ПРОБЛЕМНЫЕ ВОПРОСЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ С ПРИМЕНЕНИЕМ МНОГОАГЕНТНЫХ СИСТЕМ

Язов Ю. К.[1], Авсентьев А. О.[2]

DOI: 10.21681/2311-3456-2024-6-85-97

Цель статьи: *раскрыть проблемные вопросы защиты информации от утечки по техническим каналам, возникающим за счет побочных электромагнитных излучений, с применением перспективных многоагентных систем и управления ими, показать необходимость и пути количественной оценки эффективности такой защиты.*

Методы исследования: *применены методы морфологического и функционально-структурного анализа процессов распределенного управления защитой информации от утечки по техническим каналам, а также методы теории вероятностей и теории составных сетей Петри-Маркова в интересах моделирования и оценки эффективности процессов централизованно-децентрализованного управления защитой.*

Полученный результат: *показана актуальность создания многоагентной системы защиты информации от утечки по техническим каналам; отмечена необходимость управления защитой в таких системах, раскрыты особенности централизованно-децентрализованного (смешанного) принципа управления в многоагентной системе на примере защиты речевой информации от утечки по техническим каналам, возникающим за счет побочных электромагнитных излучений радиоэлектронного оборудования в составе объектов информатизации.*

Раскрыты проблемные вопросы построения подсистем управления в составе многоагентных систем защиты информации от утечки по техническим каналам, возникающим за счет побочных электромагнитных излучений, связанных с понятием и формированием показателей эффективности защиты, влиянием управления защитой на ее эффективность, распределения управляющих воздействий по субъектам управления. Приведены составная сеть Петри-Маркова, моделирующая процесс утечки речевой информации по побочным электромагнитным излучениям, и аналитические соотношения для расчета показателя эффективности управления защитой информации в многоагентной системе.

Научная новизна *статьи состоит в том, что в ней впервые поставлена проблема реализации смешанного принципа управления защитой информации от утечки по техническим каналам на основе многоагентной системы и рассмотрены первоочередные методологические аспекты количественной оценки эффективности такой защиты.*

Ключевые слова: *побочное электромагнитное излучение, управление защитой, смешанный принцип управления, эффективность защиты, эффективность управления, мера защиты, частный показатель, математическая модель.*

Введение

На объектах информатизации (ОИ), создаваемых в интересах обеспечения деятельности различных организаций, условия реализации информационных процессов по обработке информации могут значительно отличаться. Это обусловлено, во-первых, различиями форм представления этой информации и ее материальных носителей, во-вторых, использованием для ее обработки различных технических средств и систем, в-третьих, отличиями архитектурных характеристик зданий, сооружений и помещений, в которых эти средства и системы размещаются [1]. В связи с тем, что такого рода информационные процессы реализуются во времени, то в совокупности с указанными обстоятельствами это, с одной стороны, обусловливает специфику динамики этих процессов, а с другой – определяет условия реализации угроз безопасности информации, в том числе угроз ее утечки по техническим каналам (ТКУИ) [1, 2].

Меры защиты информации (ЗИ) от утечки по ТКУИ, как правило, реализуются в составе систем защиты информации (СЗИ), развертываемых на ОИ. Для их выбора и применения в составе СЗИ создается подсистема управления защитой. В настоящее время управление в функционирующих СЗИ осуществляется по централизованному принципу из одного центра управления в составе ОИ. В [3] отмечено, что на больших ОИ, включающих десятки и сотни датчиков и аппаратных или программно-аппаратных элементов средств защиты, состав и настройки которых необходимо изменять в динамике изменения обстановки, централизованное построение и управление системой из-за большого количества процедур анализа и принятия решений по управлению с высокой вероятностью может приводить к неадекватным решениям и, как следствие, к снижению эффективности защиты информации на ОИ. С целью

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

учета условий реализации разнородных процессов обработки информации на ОИ, ее перехвата по ТКУИ и защиты от перехвата в [3] предложено переходить к централизованно-децентрализованному (смешанному) принципу управления СЗИ на основе многоагентной системы защиты информации (МАСЗИ). В этом случае система решений в ходе управления защитой распределяется между агентами МАСЗИ, а сами агенты распределяются по территории ОИ и его элементам. Эффективность защиты информации как степень соответствия результата защиты, цели защиты в этих условиях следует рассматривать с учетом того, насколько эффективно управление МАСЗИ.

Следует отметить, что в настоящее время исследованиям, связанным с разработкой и применением многоагентных систем в других сферах деятельности, уделяется значительное внимание. В основном такие исследования посвящены развитию теории агентов, исследованию математических методов описания их свойств, архитектуры построения, как агентов, так и систем в целом, методов и средств их коммуникации, методов и программных средств поддержки миграции агентов и др. [4;5;6;7], а также[3,4,5]. Однако применение МАСЗИ от утечки по ТКУИ связано с необходимостью решения ряда проблемных вопросов построения таких систем, разработкой подсистем и алгоритмов управления мерами и средствами защиты[6], оценки эффективности ЗИ в МАСЗИ и эффективности управления ею и др., которые до настоящего времени применительно к ЗИ даже не рассматривались.

Данная статья посвящена вопросам управления защитой информации в МАСЗИ от утечки речевой информации по ТКУИ, возникающим за счет побочных электромагнитных излучений (ПЭМИ) радиоэлектронного оборудования в составе ОИ, оценки эффективности такого управления с учетом фактора времени. Конечно, рассмотреть все проблемные вопросы управления защитой в МАСЗИ в одной статье невозможно, поэтому ниже рассматриваются те из них, которые в первую очередь подлежат решению по данной проблеме.

1. Управление защитой информации от утечки по ПЭМИ с применением МАСЗИ и проблемные вопросы его реализации

Предшественниками многоагентных систем можно считать адаптивные системы, которые подстраивались под ситуацию или обстоятельства и адекватным образом меняли свое поведение или характеристики, чтобы обеспечить решение стоящих перед ними задач. Однако многоагентная система, рассматриваемая первоначально как совокупность агентов, выполняющих каждый свои функции (с адаптивными изменениями своих характеристик в ходе функционирования) без централизованного управления ими со стороны администратора системы (типа «оркестра без дирижера»), оказалась значительно сложнее просто адаптивной системы, так как система решений в ней и система управления объектами стали распределенными как по территории, так и по времени.

Агент в составе многоагентной системы — это самостоятельная программная система, «имеющая возможность принимать воздействие из внешнего мира, определяющая свою реакцию на это воздействие и формирующая ответное действие, изменяющая свое поведение с течением времени в зависимости от накопленной информации и извлеченных из нее знаний, обладающая мотивацией и способная после делегирования полномочий пользователем поставить себя на его место и принять решение, соответствующее ситуации»[7]. Создание таких агентов стало возможным за счет внедрения элементов искусственного интеллекта, однако их создание является достаточно сложной задачей.

В связи с изложенным скоро стало ясно, что такие системы с полностью децентрализованным управлением пока создать весьма сложно, а в некоторых случаях и нецелесообразно. Поэтому вполне логичным стал переход к многоагентным системам, в которых реализуется смешанный (централизованно-децентрализованный) принцип управления процессами и объектами. Это, конечно, «откат» к промежуточному варианту многоагентной системы, но он позволяет на основе имеющихся технологий создавать весьма продвинутые системы, в том числе в области ЗИ.

Применительно к МАСЗИ от утечки по ТКУИ в [3] был предложен вариант состава и структуры такой системы, однако при этом практически не затрагивались проблемные вопросы управления защитой в МАСЗИ и тем более оценки влияния такого управления на эффективность защиты.

Под управлением ЗИ на ОИ понимается совокупность целенаправленных воздействий на радиоэлектронное оборудование в составе ОИ и на средства защиты от утечки по ТКУИ, а также команд (указаний,

3 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: 15.10.2024).

