Сохранение перспектив развития рынка образовательных услуг должно основываться также на интеграции фундаментального уровня образования и его выраженной практической направленности. Исходя из этого, инновационные формы стратегического партнерства кредитных организаций и высших учебных заведений должны включать:

- совместный мониторинг текущего состояния и прогнозирование колебаний спроса;
- разработка профессиональных компетенций и корпоративных профессиональных стандартов для основных категорий банковского персонала;
- актуализация образовательного контента вуза при участии экспертов из числа ведущих специалистов партнерского банка;
- формирование методик отбора и первичного профессионального развития будущих сотрудников банка из числа учащихся старших курсов с учетом специфики предлагаемых к замещению рабочих мест;
- совместная разработка корпоративных программ повышения квалификации и профессиональной переподготовки для различных категорий сотрудников банка в режиме непрерывного образования;
- привлечение ведущих специалистов партнерского банка к учебно-методической деятельности вуза (проведение мастер-классов и тренингов, участие в разработке учебно-методического контента);
- проведение стажировок преподавателей партнерского вуза в соответствующих службах и подразделениях банка.

Список литературы

1. Веснин В. Р. Основы менеджмента / В. Р. Веснин. – М. : Триада ЛТД, 2007. – С. 117–118.
2. Герчикова И. Н. Менеджмент. Банки и биржи / И. Н. Герчикова. – М. : ЮНИТИ, 2005. – С. 21–23.
3. Розанова В. А. Психология управления / В. А. Розанова. – М. : ЗАО Бизнес-школа «Интел-Синтез», 2005. – С. 71–72.

References

1. Gerchikova I. N. Banki i birzhi / I. N. Gerchikova. – M. : UNITI, 2005. – P. 21–23.
2. Rozanova V. A. Psikhologia upravlenia / V. A. Rozanova. – M. : ZAO Biznes-shkola «Intel-Sintez», 2005. – P. 71–72.
3. Vesnin V. R. Osnovi menegmenta / V. R. Vesnin. – M. : Triada LTD, 2007. – P. 117–118.

УДК 004.021

МУЛЬТИАГЕНТНЫЕ ТЕХНОЛОГИИ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Приходько Максим Александрович, *докторант, кандидат физико-математических наук, Московский государственный горный университет, 119991, г. Москва, Ленинский проспект, 6, e-mail: spex19@mail.ru.*

В работе рассматривается проблема несанкционированной утечки информации в инфокоммуникационных мультиагентных системах. Под утечкой информации понимается получение регламентированными средствами данных, доступ к которым формально должен быть ограничен. Понятие утечки информации иллюстрируется на примере систем интерактивного контроля знаний (интернет-тестирования), где отсутствие необходимых ограничений может приводить к раскрытию формулировок правильных ответов. Рас-

сматриваются существующие способы разграничения доступа к информации и их недостатки. Наряду с проблемой возникновения несанкционированной утечки информации, формулируется также проблема обнаружения самого факта несанкционированной утечки, особо актуальная для систем с большим числом пользователей, запрашивающих и получающих информацию в режиме реального времени (интернет-порталы). Обосновывается возможность использования мультиагентных систем для решения сформулированных проблем. В качестве критериев возникновения несанкционированной утечки информации предлагается использовать энтропийные характеристики действий пользователей и информационных потоков системы. Обосновывается целесообразность использования многоагентных систем, контролирующих информационные потоки, содержащие защищаемую информацию, на разных уровнях абстракции данных. Приводится концепция мультиагентной системы обнаружения и предотвращения несанкционированных утечек информации. Формулируются требования к подобной системе и решаемые ею задачи.

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

MULTI-AGENT UNAPPROVED INFORMATION LEAK DETECTION SYSTEM IN E-LEARNING SYSTEMS

***Prikhodko Maxim A.**, Doctoral trainee, Cand. of Physics and Mathematics, Moscow State Mountain University, 6, Leninsky avenue, Moscow, 119991, Russia, e-mail: spex19@mail.ru*

This work considers problems of unapproved leaks in multi-agent informational communication systems. By unapproved leaks receiving of restricted data by regulated means is implied. The concept of unapproved leak is illustrated by the example of interactive knowledge control systems (Internet-testing), where lack of restriction may lead to exposure of the correct answers. Present methods of data restriction and their disadvantages are considered. Along with the problem of unapproved leak the problem of unapproved leak detection is formulated, that is particularly actual for the systems with huge number of users, requesting and receiving information in real-time (Internet-portals). The possibility of usage of multi-agent systems for solving the formulated problems is proved. As the criteria of the origin of unapproved leak it is proposed to use entropic characteristics of user's actions and data flows of a system. Advisability of usage of multiagent systems, controlling data flows with restricted information on different levels of data abstraction is proved. Concept of multi-agent unapproved leaks detection and prevention system is listed. System requirements and current tasks are formulated.

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

В наше время системы дистанционного обучения зачастую представляют собой большие территориально распределенные комплексы, неоднородные как по составу технических средств, так и по 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 любую большую систему в виде множества интеллектуальных агентов различных видов, взаимодействующих между собой. Подобное описание, помимо своей естественности, имеет и другие преимуще-

ства: 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 т.д.

