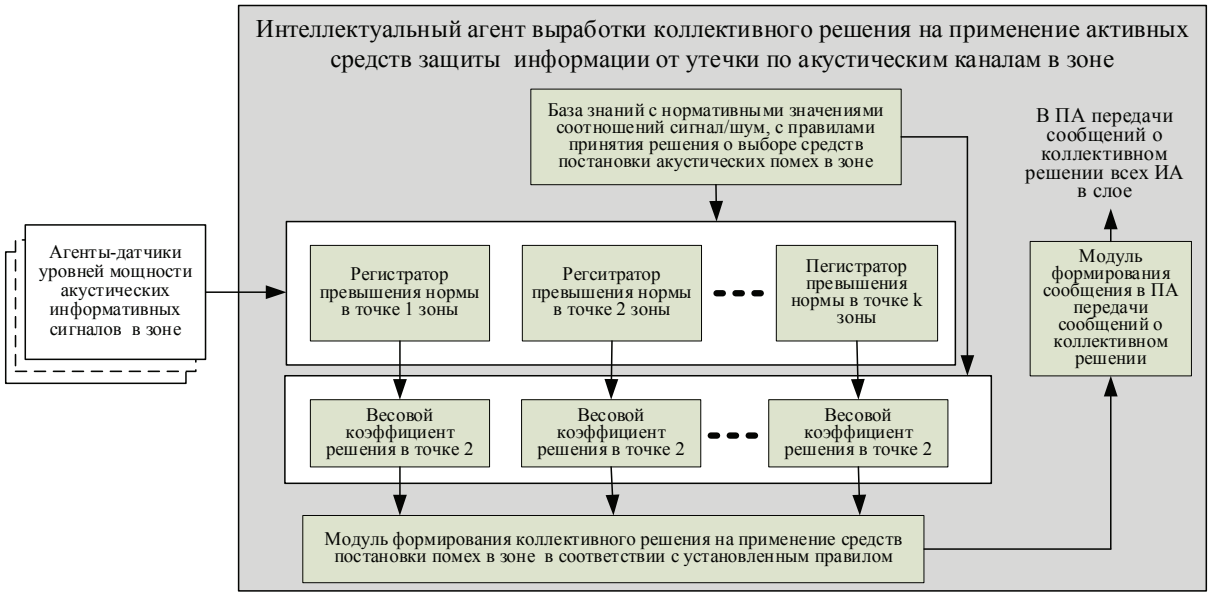

Рис. 3. Пример структуры интеллектуального агента, предназначенного для выработки коллективного решения на применение активных средств защиты информации от утечки по акустическим каналам в зоне

— аппарат теории нечетких суждений, нечетких множеств и нечеткой логики;
— математическая логика и теория предикатов[6], аппарат логических сетей и др.

Структура ИА будет существенно зависеть от того, какой метод или аппарат искусственного интеллекта применяется в ИА, и определяется в ходе проектирования такого агента. Пример структуры ИА, выполняющего функции формирования коллективного решения на основе данных от агентов-датчиков по защите информации от утечки по ТКУИ приведен на рис. 3.

Поскольку занимаются проблемами создания МАС крупные компании, сегодня разработаны несколько программных продуктов, позволяющих проектировать МАС. К ним относится, например, программное средство MASDK 4.0, разработанное СПИРАН [14], зарубежные средства agentTool, agentBuilder, PASSI, MASDK [16] и ряд других.

Вместе с тем разработанные средства оказываются практически неприменимы для создания МАСЗИ от утечки по ТКУИ, так как в них невозможно учесть специфику содержания задач, решаемых при защите информации от утечки по ТКУИ, и тем более выполняемых при этом функций агентами, их взаимодействия между собой, содержание команд и сообщений и т.д. В связи с этим требуется разработка специфических средств для автоматизации процессов проектирования рассматриваемых МАСЗИ.

3. Перспективы развития методического обеспечения создания многоагентных систем защиты информации от утечки по техническим каналам

Сегодня следует констатировать, что ни в России, ни за рубежом нет не только работ, посвященных разработке МАСЗИ от утечки по ТКУИ, но нет никаких исследований, посвященных развитию методического обеспечения создания таких систем защиты. На практике преимущественно используется методическое обеспечение оценки возможности перехвата информативных сигналов по энергетике.