4 Бежицкая Е. А., Казанцева П. И Многоагентные технологии в задачах управления // Актуальные проблемы авиации и космонавтики. 2018. Т. 2. № 4 (14). С. 289–291.

5 Городецкий В. И., Скобелев П. О. Многоагентные технологии для индустриальных приложений: реальность и перспектива // Труды СПИИРАН, № 6 (55). 2017. С. 11–45.

6 Фуртат И. Б. Адаптивное и робастное управление мультиагентными системами/ И. Б. Фуртат. – СПб: Университет ИТМО, 2016. – 155 с.

7 Бежицкая Е. А., Казанцева П. И. Многоагентные технологии в задачах управления // Актуальные проблемы авиации и космонавтики. 2018. Т. 2. № 4 (14). С. 289–291.

предписаний) подразделениям и должностным лицам на проведение организационных и организационно-технических мероприятий по решению задач ЗИ. Управление осуществляется организационными (организационно-техническими) и техническими мерами защиты. К организационным относятся меры, направленные, например, на поиск и задержание нарушителей на территории ОИ, введение ограничений на посещение ОИ или отдельных помещений и т.п. К организационно-техническим относятся меры организационного характера, реализуемые с применением технических средств, например, поиск с использованием специальной аппаратуры закладочных устройств, установка экранов и заземлений и др. К техническим мерам относятся меры технического характера, реализуемые с применением средств защиты. Цель управления состоит в своевременном (в том числе заблаговременном) применении адекватных мер защиты и достижении тем самым эффективной защиты информации от утечки по ТКУИ.

При применении организационных и организационно-технических мер защиты субъектом управления является орган управления защитой на ОИ (или уполномоченное должностное лицо), а объектом управления – выделенное для реализации мер защиты подразделение или должностные лица.

При применении технических мер защиты объектами управления являются средства защиты (средства постановки помех, экранирования, заземления и др.), а субъектами управления соответствующие интеллектуальные агенты или орган управления.

Управление в МАСЗИ включает в себя следующие действия:

- сбор необходимой для управления защитой информации, касающейся характеристик функционирующих каналов утечки информации за счет ПЭМИ (в том числе для выявления возможных датчиков информации и оценки уровней излучений ПЭМИ, по которым может перехватываться информация, для определения предполагаемого состава, характеристик и размещения технических средств перехвата, для выявления условий и характеристик среды распространения ПЭМИ и др.);
- оценку необходимости и возможности защиты перехватываемой информации и принятие решений по защите;
- выбор и организацию применения адекватных организационных (организационно-технических) и технических мер защиты с оценкой ожидаемой эффективности защиты с их применением;
- выделение, расстановку и включение (с последующим выключением) аппаратных средств защиты, настройку их параметров и контроль функционирования;
- контроль (мониторинг) эффективности защиты информации от утечки по техническим каналам.

Особенностями управления защитой в МАСЗИ являются:

- распределенность функций управления между интеллектуальными агентами системы и центральным органом управления защитой на ОИ;

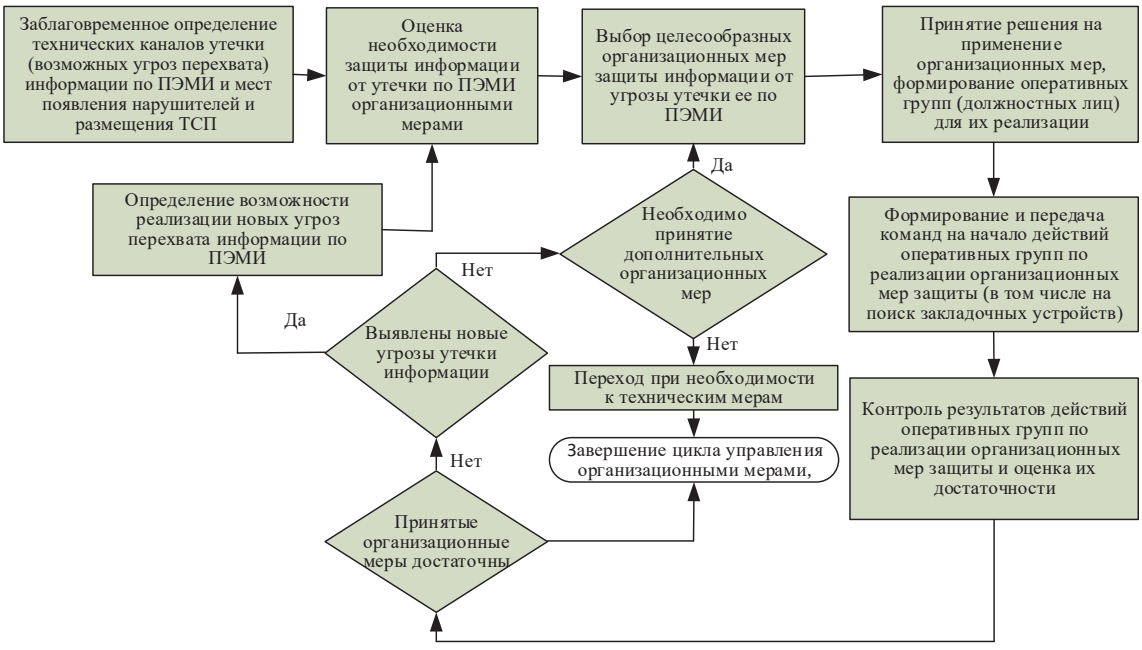


Рис. 1. Цикл управления организационными (организационно-техническими) мерами защиты информации от утечки по ПЭМИ на объекте информатизации

DOI: 10.21681/2311-3456-2024-6-85-97

- различие функций управления, реализуемых центральным органом управления при применении организационных (организационно-технических) и технических мер;
- различие функций управления при принятии заблаговременных и оперативных мер защиты;
- различие функций управления агентами, предназначенными: а) для сбора и обработки информации, необходимой для принятия мер защиты от утечки по ПЭМИ; б) для оценки возможностей и принятия решений по защите информации от утечки по ПЭМИ; г) для выявления функционирующего ТКУИ и подавления ТСП радиопомехами; д) для управления защитой от утечки по ТКУИ, содержащим различные ТСП (например, закладочные устройства, мобильные или стационарные ТСП);
- наличие случайных факторов, которые могут повлиять на управление защитой информации от утечки по ПЭМИ.

Описание циклов управления защитой информации при применении организационных и организационно-технических мер защиты применительно к каналам утечки по ПЭМИ приведено на рис. 1, а технических мер – на рис. 2.

Каждый из рассматриваемых циклов управления включает в себя две части: предварительную и непосредственную. В предварительной части управление заключается в заблаговременном анализе возможных угроз утечки информации по ПЭМИ (выявлении технических каналов утечки), которые могут быть в повседневной деятельности или при проведении различных мероприятий на ОИ (совещаний, сборов, конференций, комиссий и т.п.), в разработке модели действий нарушителя при перехвате ПЭМИ, оценке возможностей перехвата ПЭМИ различными ТСП – закладочными устройствами, мобильными (носимыми или возимыми) ТСП, стационарными средствами, которые могут устанавливаться в соседних с ОИ зданиях, в определении мер защиты, которые должны быть приняты и выполняться ежедневно при повседневной деятельности ОИ и которые могли бы быть приняты дополнительно при проведении на ОИ указанных мероприятий, в оценке ожидаемой эффективности мер защиты при повседневной деятельности на ОИ и др.

