УДК 004.65

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ: МЕТОДЫ И ТЕХНОЛОГИИ

ГВОЗДИНСКИЙ А.Н., ФИЛАТОВ В.А., ЧАЛАЯ Л.Э.

Рассматриваются модели и механизмы реализации политики безопасности. Выделяются наиболее перспективные из них для создания и использования в проектировании систем защиты информации в распределенных БД. Предлагается мультиагентная модель информационной безопасности системы распределенных БД.

Введение

Основой современных информационных технологий является автоматизированная компьютерная обработка данных. При создании распределенных систем управления информацией необходимо решать две довольно противоречивые задачи.

Первая из них состоит в том, чтобы создать систему с минимальной стоимостью. Стоимость создания подобных систем пропорциональна степени использования коллективных ресурсов. Это означает, что в целях минимизации стоимости системы целесообразно создавать коллективный ресурс для всех ее пользователей, включая средства поддержки сохранения информации, программные и аппаратные средства ее обработки и доступа к другим средствам и системам. Удачно выбранные организация доступа и возможность коллективного ресурса значительно уменьшают стоимость создания и эксплуатации системы при реализации заданных требований к ее функционированию.

Обработка информации с использованием возможностей коллективного ресурса не означает, что каждому пользователю системы должны быть доступны эти возможности. Доступность определяется правилами (требованиями), которые формулируются при создании системы. Именно соблюдение этих правил при делении пользователей системы на отдельные классы и предопределяет необходимость решения *второй* задачи – организовать процесс передачи и обработки информации так, чтобы каждый пользователь получал только ту информацию, которую ему разрешено получать [1,2].

Очевидно, что повсеместная индивидуализация ресурса для каждого пользователя системы является оптимальным решением второй задачи, однако в значительной мере увеличивает стоимость создания и эксплуатации любой системы обработки информации. Именно в этом понимании целевые установки первой и второй задачи противоречат одна другой. С развитием и расширением сферы применения средств вычислительной техники острота проблемы обеспечения безопасности в вычислительных системах и защиты информации возрастает по ряду объективных причин. Главная из них – повышение доверия к компьютерным системам и информационным технологиям. Им доверяют самые ответственные задачи, от качества которых зависит жизнь и благосостояние многих людей. Компьютерные системы управляют технологическими процессами на предприятиях и атомных электростанциях, движением самолетов и ракет, выполняют финансовые операции, обрабатывают секретную информацию.

Сегодня проблема защиты вычислительных систем приобретает еще большее значение в связи с развитием и распространением сетей персональных компьютеров и Internet. Распределенные системы и сети с удаленным доступом выдвинули на первый план вопрос защиты передаваемой информации. Доступность средств вычислительной техники привела к распространению компьютерной грамотности в широких кругах населения. Это, в свою очередь, вызвало многочисленные попытки вмешательства в работу государственных и коммерческих систем. Многие из этих попыток достигали цели и нанесли значительный ущерб собственникам информации вычислительных систем.

Целостную картину всех возможностей защиты создать довольно сложно, поскольку еще нет единой теории защиты информационных систем. Существует много подходов и точек зрения относительно методологии их построения, используются последние достижения науки, передовые технологии.

1. Защита компьютерных систем обработки информации

Известны разные варианты защиты – от охранника на входе офиса до математически выверенных средств защиты данных. Кроме того, можно говорить о глобальной защите и ее отдельных аспектах: защита персонального компьютера, сетей, баз данных (БД) и т.п.

Следует отметить, что абсолютно защищенных систем нет. Можно говорить о защите и надежности системы, во-первых, только с определенной вероятностью, а во-вторых, о защите от некоторой категории злоумышленников. *Защита – это соревнование обороны и нападения: кто больше знает, предусматривает, инвестирует, тот и выигрывает.* Вопреки всем неудобствам, которые приносят средства защиты во время работы, во многих случаях они могут быть абсолютно необходимы для нормального функционирования систем. В первую очередь это касается систем электронной коммерции и банковских систем. К основным из упомянутых неудобств можно отнести:

– дополнительные сложности в работе с большинством защищенных систем;

– повышение стоимости защищенной системы;

– дополнительная нагрузка на системные ресурсы, увеличение времени на выполнение одного и того же задания в связи с замедлением доступа к данным;

– необходимость привлечения дополнительного персонала, который отвечает за охрану и поддержку системы защиты.