Вместе с тем имеются многочисленные работы по методическому обеспечению организации и ведения технической защиты информации в информационных (компьютерных) системах, в том числе относящихся к критически важной информационной инфраструктуре Российской Федерации. По результатам анализа этих работ можно определить и направления развития методического обеспечения по проблеме создания МАСЗИ. На рисунке 4 приведены основные аспекты разработки методического обеспечения создания и функционирования перспективных МАСЗИ от утечки по ТКУИ.

6 По мере развития теории агентов в качестве базовой формальной модели интеллектуального агента специалистами была выбрана BDI-модель (BDI от англ. Belief–Desire–Intention, Убеждение–Желание–Намерение), в которой знания, намерения и механизмы рассуждений описываются в терминах исчисления предикатов, расширенного модальными и темпоральными операторами [16].

Рис. 4. Основные аспекты развития методического обеспечения создания и функционирования многоагентных систем защиты информации от утечки по техническим каналам для ОВД

Указанные на рисунке 4 и подлежащие разработке модели, алгоритмы и методики разрабатывались и для традиционных систем защиты информации с централизованным принципом построения. Однако есть и специфика, связанная с групповым поведение агентов и выработкой коллективных решений по защите информации, выбору мер и средств защиты и размещению средств по территории ОИ, с оценкой эффективности МАСЗИ и ее агентов и т.д. Кроме развития методологии создания МАСЗИ от утечки по ТКУИ, крайне важным для практики их создания является разработка программных средств проектирования МАСЗИ и их элементов для различных по назначению, составу и алгоритмам функционирования ОИ. Наконец, необходимо обратить внимание на создание и разработку моделей и методик оценки эффективности функционирования МАСЗИ с учетом фактора времени, а также алгоритмов распределенного применения

средств контроля состояния защищенности информации от утечки по ТКУИ на ОИ. До сих пор такие разработки не проводились.

Заключение

1. В настоящее время СЗИ создаются по централизованному принципу, когда управление системой защиты осуществляется из одного центра управления, создаваемого на ОИ. Однако для больших ОИ, в состав которых могут входить десятки и сотни датчиков и аппаратных или программно-аппаратных элементов средств защиты, состав и настройки которых должны изменяться в динамике изменения обстановки, централизованное управления системой из-за большого количества процедур анализа и принятия решений по управлению с высокой вероятностью может приводить к сбоям.

Выходом из создавшейся ситуации представляется переход к многоагентной системе защиты информации от утечки по техническим каналам.

2. До сих пор исследования, направленные на создание МАСЗИ от утечки по техническим каналам, не проводились. При выявлении состава агентов МАСЗИ и их функционала необходимо учитывать совокупность подлежащих выполнению функций, таких как обнаружение и блокирование действий нарушителя, локализация (на основе пассивных мер защиты) побочных информативных сигналов структурных элементов ОИ, получение агентами данных, необходимых для принятия решения на применение мер и средств защиты, управление средствами защиты, поиск закладочных устройств, оценка защищенности информации от утечки по ТКУИ и др. С учетом изложенного определена примерная структура МАСЗИ и состав включаемых в нее агентов (простых, интеллектуальных и мета-агентов). Отмечено, что перспективные МАСЗИ, во-первых, должны представлять собой многослойную структуру, каждый слой которой привязан к определенному виду ТКУИ, и содержать один или несколько агентов, обеспечивающих решения задач поддержки принятия решений по защите информации в интересах МАСЗИ в каждом слое и системы в целом и управление другими агентами. Во-вторых, МАСЗИ, как правило, будут иметь зональную структуру, поскольку ее элементы распределяются по территории ОИ, по различным зданиям и помещениям, что обусловливает распределение мер и средств защиты по зонам.

3. В настоящее время отсутствуют какие-либо исследования, посвященные развитию методического обеспечения создания и функционирования МАСЗИ от утечки по техническим каналам. На практике преимущественно используется методическое обеспечение оценки возможности перехвата информативных сигналов по энергетике. Предложенные подлежащие первоочередной разработки модели, алгоритмы и методики позволят на научной основе развернуть исследования по разработке эффективных МАСЗИ от утечки по техническим каналам и тем самым существенно повысить защищенность информации, циркулирующей в ОВД.