В непосредственной части управление защитой включает:

- отслеживание изменений, происходящих на ОИ и существенных для возникновения угроз утечки информации по ПЭМИ при повседневной деятельности;
- уточнение состава и оценку возможностей реализации угроз утечки информации по ПЭМИ в ходе конкретных мероприятий, проведение которых планируется на ОИ, в зависимости от их содержания и сроков проведения;
- уточнение совокупности мер защиты, которые должны применяться на ОИ при проведении очередного запланированного мероприятия на ОИ;

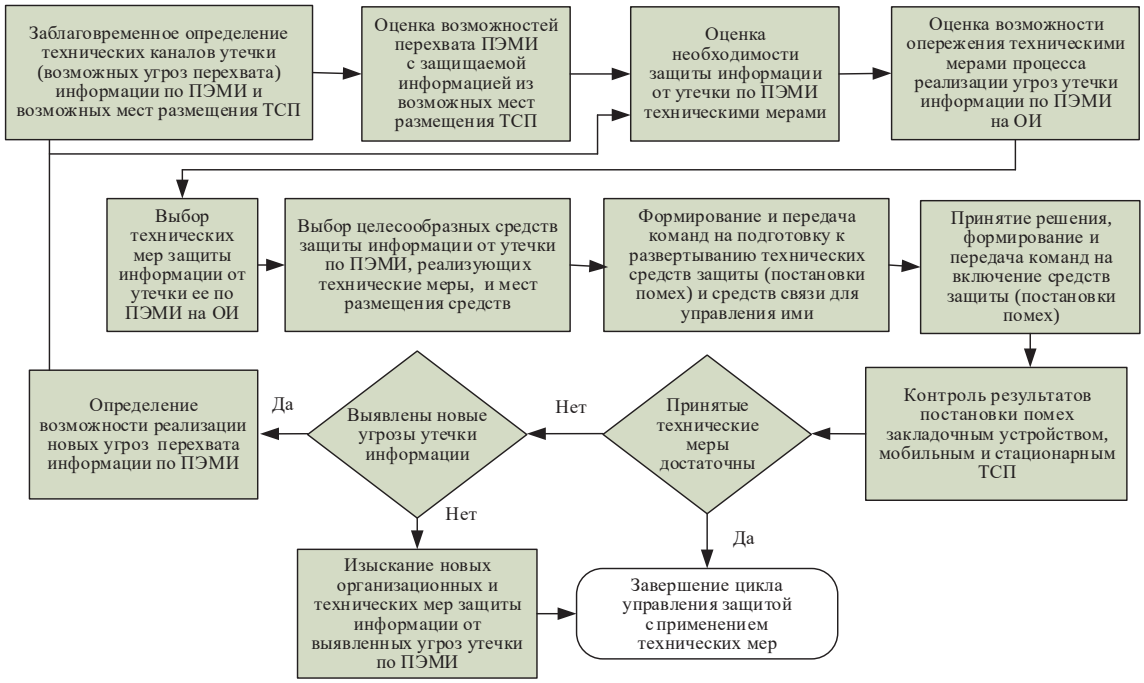


Рис. 2. Цикл управления техническими мерами защиты информации от утечки по ПЭМИ на объекте информатизации

- формирование состава сил и выбор технических средств для реализации организационных и технических мер защиты информации от утечки по ПЭМИ на очередном мероприятии, в том числе сил и средств для возможного усиления защиты при непредусмотренных изменениях условий защиты, касающихся состава и функционирования ОИ, деятельности нарушителей и функционирования ТСП;
- оценку необходимости и сроков применения активных технических средств защиты (постановки помех);
- оценку ожидаемой эффективности организационных и технических мер защиты на очередном подлежащем проведению мероприятии на ОИ;
- отслеживание изменений на ОИ (например, состава и характеристик развертываемого радиоэлектронного оборудования) в ходе проведения очередного мероприятия и в деятельности нарушителей (при наличии новых или отсутствии точных сведений о составе и размещении ТСП, о характеристиках динамики действий нарушителей на территории ОИ и за его пределами и др.);
- формирование и передачу команд на начало действий и отслеживание их выполнения выделенными оперативными группами для поиска на территории ОИ нарушителей и пресечения их деятельности, выявления и ликвидации закладочных устройств;
- формирование и передачу команд на начало применения активных средств защиты (постановки помех) и их выключения по мере надобности;
- контроль и проверка эффективности постановки помех для подавления ТСП информации по ПЭМИ.

При подготовке и реализации действий, как при предварительном, так и при непосредственном управлении защитой, имеет место целый ряд следующих подлежащих разрешению проблемных вопросов, связанных с функционированием и с созданием МАСЗИ.

1. Для создания подсистемы управления в МАСЗИ необходимо разработать линейку интеллектуальных агентов, то есть программных и программно-аппаратных средств на базе элементов искусственного интеллекта, позволяющих управлять техническими средствами защиты на ОИ от утечки по ПЭМИ, другими агентами (датчиками, средствами сбора данных, необходимых для управления, агентами обработки собираемых данных и выработки вариантов решений по ним, агентами передачи данных и т.д.).
2. Необходимо иметь средства защиты, которыми можно управлять с помощью интеллектуальных агентов, то есть включать, выключать, проводить настройку параметров (например, по частоте, мощности, направлению излучения).
3. Необходимо разработать комплекс средств для оснащения органа управления МАСЗИ, позволяющий решать всю совокупность задач, связанных с управлением защитой (например, программных средств для сбора обработки и предоставления данных, необходимых для применения мер и средств защиты, проведения расчетов при подготовке таких данных и др.).

До сих пор указанные проблемные вопросы, касающиеся практической части защиты информации от утечки по ТКУИ с использованием МАСЗИ, даже не ставились.

Функционирование МАСЗИ невозможно без соответствующего методического обеспечения управления защитой. Однако это связано с решением ряда проблемных вопросов и, в частности, касающихся понятий «эффективность защиты» и «эффективность управления защитой». Под эффективностью защиты информации принято понимать «степень соответствия результатов защиты информации поставленной цели»[8]. Эффективность характеризует меру приближения уровня защищенности информации к уровню, определенному целью защиты (чаще всего сегодня цель состоит в выполнении установленных нормативными документами требований). Однако в общем случае может быть и иная цель или несколько иерархически упорядоченных целей (рис. 3).

Так как формулирование целей защиты является прерогативой обладателя информации, то оценка эффективности ее защиты в этом смысле является субъективной (за исключением случая, когда обладателем является государство или ведомство, осуществляющее целеполагание). Многообразие возможных целей и содержания защищаемой информации обусловливает наличие проблемы создания единой методологии оценки эффективности ее защиты.

Еще более сложным оказывается проблемный вопрос оценки эффективности управления защитой. Несмотря на то, что исследования, касающиеся вопросов управления объектами, войсками, организациями и т.д. проводятся уже много десятилетий, методологические аспекты оценки его эффективности применительно к проблематике ЗИ практически не развиты, а сама оценка ограничивается использованием, в основном, качественных частных показателей, например, таких как устойчивость, непрерывность, оперативность и скрытность управления.

Попытки разработки математической модели оценки эффективности защиты информации от утечки по ПЭМИ были предприняты, например, в [2],

8 ГОСТ Р 50922 – 2006 г. Защита информации. Основные термины и определения.

Рис. 3. Иерархия возможных целей защиты информации от утечки по ПЭМИ в организации (на предприятии)

на основе применения количественных показателей. Было показано, что при таком моделировании необходимо использовать аппарат составных сетей Петри-Маркова для учета фактора времени и различных логических условий реализации угроз утечки информации по ТКУИ. Однако в этой работе даже не стоял вопрос разработки математической модели оценки эффективности управления защитой. Вместе с тем следует подчеркнуть, что отсутствие учета фактора времени делает оценку эффективности управления защитой информации несостоятельной. Однако какие-либо математические модели управления защитой от утечки по ТКУИ с учетом фактора времени сегодня отсутствуют.