1.1. Основные понятия безопасности информационных систем

Под безопасностью компьютерных систем обработки информации понимают способность противодействовать попыткам нанесения ущерба информационным ресурсам в процессе общения с системой. Такая безопасность достигается путем обеспечения конфиденциальности обрабатываемой информации, а также целостности и доступности компонентов и ресурсов системы согласно установленным правилам.

Конфиденциальность – это свойство информации быть известной только субъектам, которые прошли соответствующую проверку – авторизованным субъектам системы (пользователям, программам, процессам и т.п.). Для других субъектов системы эта информация является закрытой.

Целостность компонента (ресурса) системы – свойство быть неизменным (в семантическом понимании) при ее функционировании. Изменения в компоненты системы могут вноситься исключительно ее уполномоченными авторизованными субъектами.

Доступность компонента (ресурса) системы – свойство быть доступным для использования авторизованными субъектами системы в любое время.

Различают внешнюю и внутреннюю безопасность компьютерных систем. Внешняя предусматривает защиту системы от стихийного бедствия, от проникновения злоумышленников извне в целях похищения отдельных ее компонентов, получения доступа к носителям информации или вывода системы из строя. Предметом внутренней безопасности является обеспечение надежной и корректной работы системы, целостности ее программ и данных.

Все усилия относительно создания внутренней безопасности компьютерных систем сосредоточены на создании надежных и удобных механизмов регламентации деятельности всех ее пользователей и обслуживающего персонала, соблюдении установленной в организации дисциплины прямого или косвенного доступа к ресурсам и к информации. В настоящее время известны два подхода к обеспечению безопасности компьютерных систем – фрагментарный и комплексный.

Фрагментарный подход ориентируется на противодействие определенным угрозам при определенных условиях. Примерами реализации такого подхода могут быть специализированные антивирусные средства, отдельные мероприятия регистрации и управления, автономные средства шифрования и т.п. Главная особенность (которая является одновременно и основным недостатком) фрагментарного подхода – отсутствие единой защищенной среды обработки информации. Преимуществом фрагментарного подхода является его высокая избирательность относительно конкретной угрозы и эффективность действий в заданном направлении. Но даже небольшое изменение угрозы приводит к потере эффективности защиты. Быстро распространить действие локальных мероприятий на всю систему практически невозможно.

Особенностью *комплексного подхода* является создание защищенной среды обработки информации, включающее различные мероприятия противодействия угрозам: правовые, организационные, программно-технические. Защищенная среда обработки информации формируется на основе регламента процессов обработки информации. Организация защищенной среды дает возможность гарантировать в границах принятой политики безопасности необходимый уровень защиты системы. Комплексный подход применяют как для защиты больших многопользовательских государственных или коммерческих систем, так и для сравнительно небольших систем, обрабатывающих важную экономическую, политическую или военную информацию.

Для организации надежной защиты следует четко представлять, от каких видов информационных атак необходимо защищаться.

Угроза безопасности – это потенциально возможное воздействие на систему, которое может прямо или косвенно нанести ущерб ресурсам информационной системы. Реализацию угрозы обычно называют атакой. Угрозы безопасности можно классифицировать по таким признакам:

- цели атаки;
- принцип воздействия на систему;
- объекты атаки;
- способы проведения атаки.

Потери от атак каждого вида, как правило, обратно пропорциональны частоте их появления. От нарушений, вызванных небрежностью, требуется защита с минимальными программно-аппаратными затратами; от попыток зондирования системы – более эффективный подход; от проникновения – многоуровневая система информационной безопасности. Защитные мероприятия должны быть адекватны вероятности осуществления и степени угрозы. Только комплексный анализ угроз и степени защищенности информационной системы может обеспечить относительную безопасность.

1.2. Этапы построения системы защиты информации

Система защиты компьютерной информации – это совокупность правовых норм, организационных, административных и программно-технических средств, направленных на противодействие угрозам нормальному функционированию системы в целях сведения к минимуму возможных материальных и моральных потерь пользователей и собственников системы.

Основные этапы построения системы защиты представлены на рис.1.