4. Научная новизна выполненного исследования состоит в следующем:

- во-первых, впервые предложено использовать многоагентные системы для решения проблемы защиты информации от утечки по техническим каналам;
- во-вторых, показано, что МАСЗИ должна включать в себя пять подсистем, в том числе агентную платформу с совокупностью простых и интеллектуальных агентов, базу знаний, подсистему коммуникационного взаимодействия агентов, подсистему анализа и расчетов и подсистему управляемых (подключаемых) средств защиты;
- во-третьих, на основе анализа состава, структуры и функций перспективных многоагентных систем защиты определены направления развития методического обеспечения создания и функционирования таких систем.

Литература

1. Avsentiev, O. S. Simulation of processes of information protection of informatization objects from leakage on technical channels using a Petri-Markov network apparatus / O.S. Avsentiev, A.O. Avsentiev, A.G. Krugov, Yu.K. Yazov. — Текст : электронный // Journal of Computational and Engineering Mathematics. — 2021. Т. 8. № 2. С. 32-41. — DOI: 10.14529/jcem210201. https://www.elibrary.ru/item.asp?id=46552937 (дата обращения: 19.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
2. Защита информации в информационных системах от несанкционированного доступа: монография / Ю. К. Язов, С. В. Соловьев. — Воронеж: Кварта, 2018. — 440 с. ISBN 978-5-93737-158-4. — Текст : непосредственный.
3. Авсентьев, О. С. К вопросу о формировании системы защиты информации от утечки по техническим каналам, возникающим за счет побочных электромагнитных излучений объектов информатизации / О. С. Авсентьев, А. Г. Вальде. Текст : электронный //

