ти сетевой структуры, которая уже занята контрагентами. Далее достижимость узлов начинает расти вне зависимости от выбранного ранее направления «движения» (с увеличением или уменьшением номера узла). Отметим, что положение «критичного» узла не абсолютно, а зависит от конфигурации и размера области сетевой среды, уже охваченной агентами.

Рассмотренные классические сетевые структуры подтверждают обоснованность выбранного информационно-потенциального подхода, а также дают представление о том, информационные потенциалы каких видов наиболее интересны для исследования с практической точки зрения.

Библиографический список

1. ***Козлов В. В.*** Релятивистский вариант гамильтонова формализма и волновые функции водородоподобного атома / В. В. Козлов, Е. М. Никишин // Вестник МГУ. – М. : МГУ, 1986. – № 5. – С. 11–20. – (Сер. 1. Матем., мех.)

2. ***Приходько М. А.*** Проблемы взаимодействия конкурирующих интеллектуальных агентов в распределенных мультиагентных системах обработки информации / М. А. Приходько, Н. И. Федунец // Горный информационно-аналитический бюллетень. – М. : МГГУ, 2010. – № ОВ5. – С. 252–260.

3. ***Приходько М. А.*** Взаимодействие конкурирующих интеллектуальных агентов в распределенных мультиагентных системах обработки информации при экспоненциальном и равномерном возрастании числа контрагентов / М. А. Приходько // Горный информационно-аналитический бюллетень. – М. : МГГУ, 2010. – № ОВ5. – С. 236–251.

УДК 004.021

ПРОБЛЕМА НЕСАНКЦИОНИРОВАННОЙ УТЕЧКИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ МУЛЬТИАГЕНТНЫХ СИСТЕМАХ

Н.И. Федунец, М.А. Приходько

В работе рассматривается проблема несанкционированной утечки информации в инфокоммуникационных мультиагентных системах. Приводится концепция мультиагентной системы обнаружения и предотвращения несанкционированных утечек информации.

Ключевые слова*: утечка информации, несанкционированная утечка, инфокоммуникационная система, мультиагентная система, распределенная система, агент, контрагент, интеллектуальные агенты, конкурирующие агенты.*

Key words*: leak, unapproved leak, informational communication system, multi-agent system, distributed system, agent, counter-agent, intellectual agents, rival agents.*

В наше время инфокоммуникационные системы зачастую представляют собой большие территориально распределенные комплексы, неоднородные как по составу технических средств, так и используемому программному обеспечению. Задача исследования и моделирования таких систем традиционными методами становится все более трудной, и требует новых подходов для своего решения. Одним из таких подходов является динамично развивающаяся теория мультиагентных систем, позволяющая описать большую инфокоммуникационную систему в виде множества интеллектуальных агентов различных видов, взаимодействующих между собой. Подобное описание помимо своей естественности имеет и другие преимущества: возможность описания и моделирования крупномасштабных динамических организаций компонент и групп компонент, возможность оценки свойств групп компонент, предсказания глобальных свойств системы в целом и ее поведения, и многие другие.

Современные исследователи под интеллектуальными агентами обычно понимают некоторые программные компоненты, взаимодействующие друг с другом. Однако это определение может быть совершенно естественно расширено до понятия интеллектуального агента как некоторого элементарного процесса обработки информации, который может на практике реализовываться не только программными способами. Такое расширение понятия интеллектуального агента позволяет по-новому взглянуть на мультиагентные системы и происходящие в них процессы.

Одним из таких процессов является воспроизводство информации, формирование, управление и контроль над информационными потоками, приводящими к перераспределению информации, в том числе ее выводу за пределы системы (конечным пользователям). Наиболее ярко эти процессы проявляются в распределенных системах обработки информации, одной из основных функций которых является доставка определенной информации (электронного контента) своим пользователям. Такие системы можно объединить в большой класс инфокоммуникационных систем, а их примерами служат многочисленные интернет-сервисы по предоставлению доступа к банкам электронных материалов – от видеохостингов (http://www.youtube.com) до электронных библиотек (http://www.rsl.ru).