Одним из важнейших информационных процессов систем дистанционного обучения является воспроизводство информации, формирование, управление и контроль над информационными потоками, приводящими к перераспределению информации, в том числе ее выводу за пределы системы (конечным пользователям). Зачастую процесс перераспределения и доступа 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.

Наиболее распространенным базовым механизмом 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 тестирования.

Представим себе пользователя системы дистанционного обучения, 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 достаточно пройти *большое* число тестов, которое позволит сформировать список *всех* правильных ответов на вопросы теста. Таким образом, используя регламентированную возможность проверить свои знания, пользователь системы получает доступ к правильным ответам на вопросы по предмету, обладать которыми он в общем случае не должен.

Анализ описанной проблемы раскрытия формулировок правильных ответов на вопросы тестирования [2] показывает, что эффективное противодействие несанкционированной утечке информации возможно только при создании *многоуровневой* интеллектуальной системы фильтрации информации и ограничения прав доступа к ней. В частности, в АСИКЗ «Аргус-М» были реализованы следующие ограничительные механизмы:

- механизм защиты от раскрытия точных формулировок правильных ответов;
- механизм защиты от раскрытия информации о правильности/неправильности варианта ответа;
- механизм защиты от раскрытия набора ответов, гарантирующих определенную оценку;
- механизм защиты от возможного изменения варианта ответа для вопроса, на который ответ уже был дан;
- механизм защиты от нерегламентированной навигации по системе во время прохождения аттестации;
- механизм защиты результатов контроля знаний от попыток несанкционированного изменения без использования системы (т.е. от «взлома» данных системы злоумышленником извне).

Вместе с тем опыт эксплуатации автоматизированной обучающей системы «Аргус-М» [2] убеждает, что традиционных средств противодействия несанкционированной утечке информации в инфокоммуникационных системах недостаточно. Любая возможность получить санкционированный доступ к информации потенциально является источником возникновения ее несанкционированной утечки. А с учетом масштабов современных систем дистанционного обучения 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 возникновения несанкционированных утечек информации.

Как видно из примера, возникновение таких утечек обусловлено гораздо большим упорядочиванием некоторых действий пользователя, которые в общем случае носят случайный характер. Поэтому критерием выявления несанкционированных утечек информации могут стать энтропийные характеристики системы, описывающие, например, *неупорядоченность* действий пользователя или функционирования определенных фрагментов 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.

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 просто 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. Проиллюстрируем это на ранее рассмотренном примере тестирования.

Информация о правильности выбранного ответа, а также правильном варианте ответа, предоставляется пользователю АСИКЗ «Аргус-М» в нескольких случаях:

- в подробной расшифровке результатов тестирования;
- в сводной таблице результатов тестирования на странице тестирования;
- в сводной таблице результатов тестирования на странице пользователя.

Кроме того, информация о возможных вариантах ответа предоставляется пользователю непосредственно в момент прохождения теста. Таким образом, налицо необходимость создания трехуровневой системы, состоящей из интеллектуальных агентов трех типов, собирающих и анализирующих информацию об активности пользователя на уровне прохождения теста, просмотра сводных результатов и просмотра подробной расшифровки результатов.

Данные интеллектуальные агенты должны уметь общаться друг с другом для обмена информацией об активности пользователя. Они также должны уметь анализировать активность многих пользователей с целью выявления корреляций в их действиях следующих типов:

- один человек под видом нескольких пользователей инициирует несанкционированную утечку информации;
- группа пользователей скоординированными действиями инициирует несанкционированную утечку информации.

Наличие нескольких *разнотипных* агентов усложняет задачу маскировки утечки информации регламентированной деятельностью, так как снижение активности пользователя на одном из уровней ведет к повышению активности на другом с целью добычи необходимой информации. А это, в свою очередь, позволяет варьировать качества интеллектуальных агентов, повышая в целом чувствительность системы.

Сформулированная проблема несанкционированной утечки информации открывает новую увлекательную область применения мультиагентных систем в современных системах дистанционного обучения. 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 систем дистанционного обучения, которые могут служить индикаторами несанкционированных утечек информации. А область интерактивного тестирования предлагает поле для практической реализации и отработки решений по созданию такой системы.

Список литературы

1. Приходько М. А. Автоматизированная обучающая система «Аргус-М» – первый свободный веб-сервис дистанционного обучения / М. А. Приходько // Роль бизнеса в трансформации российского общества : сб. тез. докл. V Междунар. науч. конгресса. – М., 2010.

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. – М., 2009.

References

1. Prihodko M. A. Avtomatizirovannaya obuchayushaya sistema “Argus-M” – pervyi svobodnyi veb-servis distancionnogo obucheniya / M. A. Prihodko // Rol biznesa v transformacii rossiiskogo obshestva : sb. tez. dokl. V Mezhdunar. nauch. kongressa. – M., 2010.

2. Prihodko M. A. Trebovaniya k sistemam interaktivnogo kontrolya znanii v tradicionnykh uchebnykh zavedeniyakh (vuzakh) na primere ASIKZ “Argus-M” / M. A. Prihodko // Informatizaciya obrazovaniya – 2009 : mat-ly Mezhdunar. nauch.-metod. konf. – M., 2009.