Вестник Воронежского института МВД России. — 2021. № 2. С. 22-33. https://www.elibrary.ru/item.asp?id=46221802 (дата обращения: 19.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
4. Городецкий, В. И. Многоагентные системы (обзор)/ В. И. Городецкий, М. С. Грушинский, А. В. Хабалов. — Текст электронный. — 2015. — URL: https://777russia.ru/ book/uploads/ОСНОВЫ%20РОБОТОТЕХНИКИ/Городецкий%20В.И.%2C%20Многоагентные%20системы%20%28обзор%29.doc. (дата обращения: 19.08.2022).
5. Wang, H. Multiagent hierarchical cognition difference policy for multiagent cooperation / H. Wang., J. Yi., Z. Pu., Z. Liu. – Текст : электронный // Algorithms. — 2021. Т. 14. № 3. — DOI: 10.3390/a14030098. https://www.elibrary.ru/item.asp?id=45984393 (дата обращения: 19.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
6. Hua, Y. Formation-containment tracking for general linear multi-agent systems with a tracking-leader of unknown control input / Y. Hua, X. Dong, L. Han, Q. Li, Z. Ren. -Текст : электронный // Systems & Control Letters, vol. 122, pp. 67–76, 2018. URL: https://www.semanticscholar.org/paper/Formation-containment-tracking-for-general-linear-a-Hua-Dong/40c82ecb36b79b62925895ef33ed9fa4316fef70 (дата обращения: 19.08.2022).
7. Wang, L. Distributed continuous-time containment control of heterogeneous multiagent systems with nonconvex control input constraints / Wang L., Li X., Zhang Y. -Текст : электронный // Complexity. 2022. Т. 2022. С. 7081091. — DOI: 10.1155/2022/7081091. https://www.elibrary.ru/item.asp?id=49058081 (дата обращения: 21.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
8. Грушо, Н. А. Сравнение архитектур многоагентных систем/ Н. А. Грушо, Е. Е. Тимонина. — Текст : электронный // Информационные технологии. — Москва. — 2019. Т. 25. № 5. С. 293-299. https://www.elibrary.ru/item.asp?id=38470623 (дата обращения: 21.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
9. Зайцев, Е. И. Многоагентные системы и многоагентные банки знаний / Е. И. Зайцев, И. В. Степанова, Р. Ф. Халабия. — Текст : электронный // Успехи современной науки. Белгород — 2017. Т. 4. № 4. С. 155-159. https://www.elibrary.ru/item.asp?id=29317763 (дата обращения: 23.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
10. Бежитская, Е. А. Многоагентные технологии в задачах управления/ Е. А. Бежитская, П. И. Казанцева. — Текст : электронный // Актуальные проблемы авиации и космонавтики. Сибирский государственный университет науки и технологий им. акад. М.Ф. Решетнева. Красноярск – 2018. Т. 2. № 4 (14). С. 289-291. https://www.elibrary.ru/item.asp?id=36804784 (дата обращения: 23.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
11. Хованских, С. А. Методика защиты распределенных вычислений в многоагентной системе / С. А. Хованских, В. А. Литвиненко, В. С. Хованскова. — Текст : электронный // Известия ЮФУ. Технические науки. 2019. № 4 (206). С. 68-80. — DOI: 10.23683/2311-3103-2019-4-68-80. https://www.elibrary.ru/item.asp?id=42197979 (дата обращения: 23.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
12. Кошелев, Д. А. Возможность применения многоагентной системы для обнаружения внедрения и атак / Д. А. Кошелев, Т.В. Корж. — Текст : электронный // Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А.С. Попова: Радиолокация, навигация, связь. В 6-ти томах. 2019. С. 106 – 113. https://www.elibrary.ru/item.asp?id=37394333 (дата обращения: 23.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
13. Листопад С.В. Стимуляция конфликтов агентов в гибридных интеллектуальных многоагентных системах / С. В. Листопад, И. А. Кириков. — Текст : электронный // Системы и средства информатики. 2021. Т. 31. № 2. С. 47-58. — DOI: 10.14357/08696527210205. https://www.elibrary.ru/item.asp?id=45824719 (дата обращения: 23.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
14. Городецкий, В. И. Многоагентные технологии для индустриальных приложений: реальность и перспектива / В. И. Городецкий, П.О. Скобелев. — Текст : электронный // Труды СПИИРАН, № 6 (55). 2017. С. 11–45. — DOI: 10.15622/sp.55.1. https://www.elibrary.ru/item.asp?id=30685497 (дата обращения: 23.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.нием строя роботов при динамически изменяющихся условиях // Искусственный интелект и принятие решений.
15. Авсентьев, А. О. Вербальная модель угроз утечки информации по техническим каналам в процессе создания объектов информатизации / А. О. Авсентьев, А. Г. Вальде. — Текст : электронный // Вестник Воронежского института МВД России. 2022. № 2. С. 65-75. https://www.elibrary.ru/item.asp?id=48732009 (дата обращения: 23.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.
16. Бежитская, Е. А. Обзор и сравнение программных средств для реализации многоагентных систем / Е. А. Бежитская, С. С. Бежитский, П. И. Казанцева. — Текст : электронный // Решетневские чтения. 2018. С. 102-103. https://www.elibrary.ru/item.asp?id=36741639 (дата обращения: 23.08.2022). — Режим доступа: Научная электронная библиотека eLIBRARY.RU.

INFORMATION PROTECTION FROM LEAKAGE THROUGH TECHNICAL CHANNELS ON THE BASIS OF ADAPTIVE MULTI-AGENT SECURITY SYSTEM AT THE INFORMATIZATION OBJECT

Yazov Yu.K.[7], Avsentiev A.O.[8]

Purpose: *to show the creation and consideration perspective of the ways to build a multi-agent information security system at an informatization object with the implementation of a decentralized and mixed (centralized-decentralized) principle of its design and functioning in order to exclude the extraction of various types of information, data about the characteristics of the informatization object and relationships between its structural elements.*

Method: *the method of functional and structural analysis of technical channels of leaking information circulating in the form of speech information at the informatization objects of the internal affairs bodies in the course of their daily activities or during official activities, as well as ways to build an information security system from leakage through technical channels is applied.*

Result: *the factors determined are those that are necessary to be taken into account when substantiating the composition and functions of agents of a multi-agent information security system, depending on the conditions characterizing the dynamics of the intruder's actions to obtain protected information, the dynamics of the application of measures and means of protection. It is shown that a multi-agent protection system composition can include two classes of agents - simple and intelligent, and the system itself must be a multilayer structure, each layer of which is tied to a certain type of technical information leakage channels, and contain one or more agents (meta-agents), which provide solution of decision support tasks for information protection in each layer and in the security system as a whole and control of other agents. Examples of the composition and structure of a multi-agent system for protecting against leakage through technical channels, as well as examples of the structure of a simple and intelligent agent for such a system are given.*