Несмотря на множество различий, практически у всех таких систем есть одна общая черта – зачастую доступ к информации, предоставляемой системой, регламентируется рядом правил, в том числе ограничивающих его на платной основе. Это приводит к необходимости создания различных механизмов контроля и ограничения доступа, а также ставит перед проблемой обнаружения нарушений введенных ограничений.

Одним из базовых механизмов разграничения доступа является регистрация и последующая аутентификация пользователя в системе. Для незарегистрированных пользователей доступ ограничивается единообразно, а для зарегистрированных – согласно данным их профиля.

Вместе с тем даже при наличии большого числа ограничений нередко наблюдается эффект несанкционированной утечки информации, когда пользователь системы, пользуясь регламентированными возможностями и способами получения информации, в конечном итоге получает информацию, доступ к которой для него должен быть ограничен. Проиллюстрируем это явление на примере систем дистанционного тестирования.

Представим себе пользователя системы дистанционного тестирования, проходящего пробные тесты по некоторому предмету. Пусть общая база вопросов по предмету содержит 500 вопросов, а для пробного теста из общей базы случайным образом отбираются 10 вопросов. В качестве образовательного элемента в конце пробного теста пользователю отображается подробная расшифровка тестирования, содержащая информацию о правильных ответах на вопросы, в которых были допущены ошибки.

Предполагается, что пользователь системы будет использовать пробные тестирования с целью проверки своих знаний, однако существует способ эксплуатации данной функции системы, позволяющий узнать правильный ответ на любой *заранее известный* вопрос. Для этого необходимо пройти достаточно *большое* число тестов, которое позволит сформировать список *всех* правильных ответов на вопросы прдемета. Таким образом, используя регламентированную возможность проверить свои знания, пользователь системы получает доступ ко *всем* правильным ответам на вопросы предмета, обладать которыми он не должен.

Анализ описанной проблемы раскрытия формулировок правильных ответов на вопросы тестирования [2, с. 283] показывает, что эффективное противодействие несанкционированной утечке информации возможно только при создании *многоуровневой* интеллектуальной системы фильтрации информации и ограничения прав доступа к ней. Вместе с тем опыт эксплуатации автоматизированной обучающей системы «Аргус-М» [1, с. 499] убеждает, что традиционных средств противодействия несанкционированной утечке информации в инфокоммуникационных системах недостаточно. Любая возможность получить санкционирован-

ный доступ к информации потенциально является источником возникновения ее несанкционированной утечки. А с учетом масштабов современных инфокоммуникационных систем само обнаружение утечки информации становится более сложной и важной задачей, чем ее блокирование. Поэтому налицо потребность в разработке новых систем контроля над информационными потоками, призванных не только ограничить доступ к тем или иным данным, но и *обнаружить* изменения в информационных потоках и появление несанкционированных утечек.

Базисом создания таких систем контроля над информационными потоками инфокоммуникационных систем могут стать мультиагентные системы, построенные на основе интеллектуальных агентов, анализирующих в режиме реального времени информационные потоки. Причем первостепенной задачей данных агентов должно быть не ограничение доступа к информации, а выявление несанкционированных утечек информации. Второй важнейшей задачей системы контроля должно стать определение инициатора утечки информации, а главное – *ее причины*. Проще говоря, система контроля должна не только ответить на вопрос, есть ли утечка информации, но и определить, почему она происходит, а также кто ее инициирует.

Как видно из примера, возникновение таких утечек обусловлено гораздо бо́льшим упорядочиванием некоторых действий пользователя, которые в общем случае носят во многом «случайный» характер. Поэтому критерием выявления несанкционированных утечек информации могут стать энтропийные характеристики системы, описывающие, например, *неупорядоченность* действий пользователя или функционирования определенных фрагментов самой инфокоммуникационной системы. Сигналом к активации дополнительных ограничений или блокированию подозрительной активности является снижение энтропии выбранных характеристик, говорящее о росте упорядоченности опасных действий.