Кроме этого, эффективность управления защитой с использованием количественных показателей можно оценивать, по крайней мере, двумя путями:

- во-первых, по его влиянию на эффективность защиты информации от утечки. В этом случае оценивается изменение показателя эффективности защиты (или показателя повышения защищенности информации) в результате применения мер защиты.
- во-вторых, по результативности самого управления, то есть достижения цели управления. Такими целями могут быть, например, своевременное применение адекватных мер защиты от утечки по ПЭМИ (оперативность управления) или опережение мерами защиты процесса реализации угрозы утечки информации по ПЭМИ.

Такая многоаспектность оценки должна быть учтена при разработке единого методического обеспечения оценки эффективности управления защитой. При этом при оценке по каждому из указанных путей также имеют место проблемные вопросы методологического характера, которые рассматриваются далее.

2. Система показателей оценки эффективности защиты информации от утечки по ПЭМИ в МАСЗИ и управления защитой

Наряду с тем, что оценка эффективности управления защитой и, соответственно, необходимое для этого методическое обеспечение (см. раздел 1), а в случае оценки его эффективности по влиянию на эффективность защиты также от цели самой защиты, имеет место ряд других важных факторов, подлежащих учету при такой оценке, к которым относятся следующие.

Во-первых, при централизованно-децентрализованном управлении защитой крайне важным становится взаимосвязь иерархически формируемых решений по управлению. Действительно, чтобы принять решение на включение и соответствующую настройку средства постановки помех, необходимо иметь решения органа управления, касающиеся применения средства, объекта воздействия, места размещения средства, направления или сектора постановки помехи. Тогда интеллектуальный агент принимает решения по выбору диапазона частот, времени включения и выключения (в зависимости от, например, наличия ПЭМИ с защищаемой речевой информацией по данным от агентов-датчиков), а также по выдаче команд для проведения необходимых настроек управляемого средства защиты. Сегодня система таких взаимосвязанных решений пока отсутствует. Вместе с тем от нее существенно зависит эффективность управления защитой как интеллектуальными агентами, так защитой в МАСЗИ в целом.

Во-вторых, сегодня отсутствует система показателей оценки эффективности управления защитой в МАСЗИ с использованием централизованно-децентрализованного принципа управления; и тем более математические модели для их расчета не разрабатывались.

Применительно к предварительным действиям, направленным на реализацию организационных и организационно-технических мер защиты, эффективность управления оценивается тем, насколько адекватными являются принятые меры защиты, то есть, по сути, соответствуют эффективности защиты информации на ОИ.

Применительно к техническим мерам эффективность управления может оцениваться как по влиянию на эффективность защиты, так и по достижению частной цели управления. На рис. 4 показан вариант системы таких показателей, включающей в себя интегральные и частные показатели. При этом показатель оценки эффективности управления защитой в МАСЗИ в целом (интегральный показатель) представляет собой функционал, определяемый через вероятности реализации совокупности угроз утечки информации в отсутствии и при применении организационно-технической системы управления. Для оценки функционирования элементов МАСЗИ, а также для учета различных условий и существенных факторов, влияющих на эффективность управления, могут применяться частные показатели, примеры которых показаны на рис. 4. Рассматривая вариант, когда эффективность непосредственного управления оценивается по влиянию на эффективность защиты, необходимо отметить, что в [13] предлагалось с использованием теории рисков применять в качестве интегральных показателей эффективности защиты следующие:

разностный – $\eta_d(t) = 1 - R^{(ЗИ)}(t)$; (1)

относительный – $\eta_r(t) = \frac{R^{(ЗИ)}(t)}{R^{(0)}(t)}, R^{(0)} > 0$; (2)

относительный разностный –

$$\eta_{rd}(t) = \frac{\left|R^{(0)}(t) - R^{(ЗИ)}(t)\right|}{R^{(0)}(t)}, R^{(0)} > 0, \quad (3)$$

где $R^{(ЗИ)}(t)$ и $R^{(0)}$ – риски при реализации угроз утечки информации в условиях применения и отсутствия мер защиты соответственно, при этом для u-й угрозы риск ее реализации определяется как $R_u(t) = \overline{\zeta_u} \cdot P_u(t)$, $\overline{\zeta_u}$ – математическое ожидание ущерба, наносимого при ее реализации, а $P_u(t)$ – вероятность реализации u-й угрозы. Наиболее удобным и нашедшим применение в практике анализа угроз стал относительный разностный показатель.

В условиях управления защитой вероятность парирования угрозы, как правило, ниже, чем при его отсутствии. Тогда по аналогии эффективность управления защитой от u-й угрозы может быть оценена интегральным относительным разностным показателем, который с учетом того, что меры защиты и управление ими, если не исключают возможности реализации угрозы, не влияют на возможный ущерб от ее реализации, рассчитывается по формуле:

$$\eta_{rd}^{(u)}(t) = \frac{\left|P_{u0}^{(ЗИ)}(t) - P_{uy}^{(ЗИ)}(t)\right|}{P_{u0}^{(ЗИ)}(t)}, \quad (4)$$

где $P_{u0}^{(ЗИ)}(t)$ и $P_{uy}^{(ЗИ)}(t)$ – вероятности реализации u-й угрозы в условиях применения мер защиты без управления и с управлением ими соответственно.

Если на ОИ выявлено U угроз утечки информации, реализуемых с вероятностями $P_{u0}^{(ЗИ)}(t)$ и $P_{uy}^{(ЗИ)}(t)$, и все

Рис. 4. Система показателей эффективности управления защитой в МАСЗИ по влиянию на эффективность защиты[9]

9 Здесь не учитываются показатели оценки устойчивости, непрерывности и скрытности управления, которые в общем случае также нужно количественно оценивать для учета факторов возможного негативного воздействия на систему управления со стороны нарушителя

угрозы парируются, то показатель эффективности управления рассчитывается следующим образом:

$$\eta_{rd}^{(u)}(t) = \frac{\left| \prod_{u=1}^{U} P_{u0}^{(ЗИ)}(t) - \prod_{u=1}^{U} P_{uy}^{(ЗИ)}(t) \right|}{\prod_{u=1}^{U} P_{u0}^{(ЗИ)}(t)}. \quad (5)$$

Если необходимо парировать и парируются только k угроз из U, то

$$\eta_{rd}^{(u)}(t) = \left| \frac{\frac{1}{k!} \cdot \frac{d^k}{ds^k} \left\{ \prod_{u=1}^{U} \left[1 - P_{u0}^{(ЗИ)}(t) + s \cdot P_{u0}^{(ЗИ)}(t) \right] - \prod_{u=1}^{U} \left[1 - P_{uy}^{(ЗИ)}(t) + s \cdot P_{u0}^{(ЗИ)}(t) \right] \right\}}{\frac{1}{k!} \cdot \frac{d^k}{ds^k} \left\{ \prod_{u=1}^{U} \left[1 - P_{u0}^{(ЗИ)}(t) + s \cdot P_{u0}^{(ЗИ)}(t) \right] \right\}} \right|_{s=0}. \quad (6)$$

Однако расчет такого показателя обусловливает необходимость разработки соответствующих математических моделей для оценки вероятностей реализации каждой угрозы. Ниже предлагается подход к оценке такого показателя эффективности с применением математических моделей, разрабатываемых на основе аппарата составных сетей Петри-Маркова [8, 9].

3. Математическая модель оценки эффективности управления средствами защиты информации от утечки по ПЭМИ

Рассмотрим часто встречающуюся на практике ситуацию, когда необходимо осуществить защиту речевой информации в ходе проведения некоторого мероприятия (совещания, сбора, конференции и т.п.) от утечки по ПЭМИ с применением средства постановки помех. Мероприятие проводится в ограниченный период времени, а конфиденциальная информация может быть перехвачена по ПЭМИ при эпизодическом появлении нарушителя на территории ОИ и развертывания, например, мобильного (на автомобиле) средства перехвата.