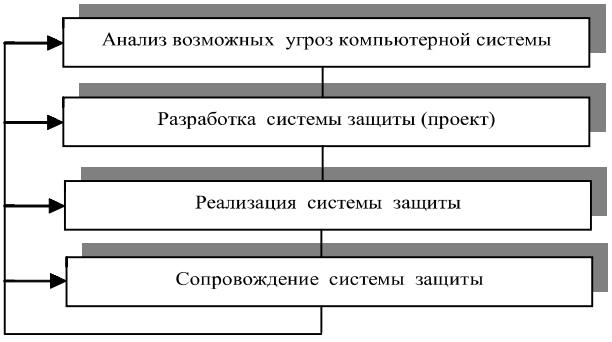

Рис. 1. Этапы построения системы защиты

Этап анализа возможных угроз компьютерной системе обработки информации необходим для фиксирования на определенный момент времени состояния системы (конфигурации аппаратных и программных средств, технологии обработки информации) и определения возможных злонамеренных действий для любого компонента системы. Из множества возможных действий избирают лишь те, которые могут реально состояться и нанести ущерб пользователям и собственникам системы.

На этапе планирования формируется структура системы защиты как совокупность мероприятий противодействия различного характера. Известно не так много универсальных способов защиты информационных систем. Наиболее эффективными являются:

– идентификация и аутентификация субъектов системы;

– контроль доступа к ресурсам системы;

– регистрация и анализ событий, которые происходят в системе;

– контроль целостности объектов системы;

– шифрование данных;

– резервирование ресурсов и компонентов системы.

Эти универсальные способы могут применяться в разных вариациях в конкретных методах и мероприятиях защиты.

Результатом этапа планирования является план защиты информационной системы – документ, который содержит описание и перечень ее компонентов, требующих защиты, варианты возможных воздействий на них (атак), стоимость защитных мероприятий, правила обработки информации в системе. На этапе реализации системы проводятся мероприятия по вводу всех ее компонентов в эксплуатацию.

Существует два основных способа реализации механизмов защиты информационных систем:

– «дополнительная» защита, в которой средства защиты – это дополнения к основным программным и аппаратным средствам системы обработки информации. Подобного подхода в обеспечении безопасности придерживается, например, фирма IBM;

– «встроенная» защита состоит в том, что ее механизмы являются неотъемлемой частью информационной системы, разработанной и реализованной с учетом требований безопасности. Механизмы защиты могут быть реализованы в виде отдельных компонентов системы и распределены среди ее составляющих. При этом средства защиты составляют единый механизм, который отвечает за безопасность всей системы. Этот способ использовался компанией DEC при разработке системы VAX/VMS.

Оба способа имеют свои преимущества и недостатки. Дополнительная защита более гибкая, её механизмы и конфигурацию можно изменять по мере необходимости. Основное преимущество встроенной защиты – надежность и локальная оптимальность. Средства защиты при этом разрабатываются и реализовываются вместе с самой системой. Тем не менее, встроенная защита имеет жестко зафиксированный набор функций, которые невозможно расширить или функционально изменить. Некоторые функции можно только исключить.

«Дополнительная» и «встроенная» защиты в чистом виде встречаются редко. Как правило, используются их комбинации, которые дают возможность объединять преимущества и компенсировать недостатки каждой.

2. Модели и механизмы реализации политики безопасности

Набор правил и практических рекомендаций по защите информации определяется политикой безопасности. Она может быть индивидуальной и зависящей от конкретной технологии обработки информации, программных и технических средств. Основу политики безопасности составляет способ управления доступа субъектов к объектам системы. *Субъект* – активный компонент системы, который может изменять ее состояние. *Объект* – пассивный компонент системы, который сохраняет, принимает и передает информацию.

Для реализации системы управления доступом создается математическая модель информационной системы. Она может моделировать все ее состояния, переходы из одного состояния в другое, а также показывать, какие состояния можно считать безопасными. Для этого применяется широкий спектр математических методов моделирования (теория графов, теория цифровых автоматов и т.п.).

Существует два вида политики безопасности:

– избирательная;

– полномочная.

Избирательная политика безопасности. Основой данного подхода является избирательное управление доступом. В основе математической модели системы находится матрица доступа, в которой объекту системы соответствует столбец, а субъекту – строка. Значение элемента, находящегося на пересечении столбца и строки матрицы, определяет тип разрешенного доступа субъекта к объекту.