Успешное функционирование подобной системы зависит от двух основных факторов. Во-первых, необходимо правильно построить модель мультиагентной системы, разместив интеллектуальные агенты соответствующих типов во всех ключевых узлах инфокоммуникационной системы, участвующих в обработке информации, утечку которой необходимо предотвратить. Во-вторых, необходимо правильно выбрать характеристики системы, энтропия которых будет использоваться как индикатор несанкционированной утечки информации. При этом необходимо избежать двух основных недостатков большинства систем контроля над нежелательными процессами – недостаточная гибкость и несрабатывание в случае неизвестной модели поведения, что свойственно сигнатурным методам, а также большое число ложных срабатываний, что свойственно статистическим методам.

Сама же система должна решать три основные задачи:

- обнаружение возникновения несанкционированной утечки информации;
- выявление причины и адресата несанкционированной утечки информации;
- блокирование нежелательной деятельности с целью предотвращения утечки информации.

Особо обратим внимание, что подобная система не только состоит из большого числа однотипных агентов, а включает в себя большое число интеллектуальных агентов *разных* типов, соответствующих разным уровням абстракции (обработки) защищаемой информации. Это позволяет контролировать информацию на всех уровнях, которые могут стать источником утечки, а также использовать большое число различных энтропийных характеристик, повышающих надежность системы защиты. Кроме того, разнотипность агентов и используемых «сигнальных» характеристик затрудняет адаптацию опасных процессов с целью маскировки несанкционированной утечки информации регламентированными действиями.

Сформулированная проблема несанкционированной утечки информации открывает новую увлекательную область применения мультиагентных систем в современных инфокоммуникационных системах. Требования к мультиагентным системам обнаружения и предотвращения несанкционированных утечек информации закладывают базис их создания,

одновременно подсказывая направление развития, заключающееся в поиске и формализации энтропийных характеристик инфокоммуникационных систем, которые могут служить индикаторами несанкционированных утечек информации.

Немаловажной задачей является также выработка рекомендаций по устранению причин возникновения выявленной несанкционированной утечки информации. Наличие четких предложений по модификации правил доступа к информации или алгоритмов функционирования инфокоммуникационной системы существенно сократит время ликвидации обнаруженной утечки и в целом повысит надежность и уровень защищенности инфокоммуникационной системы.

Библиографический список

1. ***Приходько М. А.*** Автоматизированная обучающая система «Аргус-М»» – первый свободный веб-сервис дистанционного обучения / М. А. Приходько // Роль бизнеса в трансформации российского общества – 2010 : мат-лы V Междунар. науч.-практ. конгресса / Моск. фин.-пром. академия. – М. : МФПА, 2010. – С. 499–500.

2. ***Приходько М. А.*** Требования к системам интерактивного контроля знаний в традиционных учебных заведениях (вузах) на примере АСИКЗ «Аргус-М» / М. А. Приходько // Информатизация образования – 2009 : мат-лы Междунар. науч.-метод. конф. / Волгоград. гос. пед. ун-т. – Волгоград : Перемена, 2009. – С. 283–287.

УДК 004.023

ЭВРИСТИЧЕСКАЯ МОДЕЛЬ ОБОБЩЕННОГО ПОКАЗАТЕЛЯ ТЕХНИЧЕСКОГО УРОВНЯ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

А.Н. Хабаров, А.А. Княгинин

Рассмотрена эвристическая модель обобщенного показателя технического уровня информационно-вычислительных систем, основанная на комплексном применении элементов теории полезности, многомерного шкалирования, экспертного оценивания и принятия решений. Обобщенный показатель синтезируется в линейно-квадратичной форме, что обеспечивает более высокую адекватность результатов оценки предпочтениям экспертов и лиц, принимающих решение.

Ключевые слова: *технический уровень, информационно-вычислительная система, метод оценки, обобщенный показатель.*

Key words: *technical level, computer information system, valuation method, generalized index.*

В настоящее время при оценке технического уровня (ТУ) информационно-вычислительных систем (ИВС) как продукции применяются количественные и экспертные методы. К количественным методам относятся дифференциальный, комплексный и смешанный методы [3, с. 43–67].

Дифференциальный метод оценки ТУ заключается в раздельном сопоставлении единичных показателей ТУ рассматриваемого изделия с аналогичными «эталонными» показателями.