The scientific novelty *of the article is in the fact that the idea of creating a multi-agent system is considered for the first time in relation to solving the problem of protecting information from leakage through technical channels, the composition, structure and functions of such systems are determined, as well as the directions for the development of methodological support for their creation and operation.*

Keywords: *machine learning, informatization object, technical means of receiving, technical channel of information leakage, intelligent agent, means of protection, knowledge base.*

References

1. Avsentiev, O. S. Simulation of processes of information protection of informatiza-tion objects from leakage on technical channels using a Petri-Markov network apparatus / O.S. Avsentiev, A.O. Avsentiev, A.G. Krugov, Yu.K. Yazov. — Tekst : jelektronnyj // Journal of Computational and Engineering Mathematics. — 2021. T. 8. № 2. S. 32-41. — DOI: 10.14529/jcem210201. https://www.elibrary.ru/item.asp?id=46552937 (data obrashhe-nija: 19.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
2. Zashhita informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija / Ju. K. Jazov, S. V. Solov'ev. — Voronezh: Kvarta, 2018. — 440 s. ISBN 978-5-93737-158-4. — Tekst : neposredstvennyj.
3. Avsent'ev, O. S. K voprosu o formirovanii sistemy zashhity informacii ot utechki po tehnicheskim kanalam, voznikajushhim za schet pobochnyh jelektromagnitnyh izluchenij ob#ektov informatizacii / O. S. Avsent'ev, A. G. Val'de. Tekst : jelektron-nyj // Vestnik Voronezhskogo instituta MVD Rossii. — 2021. № 2. S. 22-33. https://www.elibrary.ru/item.asp?id=46221802 (data obrashhenija: 19.08.2022). — Rezhim do-stupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
4. Gorodeckij, V. I. Mnogoagentnye sistemy (obzor)/ V. I. Gorodeckij, M. S. Grushinskij, A. V. Habalov. — Tekst jelektronnyj. — 2015. —

7 Yury K. Yazov, Dr.Sc., Professor, Chief Researcher of the Department of FAU «GNIII PTZI FSTEC of Russia», Voronezh, Russia. E-mail: Yazoff_1946@mail.ru.

8 Alexander O. Avsentiev, Ph.D. of Engineering Sciences, Associate Professor of the Department of Computer Security and Technical Expertise of the Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation, Voronezh, Russian Federation. E-mail: aoaao8787@mail.ru.