Управление средством защиты может осуществляться или органом управления МАСЗИ, или интеллектуальным агентом. И тот, и другой субъект управления, по сути, осуществляет одни и те же действия в ходе управления, при этом полагается, что вся первоначально необходимая информации для управления (решение органа управления, касающееся применения средства защиты, объект воздействия, место размещения средства защиты, направление или сектор постановки помехи) имеется. В ходе постановки помех на интеллектуальный агент в составе МАСЗИ могут поступать данные от органа управления, касающиеся появления вероятного нарушителя с мобильным средством перехвата ПЭМИ, от агентов-датчиков – возникновения ПЭМИ, по которому может перехватываться конфиденциальная информация с началом мероприятия, а также данные о диапазоне частот, в котором обнаружено ПЭМИ, виде модуляции, уровне излучения и др. В результате получения новых данных средство постановки помех перестраивается интеллектуальным агентом или непосредственно органом управления МАСЗИ. Элементы МАСЗИ, которые задействуются в ходе оперативного управления средством защиты, могут функционировать как параллельно друг другу, так и последовательно, при этом крайне важным становится учет фактора времени, без чего оценка эффективности управления оказывается несостоятельной. Как показано в [2], для моделирования таких процессов целесообразно использовать аппарат составных сетей Петри-Маркова (ССПМ) [9]. Графы ССПМ для случаев, когда отсутствует и имеется управление защитой, приведены на рис. 5[10].

Математическое ожидание времени срабатывания ССПМ при отсутствии управления мерами защиты (перемещения процесса в состояние 5) определяется из соотношения:

$$\overline{\tau_{u0}^{(ЗИ)}} = \begin{cases} \overline{\tau_{01}} + \overline{\tau_{32}} + \dfrac{\overline{\tau_{44}}}{P_{ПЭМИ}}, & \text{если нарушитель обнаруживает ПЭМИ в условиях помех с вероятностью } P_{ПЭМИ}; \\ \overline{\tau_{01}} + \overline{\tau_{33}}, & \text{если нарушитель, обнаружив помеху, меняет свое местоположение и продолжает перехват ПЭМИ без помех.} \end{cases} \quad (7)$$

где $\overline{\tau_{32}}$, $\overline{\tau_{33}}$ и $\overline{\tau_{44}}$ – математические ожидания времен перемещения процесса[11] соответственно (см. рис. 5а) по дугам (3,2z), (3, 3z), и (4,4z); $\overline{\tau_{01}}$ – математическое ожидание времени срабатывания перехода 1z,

$$\overline{\tau_{01}} = \overline{\tau_{00}} + \frac{\overline{\tau_{11}}^2 + \overline{\tau_{11}} \cdot \overline{\tau_{21}} + \overline{\tau_{11}}^2}{\overline{\tau_{11}} + \overline{\tau_{21}}}; \quad (8)$$

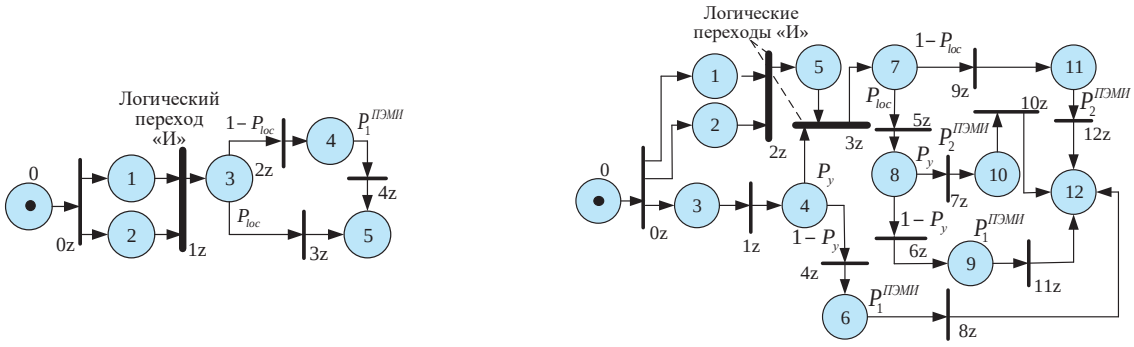
$\overline{\tau_{00}}$, $\overline{\tau_{11}}$ и $\overline{\tau_{21}}$, – математические ожидания времен перемещения процесса соответственно по дугам (0,0z), (1, 1z) и (2,1z).

Вероятность реализации угрозы в условиях отсутствия управления защитой при экспоненциальном приближении для распределений случайных времен переходов моделируемого процесса из состояний в переходы [12] определяется из соотношения:

$$P_{u0}^{(ЗИ)}(t) = (1 - P_{loc}) \cdot \left[1\text{-}\exp\left(- \frac{t}{\overline{\tau_{01}} + \overline{\tau_{32}} + \dfrac{\overline{\tau_{44}}}{P_1^{ПЭМИ}}} \right) \right] + P_{loc} \cdot \left[1 - \exp\left(- \frac{t}{\overline{\tau_{01}} + \overline{\tau_{33}}} \right) \right] \quad (9)$$

10 Время перемещения процесса из перехода в состояние считается в теории ССПМ мгновенным, а из позиции в переход конечным и случайным. Номер позиции обозначается цифрой, а перехода – цифрой с буквой z.

11 Здесь первая цифра указывает номер позиции, а вторая – номер перехода. Если какой-либо из номеров или оба номера являются двузначными, то они разделяются запятой.



а)

0 – начато мероприятие на ОИ, ожидается появление нарушителя на территории ОИ, подготовлено развертывание средства защиты, сформирована информация о возможном нарушителе, средстве перехвата и вероятном месте его развертывания;

1 – средство защиты развернуто и с началом мероприятия включено;

2 – нарушитель появился на территории ОИ, развернул средство перехвата и начал поиск ПЭМИ;

3 – нарушитель обнаружил ПЭМИ с защищаемой речевой информацией и помехи приемнику, но с вероятностью $1 - P_{loc}$ не стал менять своего местоположения, а с вероятностью P_{loc} сменил местоположение и пытается перехватить ПЭМИ в условиях, по сути, отсутствия помех;

4 – нарушитель, не меняя местоположения, начал перехват ПЭМИ в условиях помех с вероятностью $P_1^{\text{ПЭМИ}}$;

5 – угроза перехвата ПЭМИ реализована;

0z – передача команды на развертывание средства защиты и передача ориентировочной информации о нарушителе;

1z – логический переход с логикой «И», срабатываемый, если осуществлена настройка средства защиты, нарушитель предположительно появился на территории и начал поиск ПЭМИ, на ОИ начались мероприятия и возникла возможность перехвата речевой информации по ПЭМИ нарушителем;

2z – нарушитель настраивает ТСП для перехвата ПЭМИ с конфиденциальной информацией в условиях помех;

3z – нарушитель меняет свое местоположение и развертывает ТСП, перехватывает ПЭМИ с нового местоположения;

4z – с вероятностью $P_1^{\text{ПЭМИ}}$ нарушитель перехватывает ПЭМИ в условиях помех.