Полномочная политика безопасности предусматривает такие условия:

– все объекты и субъекты должны быть однозначно идентифицированы;

– каждый объект имеет отметку критичности, которая определяет ценность информации;

– каждому субъекту системы присваивается уровень прозрачности;

– чем важнее объект, тем выше признак его критичности.

Каждый субъект, кроме уровня прозрачности, имеет текущее значение уровня безопасности; последнее может изменяться от минимального до уровня прозрачности. Для принятия решения на разрешение доступа признак критичности объекта сравнивают с уровнем прозрачности и текущим уровнем безопасности субъекта. Информация может передаваться только “вверх”, т.е. субъект может иметь

доступ к объекту, если его текущий уровень безопасности не ниже, чем признак критичности объекта. Главное назначение полномочной политики безопасности – регулирование доступа с разным уровнем критичности и предотвращение несанкционированных перемещений информации с верхних уровней иерархии на нижние, а также блокировка возможных переходов с нижних уровней на верхние.

Избирательное и полномочное управление доступом, а также управление информационными потоками – три составляющие методологии защиты информации.

Все средства, которые отвечают за реализацию политики безопасности, должны быть защищены от любого вмешательства. Их объединяют в так называемые *достоверные вычислительные базы*. Это полностью защищенный механизм вычислительной системы (включает аппаратные и программные средства), который отвечает за реализацию и поддержку политики безопасности. Его функции – поддержка целостности механизмов защиты и обеспечение защиты субъектов и объектов системы [3].

2.1. Модель информационной безопасности системы распределенных баз данных

Существуют различные подходы к формализации задачи синтеза системы защиты информационной системы на основании выбранной политики безопасности. Рассмотрим один из наиболее эффективных, рассчитанный на современные программные технологии реализации [4].

Различные методы защиты информации характеризуются определенными технико-экономическими показателями. К основным характеристикам методов защиты можно отнести затраты на их разработку и эксплуатацию, безопасное время, под которым понимается математическое ожидание времени раскрытия метода защиты путем опробования множества возможных вариантов проникновения.

Безопасное время может служить оценкой эффективности метода защиты. Например, любая процедура защиты, осуществляемая программным способом, связана с затратами таких ресурсов компьютера как оперативная память, процессорное время и (или) время обмена с внешними носителями информации. Очевидно, чем сложнее процедуры контроля доступа, а также чем выше частота их реализации при функционировании БД, тем выше расходы ресурсов вычислительной системы на эксплуатацию системы защиты.

Различные способы организации одной и той же процедуры контроля доступа могут приводить к различным затратам на реализацию. Следует отметить, что указанные характеристики методов защиты связаны прямо пропорциональной зависимостью. К примеру, чем длинее пароль, используемый для управления доступом, тем выше затраты на реализацию данного метода защиты, так как значение безопасного времени возрастает с увеличением числа переборов возможных вариантов пароля.

Очевидно, что вероятность преодоления метода защиты злоумышленником определяется затратами средств последнего. По мере того, как ресурсы, вкладываемые злоумышленником для взлома метода защиты БД, начинают превышать затраты на создание рассматриваемого метода, возрастает вероятность несанкционированного доступа. При синтезе систем защиты БД от несанкционированного доступа в качестве факторов, влияющих на решение задачи проектирования, выступают ограничения, обусловленные средствами, выделенными на разработку и эксплуатацию системы, а также составом и квалификацией разработчиков. Отсюда следует, что синтезируемая система должна обеспечивать выполнение функций защиты информационных ресурсов БД от несанкционированного доступа в условиях заданных ограничений на выделенные средства для проектирования и эксплуатации.

Рассмотрим формализованные определения и методы формирования механизмов защиты канонических, логических и физических структур БД. В общем случае механизм защиты предназначен для обеспечения доступа и допуска к информации только обладающих соответствующими полномочиями пользователей. Он реализуется путем использования одного или нескольких методов защиты (организационных, процедурных, структурных, аппаратных или программных).

Механизм защиты БД определяется перечнем требований к ней по обеспечению исключения преднамеренного или непреднамеренного несанкционированного использования информации БД и прикладных программ. Он позволяет идентифицировать законных и незаконных пользователей БД и правомочность их действий, а также предотвратить незаконные действия пользователей.