URL: https://777russia.ru/ book/uploads/OSNOVY%20ROBOTOTEHNIKI/Gorodeckij%20V.I.%2C%20Mnogoagentnye%20sistemy%20%28obzor%29.doc. (data obrashhenija: 19.08.2022).
5. Wang, H. Multiagent hierarchical cognition difference policy for multiagent cooper-ation / H. Wang., J. Yi., Z. Pu., Z. Liu. – Tekst : jelektronnyj // Algorithms. — 2021. T. 14. № 3. — DOI: 10.3390/a14030098. https://www.elibrary.ru/item.asp?id=45984393 (data obrashhenija: 19.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
6. Hua, Y. Formation-containment tracking for general linear multi-agent systems with a tracking-leader of unknown control input / Y. Hua, X. Dong, L. Han, Q. Li, Z. Ren. -Tekst : jelektronnyj // Systems & Control Letters, vol. 122, pp. 67–76, 2018. URL: https://www.semanticscholar.org/paper/Formation-containment-tracking-for-general-linear-a-Hua-Dong/40c82ecb36b79b62925895ef33ed9fa4316fef70 (data obrashhenija: 19.08.2022).
7. Wang, L. Distributed continuous-time containment control of heterogeneous multi-agent systems with nonconvex control input constraints / Wang L., Li X., Zhang Y. -Tekst : jelektronnyj // Complexity. 2022. T. 2022. S. 7081091. — DOI: 10.1155/2022/7081091. https://www.elibrary.ru/item.asp?id=49058081 (data obrashhenija: 21.08.2022). — Rezhim do-stupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
8. Grusho, N. A. Sravnenie arhitektur mnogoagentnyh sistem/ N. A. Grusho, E. E. Timonina. — Tekst : jelektronnyj // Informacionnye tehnologii. — Moskva. — 2019. T. 25. № 5. S. 293-299. https://www.elibrary.ru/item.asp?id=38470623 (data obrashhe-nija: 21.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
9. Zajcev, E. I. Mnogoagentnye sistemy i mnogoagentnye banki znanij / E. I. Zajcev, I. V. Stepanova, R. F. Halabija. — Tekst : jelektronnyj // Uspehi sovre-mennoj nauki. Belgorod — 2017. T. 4. № 4. S. 155-159. https://www.elibrary.ru/item.asp?id=29317763 (data obrashhenija: 23.08.2022). — Rezhim do-stupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
10. Bezhitskaja, E. A. Mnogoagentnye tehnologii v zadachah upravlenija/ E. A. Bezhitskaja, P. I. Kazanceva. — Tekst : jelektronnyj // Aktual'nye problemy aviacii i kosmonavtiki. Sibirskij gosudarstvennyj universitet nauki i tehnologij im. akad. M.F. Reshetneva. Krasnojarsk – 2018. T. 2. № 4 (14). S. 289-291. https://www.elibrary.ru/item.asp?id=36804784 (data obrashhenija: 23.08.2022). — Rezhim do-stupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
11. Hovanskov, S. A. Metodika zashhity raspredelennyh vychislenij v mnogo-agentnoj sisteme / S. A. Hovanskov, V. A. Litvinenko, V. S. Hovanskova. — Tekst : jelektronnyj // Izvestija JuFU. Tehnicheskie nauki. 2019. № 4 (206). S. 68-80. — DOI: 10.23683/2311-3103-2019-4-68-80. https://www.elibrary.ru/item.asp?id=42197979 (da-ta obrashhenija: 23.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
12. Koshelev, D. A. Vozmozhnost' primenenija mnogoagentnoj sistemy dlja ob-naruzhenija vnedrenija i atak / D. A. Koshelev, T.V. Korzh. — Tekst : jelektronnyj // Sbor-nik trudov XXV Mezhdunarodnoj nauchno-tehnicheskoj konferencii, posvjashhennoj 160-letiju so dnja rozhdenija A.S. Popova: Radiolokacija, navigacija, svjaz'. V 6-ti to-mah. 2019. S. 106 – 113. https://www.elibrary.ru/item.asp?id=37394333 (data obrashhenija: 23.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
13. Listopad S.V. Stimuljacija konfliktov agentov v gibridnyh intellektu-al'nyh mnogoagentnyh sistemah / S. V. Listopad, I. A. Kirikov. — Tekst : jelektron-nyj // Sistemy i sredstva informatiki. 2021. T. 31. № 2. S. 47-58. — DOI: 10.14357/08696527210205. https://www.elibrary.ru/item.asp?id=45824719 (data ob-rashhenija: 23.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
14. Gorodeckij, V. I. Mnogoagentnye tehnologii dlja industrial'nyh prilozhenij: real'nost' i perspektiva / V. I. Gorodeckij, P. O. Skobelev. — Tekst : jelektronnyj // Trudy SPIIRAN, № 6 (55). 2017. S. 11–45. — DOI: 10.15622/sp.55.1. https://www.elibrary.ru/item.asp?id=30685497 (data obrashhenija: 23.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU. niem stroja robotov pri dinamicheski izmenjajushhihsja uslovijah // Iskusstvennyj intelekt i prinjatie reshenij. –
15. Avsent'ev, A. O. Verbal'naja model' ugroz utechki informacii po tehniche-skim kanalam v processe sozdanija ob#ektov informatizacii / A. O. Avsent'ev, A. G. Val'de. — Tekst : jelektronnyj // Vestnik Voronezhskogo instituta MVD Rossii. 2022. № 2. S. 65-75. https://www.elibrary.ru/item.asp?id=48732009 (data obrashhenija: 23.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.
16. Bezhitskaja, E. A. Obzor i sravnenie programmnyh sredstv dlja realizacii mnogoagentnyh sistem / E. A. Bezhitskaja, S. S. Bezhitskij, P. I. Kazanceva. — Tekst : jelektronnyj // Reshetnevskie chtenija. 2018. S. 102-103. https://www.elibrary.ru/item.asp?id=36741639 (data obrashhenija: 23.08.2022). — Rezhim dostupa: Nauchnaja jelektronnaja biblioteka eLIBRARY.RU.