б)

0 – начато мероприятие на ОИ, ожидается появление нарушителя на территории ОМ, подготовлено средство защиты, собрана информация о возможном нарушителе и средстве перехвата;

1 – включены агенты-датчики для выявления нарушителя на территории с применением средств видеонаблюдения и для отслеживания появления ПЭМИ, а также интеллектуальные агенты подготовки данных, необходимых для постановки помехи;

2 – средство защиты развернуто и готово к включению;

3 – нарушитель появился на территории ОИ, развернул средство перехвата и начал поиск ПЭМИ, включена МАСЗИ;

4 – агентами-датчиками с вероятностью P_y выявлено место расположения предполагаемого нарушителя на территории ОИ, получены данные для применения средства постановки помех для передачи на интеллектуальный агент управления средством защиты (реализован цикл управления защитой) и с вероятностью $1 - P_y$ полный цикл управления защитой сорван;

5 – включено средство защиты (постановки помех);

6 – нарушитель с вероятностью $P_1^{\text{ПЭМИ}}$ перехватил ПЭМИ в условиях помех;

7 – нарушитель обнаружил ПЭМИ с защищаемой речевой информацией и наличие помех приемнику, при этом с вероятностью P_{loc} принимает решение сменить, а с вероятностью $1 - P_{loc}$ остаться на том же месте и продолжить попытки перехвата;

8 – нарушитель с вероятностью P_{loc} сменил местоположение, агентами-датчиками начат поиск нового местоположения нарушителя на территории ОИ;

9 – агентами-датчиками с вероятностью $1 - P_y$ не удалось реализовать полный цикл управления защитой, постановка помех начата по неточным данным, нарушитель начал перехват ПЭМИ с вероятностью $P_1^{\text{ПЭМИ}} \geq P_2^{\text{ПЭМИ}}$;

10 – агентами-датчиками с вероятностью P_y реализован цикл управления постановкой помех по выявленным новым данным о нарушителе, средство защиты настроено по новым данным и включено, нарушитель с вероятностью $P_2^{\text{ПЭМИ}}$ перехватил ПЭМИ в условиях помех;

11 – нарушитель, не меняя местоположения, продолжил с вероятностью $P_2^{\text{ПЭМИ}}$ перехват информации по ПЭМИ в условиях помех;

12 – угроза перехвата речевой информации по ПЭМИ в ходе проведения мероприятия на ОИ реализована;

0z – передача команды на развертывание средства защиты, формирование ориентировочной информации о нарушителе и средстве перехвата;

1z – выявление нарушителя на территории средствами наблюдения, проведение расчетов, необходимых для постановки помех, передача команды на применение средства защиты;

2z – логический переход с логикой «И», срабатывающий, если развернуто средство защиты, нарушитель появился на территории и начал поиск ПЭМИ;

3z – логический переход с логикой «И», срабатывающий, если с вероятностью P_y реализован цикл управления средством защиты и началась постановка помех;

4z и **6z** – не подготовлены с вероятностью $1 - P_y$ необходимые данные и дана команда на подавление средства перехвата помехами по ориентировочным сведениям; нарушитель перехватывает ПЭМИ с вероятностью $P_1^{\text{ПЭМИ}} \geq P_2^{\text{ПЭМИ}}$;

5z – осуществляется поиск нарушителя на территории ОИ и определение данных для постановки помех;

7z – осуществляется с вероятностью P_y поиск нарушителя и уточнение данных о нем;

8z и **11z** – осуществляется перехват ПЭМИ нарушителем с вероятностью $P_1^{\text{ПЭМИ}}$;

10z и **12z** – осуществляется перехват ПЭМИ нарушителем с вероятностью $P_2^{\text{ПЭМИ}}$.

Рис. 5. Граф составной сети Петри-Маркова для моделирования процесса реализации угрозы: а) при отсутствии; б) при наличии управления средством постановки помех для защиты информации от утечки по ПЭМИ

При наличии управления защитой (рис.5б), которое характеризуется вероятностью P_y того, что цикл управления средством защиты будет своевременно реализован (оценивающий, по сути, оперативность управления защитой), математические ожидания времени реализации угрозы по веткам графа ССПМ (0 → 4z)), (0 → 6z), (0 → 9z), (0 → 10z) определяется следующим образом:

$$\overline{\tau_{08}} = \overline{\tau_{00}} + \overline{\tau_{14}} + \overline{\tau_{44}} + \frac{\overline{\tau_{68}}}{P_1^{ПЭМИ}};$$

$$\overline{\tau_{0,10}} = \overline{\tau_{03}} + \overline{\tau_{75}} + \overline{\tau_{87}} + \frac{\overline{\tau_{10,10}}}{P_2^{ПЭМИ}};$$

$$\overline{\tau_{0,11}} = \overline{\tau_{03}} + \overline{\tau_{75}} + \overline{\tau_{86}} + \frac{\overline{\tau_{9,11}}}{P_1^{ПЭМИ}};$$

$$\overline{\tau_{0,12}} = \overline{\tau_{03}} + \overline{\tau_{79}} + \frac{\overline{\tau_{11,12}}}{P_2^{ПЭМИ}}, \quad (10)$$

где $\overline{\tau_{03}}$ – математическое ожидание времени срабатывания логического перехода 3z,

$$\overline{\tau_{03}} = \frac{(\overline{\tau_{02}}+\overline{\tau_{53}})^2+(\overline{\tau_{02}}+\overline{\tau_{53}})\cdot(\overline{\tau_{00}}+\overline{\tau_{31}}+\overline{\tau_{43}})+(\overline{\tau_{00}}+\overline{\tau_{31}}+\overline{\tau_{43}})^2}{(\overline{\tau_{02}}+\overline{\tau_{53}}+\overline{\tau_{00}}+\overline{\tau_{31}}+\overline{\tau_{43}})}, \quad (11)$$

$\overline{\tau_{02}}$ – математическое ожидание времени срабатывания логического перехода 2z,

$$\overline{\tau_{02}} = \overline{\tau_{00}} + \frac{\overline{\tau_{12}}^2 + \overline{\tau_{12}}\cdot\overline{\tau_{22}} + \overline{\tau_{22}}^2}{\overline{\tau_{12}} + \overline{\tau_{22}}}. \quad (12)$$

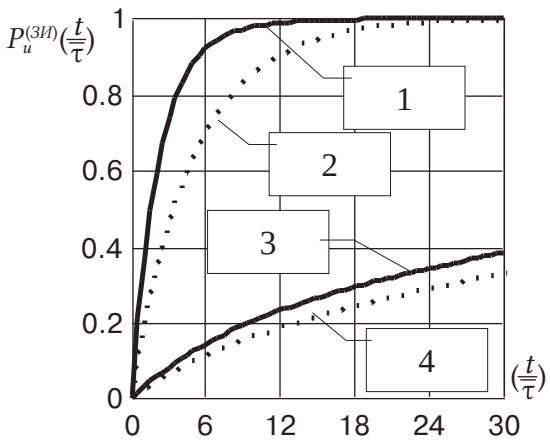
Тогда вероятность реализации угрозы находится из соотношения:

$$P_{u0}^{(ЗИ)}(t) = (1 - P_y)\cdot\left(1 - e^{\frac{t}{\overline{\tau_{08}}}}\right) + P_y\cdot\left\{P_{loc}\cdot\left[P_y\cdot\left(1 - e^{\frac{t}{\overline{\tau_{0.10}}}}\right) + (1 - P_y)\cdot\left(1 - e^{\frac{t}{\overline{\tau_{0.11}}}}\right)\right] + (1 - P_{loc})\cdot\left(1 - e^{\frac{t}{\overline{\tau_{0.12}}}}\right)\right. \quad (13)$$

В графическом виде зависимости вероятностей реализации угрозы при отсутствии и наличии управления защитой в случае, когда все математические ожидания времен перемещения процесса по сети из состояний в переходы примерно равны $\overline{\tau}$, приведены на рис. 6 и 7, а зависимость показателя эффективности управления, определяемого по формуле (4), от вероятности P_y при различных значениях показателей $P_{ПЭМИ}$ и P_{loc} – на рис. 8.

Анализ полученных зависимостей показывает следующее:

- с увеличением интервала времени вероятность реализации угрозы утечки ПЭМИ возрастает, а эффективность управления защитой падает;
- значение вероятности перемещения нарушителя по территории несущественно влияет на вероятность реализации угрозы утечки ПЭМИ из-за возможного повторного обнаружения нарушителя и постановки эффективных помех его приемнику;
- с уменьшением вероятности перехвата ПЭМИ эффективность управления возрастает;
- с уменьшением вероятности успешной реализации цикла управления защитой эффективность управления падает, однако не достигает нуля, так как остается вероятность того, что ПЭМИ в условиях фактически отсутствия управления будет перехватываться.



$P_1^{ПЭМИ} = 0{,}3;\ P_2^{ПЭМИ} = 0{,}01.$

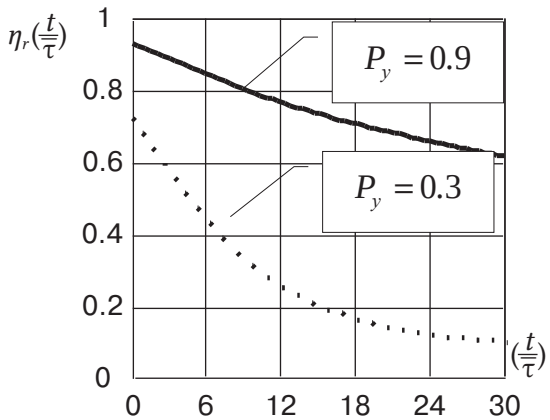
1 – управление защитой отсутствует, $P_{loc} = 0{,}9$;

2 – управление защитой отсутствует, $P_{loc} = 0{,}1$;

3 – вероятность реализации цикла управления $P_y = 0{,}9$, $P_{loc} = 0{,}9$;

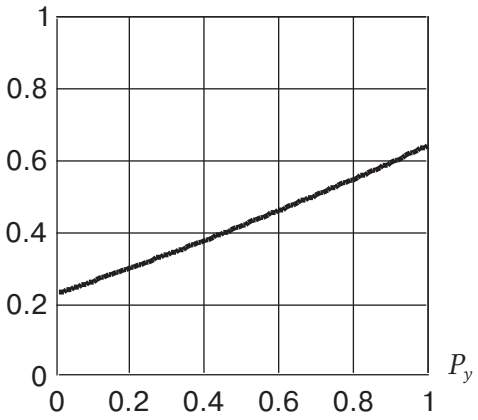
4 – вероятность реализации цикла управления $P_y = 0{,}9$, $P_{loc} = 0{,}1$;

Рис. 6. Зависимость вероятности реализации угрозы перехвата ПЭМИ от времени без управления и при наличии управления защитой



$P_{loc} = 0{,}9;\ P_1^{ПЭМИ} = 0{,}3;\ P_2^{ПЭМИ} = 0{,}01.$

Рис. 7. Зависимость показателя эффективности управления от времени при разных вероятностях реализации цикла управления



$$P_{loc} = 0{,}9;\ P_1^{ПЭМИ} = 0{,}3;\ P_2^{ПЭМИ} = 0{,}01;\ (\tfrac{t}{\overline{\tau}}) = 5.$$

Рис. 8. Зависимость показателя эффективности управления от вероятности реализации цикла управления

4. Алгоритм расчета частного показателя оперативности управления защитой информации в МАСЗИ

Введенный выше показатель оперативности управления защитой информации от утечки по ПЭМИ P_y (своевременной реализации цикла управления) представляет собой вероятность того, что случайное время τ_y, необходимое для подготовки за время $\tau_{дан}$ исходных данных, принятые за время $\tau_{реш}$ решения на применение средства защиты, подготовка и передачи за время $\tau_{ком}$ соответствующих команд, настройки и включения за время $\tau_{ср}$ средства защиты, окажется меньше случайного времени $\tau_{ТСП}$, необходимого для развертывания ТСП нарушителем за время $\tau_р$, поиска ПЭМИ и перехвата речевого сообщения за время $\tau_{пер}$ в ходе проведения мероприятия на ОИ, содержащем конфиденциальную информацию, то есть:

$$\tau_y = \tau_{дан} + \tau_{реш} + \tau_{ком} + \tau_{ср};\ \tau_{ТСП} = \tau_р + \tau_{поиск} + \tau_{пер}. \quad (14)$$

Рассмотрим случайную величину $y = \tau_{ТСП} - \tau_y$. Если $y > 0$, то цикл управления защитой будет успешно реализован. Пусть плотности распределения вероятностей для случайных величин τ_y и $\tau_{ТСП}$ равны соответственно $f_y(x)$ и $f_{ТСП}(x)$. Тогда с учетом положительно определенных значений времен плотность распределения случайной величины y, определяется следующим образом:

$$f_y(y) = \frac{1}{\overline{\tau_y} + \overline{\tau_{ТСП}}} \cdot e^{\frac{y}{\overline{\tau_{ТСП}}}} + \frac{1}{\overline{\tau_y} + \overline{\tau_{ТСП}}} \cdot \delta(y),\ y > 0\ , \quad (14)$$

где $\overline{\tau_y}$ и $\overline{\tau_{ТСП}}$ – математические ожидания времен τ_y и $\tau_{ТСП}$ соответственно; $\delta(y)$ – дельта-функция (функция Дирака).

Тогда усредненная за время t вероятность P_y определяется по формуле:

$$\overline{P_y} = \frac{\overline{\tau_{ТСП}}}{\overline{\tau_y} + \overline{\tau_{ТСП}}}. \quad (15)$$

Рассмотренный алгоритм расчета показателя оперативности управления защитой соответствует простому управлению, реализуемому или соответствующим агентом управления в МАСЗИ, или органом управления, когда не учитывается этапность процедуры (каскадность и иногда цикличность) управления, связанной с согласованием решений по управлению средством защиты между агентами и органом управления, выбором одного из нескольких возможных решений по установленным критериям, содержанием задач, решаемых в ходе управления, таких как поиск ТСП, проведение расчетов на подавление помехами ТСП, наблюдение за территорией и распознавание объектов и их действий, определение рационального размещения средств постановки помех на территории ОИ и др.

Это обусловливает необходимость разработки комплекса алгоритмов управления для обеспечения функционирования всех интеллектуальных агентов в составе МАСЗИ и соответствующих алгоритмов функционирования всех программных и программно-аппаратных средств – объектов управления. Проблемность этих вопросов определяется тем, что управление в данном случае реализуется на основе смешанного принципа управления, а решения по нему могут приниматься: а) самостоятельно каждым интеллектуальным агентом; б) согласованно несколькими агентами на одном уровне иерархии в системе управления защитой; в) путем согласования решения нижестоящего уровня с вышестоящим уровнем иерархии МАСЗИ. Каких-либо исследований по разработке соответствующих критериев и алгоритмов принятия решений при реализации смешанного принципа управления в многоагентных системах в интересах защиты информации от утечки по ТКУИ до сих пор практически не проводилось. Разработка указанных алгоритмов связана с созданием математических моделей управления, включающих в себя в качестве составных частей математические модели: сбора и обработки данных, получаемых от агентов-датчиков через подсистему связи в составе МАСЗИ с учетом фактора времени; принятие иерархически упорядоченных и согласованных оперативных решений для интеллектуальных агентов и органа управления при реализации смешанного (централизованно-децентрализованного) принципа управления.

Заключение

1. На больших ОИ, включающих десятки и сотни датчиков и аппаратных или программно-аппаратных элементов средств защиты, состав и настройки которых необходимо изменять в динамике изменения обстановки, централизованное построение и управление системой защиты из-за большого количества

процедур анализа и принятия решений по управлению может приводить к неадекватным решениям и, как следствие, к снижению эффективности защиты информации на ОИ. Парирование этих сложностей может быть достигнуто путем перехода к централизованно-децентрализованному (смешанному) принципу управления СЗИ на основе многоагентной системы защиты информации.

2. При подготовке и реализации действий, выполняемых при управлении защитой от утечки по ПЭМИ с применением МАСЗИ, имеет место целый ряд проблемных вопросов, связанных с функционированием и созданием МАСЗИ и касающихся разработки линейки интеллектуальных агентов на базе элементов искусственного интеллекта, средств защиты, которыми можно управлять с помощью интеллектуальных агентов, комплекса программных средств для оснащения органа управления МАСЗИ, позволяющего решать всю совокупность задач, связанных с управлением защитой.

3. Функционирование МАСЗИ невозможно без соответствующего методического обеспечения управления защитой. Сегодня такое обеспечение отсутствует, а его создание связано с проблемными вопросами разработки математических моделей оценки эффективности управления защитой на основе смешанного принципа управления с учетом фактора времени и различных логических условий, математических моделей управления защитой от утечки от ТКУИ, включающих в себя в том числе алгоритмы мониторинга обстановки и обработки данных, упорядоченную совокупность возможных решений, критериев и алгоритмов их принятия в МАСЗИ при выборе целесообразного состава мер защиты.

4. Для оценки эффективности управления защитой информации от утечки по ПЭМИ в МАСЗИ предложено использовать систему количественных показателей, позволяющих определить влияние управления защитой на ее эффективность. Для расчета таких показателей с учетом фактора времени и логических условий, определяющих процесс реализации угроз утечки информации по ПЭМИ целесообразно использовать аппарат составных сетей Петри-Маркова. Приведен пример применения этого аппарата для количественной оценки эффективности управления защитой информации от утечки по ПЭМИ при проведении на ОИ мероприятия (совещания, сбора или конференции).

Литература

1. *Авсентьев О. С., Кругов А. Г., Шелупанова П. А. Функциональные модели процессов реализации угроз утечки информации за счет побочных электромагнитных излучений объектов информатизации // Доклады ТУСУР. – 2020. – Т. 22, № 1. – С. 29–39.*
2. *Avsentiev O. S., Avsentiev A. O., Krugov A. G., Yazov Yu. K. Simulation of processes for protecting voice information objects against leakage through the spurious electromagnetic radiation channels using the Petri-Markov nets // Journal of Computational and Engineering Mathematics. – 2021. Vol. 8. – № 2. – P. 3–24.*
3. *Язов, Ю. К., Авсентьев А. О. Пути построения многоагентной системы защиты информации от утечки по техническим каналам // Вопросы кибербезопасности. 2022. № 5(51). С. 2–13. DOI:10.21681/2311-3456-2022-5-2-13*
4. *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*
5. *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*
6. *Грушо Н. А., Тимонина Е. Е. Сравнение архитектур многоагентных систем // Информационные технологии. — Москва. — 2019. Т. 25. № 5. С. 293–299.*
7. *Кошелев Д. А., Корж Т. В. Возможность применения многоагентной системы для обнаружения внедрения и атак // Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А.С. Попова: Радиолокация, навигация, связь. В 6 томах. 2019. С. 106–113.*
8. *Язов Ю. К., Соловьев С. В. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография/ Ю. К. Язов, Санкт-Петербург: Наукоемкие технологии, 2023. – 258с.*
9. *Язов Ю. К. Основы теории составных сетей Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография / Ю. К. Язов, А. В. Анищенко, А.С . Суховерхов. – Санкт-Петербург: Сциентиа, 2024. – 196 с.*

PROBLEMATIC ISSUES OF INFORMATION PROTECTION MANAGEMENT AGAINST LEAKAGE THROUGH TECHNICAL CHANNELS USING MULTI-AGENT SYSTEMS

Yazov Yu. K.[12], Avsentiev A. O.[13]

The purpose of the article *is to reveal the problematic issues of information protection from leakage through technical channels arising from side electromagnetic radiation, using promising multi-agent systems and its management, to show the need and ways to quantify the effectiveness of such protection.*

Research methods: *methods of morphological and functional-structural analysis of the processes of distributed information security management against leakage through technical channels, as well as methods of probability theory and Petri-Markov network theory are applied in the interests of modeling and evaluating the effectiveness of centrally decentralized security management processes.*

The result obtained: *the relevance of creating a multi-agent information protection system against leakage through technical channels is shown; the need for protection management in such systems is noted, the features of a centrally decentralized (mixed) control principle in a multi-agent system are revealed by the example of protecting speech information from leakage through technical channels arising from side electromagnetic radiation of radioelectronic equipment in the-the rate of objects of informatization.*

The problematic issues of building control subsystems as part of multi-agent information protection systems against leakage through technical channels arising from side electromagnetic radiation related to the concept and formation of protection efficiency indicators, the influence of protection management on its effectiveness, and the distribution of control actions among management entities are disclosed. A composite Petri-Markov network modeling the process of leakage of speech information by side electromagnetic radiation and analytical relations for calculating the indicator of the effectiveness of information security management in a multi-agent system are presented.

The scientific novelty *of the article lies in the fact that for the first time it poses the problem of implementing a mixed principle of managing information protection from leakage through technical channels based on a multi-agent system and considers the priority methodological aspects of quantifying the effectiveness of such protection.*

Keywords: *side electromagnetic radiation, protection management, mixed control principle, protection efficiency, management efficiency, protection measure, private indicator, mathematical model.*

References

1. *Avsent'ev O. S., Krugov A. G., Shelupanova P. A. Funkcional'nye modeli processov realizacii ugroz utechki informacii za schet pobochnyh jelektromagnitnyh izluchenij ob#ektov informatizacii // Doklady TUSUR. – 2020. – T. 22, № 1. – S. 29–39.*
2. *Avsentiev O. S., Avsentiev A. O., Krugov A. G., Yazov Yu. K. Simulation of processes for protecting voice information objects against leakage through the spurious electromagnetic radiation channels using the Petri-Markov nets // Journal of Computational and Engineering Mathematics. – 2021. Vol. 8. – № 2. – P. 3–24.*
3. *Jazov, Ju. K., Avsent'ev A. O. Puti postroenija mnogoagentnoj sistemy zashhity informacii ot utechki po tehnicheskim kanalam // Voprosy kiberbezopasnosti. 2022. № 5(51). S. 2–13. DOI:10.21681/2311-3456-2022-5-2-13*
4. *Wang, H. Multiagent hierarchical cognition difference policy for multiagent cooperation/ H. Wang., J. Yi., Z. Pu., Z. Liu. – Tekst : jelektronnyj // Algorithms. — 2021. T. 14. № 3. — DOI: 10.3390/a14030098.*
5. *Wang, L. Distributed continuous-time containment control of heterogeneous multiagent 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*
6. *Grusho N. A., Timonina E. E. Sravnenie arhitektur mnogoagentnyh sistem // Informacionnye tehnologii. – Moskva. – 2019. T. 25. № 5. S. 293–299.*
7. *Koshelev D. A., Korzh T. V. Vozmozhnost' primenenija mnogoagentnoj sistemy dlja obnaruzhenija vnedrenija i atak // Sbornik trudov XXV Mezhdunarodnoj nauchno-tehnicheskoj konferencii, posvjashhennoj 160-letiju so dnja rozhdenija A. S. Popova: Radiolokacija, navigacija, svjaz'. V 6 tomah. 2019. S. 106–113.*
8. *Jazov Ju. K., Solov'ev S. V. Metodologija ocenki jeffektivnosti zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija / Ju. K. Jazov, Sankt-Peterburg: Naukoemkie tehnologii, 2023. – 258s.*
9. *Jazov Ju. K. Osnovy teorii sostavnyh setej Seti Petri-Markova i ih primenenie dlja modelirovanija processov realizacii ugroz bezopasnosti informacii v informacionnyh sistemah: monografija / Ju. K. Jazov, A. V. Anishhenko, A. S. Suhoverhov. – Sankt - Peterburg: Scientia, 2024. – 196 s.*

12 Yuri K. Yazov, Dr.Sc., Professor, Chief Researcher of the Department of the FAA «GNII PTZI FSTEC of Russia», Voronezh, Russian Federation. E-mail: Yazoff_1946@mail.ru
13 Alexander A. Gorbachev , Ph.D. Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S. M. Shtemenko, Krasnodar, Russia. E-mail: infosec23.00@mail.ru