Пусть $Q = \{q_k : k = 1, K\}$ – множество пользователей базы данных, $B = \{b_i : i = 1, I_b\}$ – проектируемая база данных; $P = \{p_j : j = 1, j_b\}$ – прикладное программное обеспечение, где b_i и p_j – компоненты проектируемой БД и прикладного программного обеспечения соответственно. Тогда механизм защиты БД есть отображение M такое, что:

$$\{(g_k, b_i, p_j)\} \to M \to (0,1), \qquad (1)$$

где «1» соответствует правомочности доступа пользователя $q_k \in Q$ к элементам $b_i \in B$ или $p_j \in P$, а «0» – запрету на такой доступ. Следовательно, механизм защиты БД позволяет определить, какой пользователь имеет санкции на осуществление доступа к тем или иным информационным и программным элементам, которые являются единицей обмена при взаимодействии пользователей с БД.

Разработка механизма защиты БД представляет собой сложный процесс построения и анализа механизмов защиты соответствующих уровней хранения и представления информации в БД (ее канонической, логической и физической структур).

Система защиты $S = \{S_i : = 1, I\}$ представляет собой совокупность методов защиты, где S_i есть i-й метод, а I – общее число методов.

Под оптимальной системой защиты БД будем понимать такую совокупность методов $S_{opt} \subset S$ ее

защиты, которые обеспечивают экстремальное значение некоторого заданного критерия эффективности разработки или эксплуатации системы защиты БД при условии соблюдения требований к ее функционированию, выполнению структурных и функциональных ограничений, накладываемых СУБД и пользователями.

К характеристикам системы защиты БД, которые могут быть использованы в качестве критериев оптимизации, относятся:

– вероятность «взлома» защиты злоумышленниками; безопасное время, под которым понимается среднее время, необходимое для получения защищенных данных путем опробования различных вариантов доступа;

– стоимость разработки и внедрения системы защиты, эксплуатационные затраты на нее, время ее разработки и внедрения;

– минимум числа несанкционированных обращений пользователей к различным защищенным ресурсам БД; время выполнения заданного множества запросов пользователей и т.д.

Разработка системы защиты информации в БД является сложным и многоаспектным процессом. Определение механизмов и синтез оптимальной системы защиты информации БД представляет собой многоэтапный процесс анализа требований пользователей по обеспечению необходимого уровня секретности, синтеза канонической, логической и физической структур данных с учетом этих требований, выбора оптимальной совокупности методов защиты, включая выбор процедурных методов. Исходной при этом служит информация о предметной области пользователей, требования к обеспечению необходимой степени секретности данных, полномочия пользователей на использование данных при решении различных задач [4].

2.2. Мультиагентная система защиты информационных ресурсов распределенной системы

Рассмотренная выше формализованная модель защиты информационной системы может быть эффективно реализована в комплексе с распределенной мультиагентной системой администрирования, технология которой состоит в следующем. На каждом локальном персональном компьютере сети размещается программный агент. Он представляет собой специализированный программный модуль, связанный с локальной базой данных этого компьютера или другим информационным ресурсом. При этом один программный агент может решать несколько задач по управлению доступом к ресурсам данного персонального компьютера [6,7]. Фрагмент мультиагентной системы представлен на рис.2, где PCi-PCn – персональные компьютеры локальной вычислительной системы; Dij – информационные ресурсы i-го компьютера; Gi – программный агент, выполняющий роль посредника при организации доступа к ресурсам i-го компьютера.

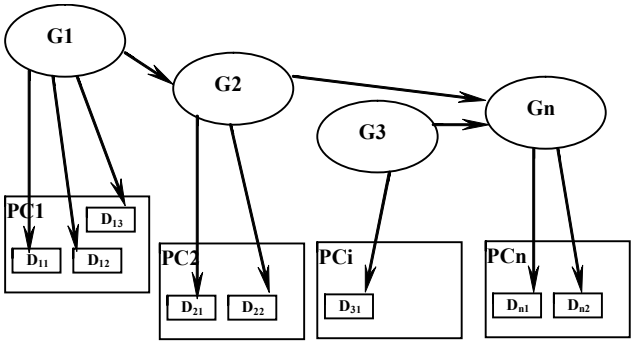

Рис. 2. Мультиагентная системы защиты информационных ресурсов вычислительной сети

Обозначим символом O множество объектов – множество персональных компьютеров PC, на которых решаются задачи администрирования: $O = \{O_1,...,O_n\}$. Множество программных агентов определим как: $G = \{G_1,...,G_n\}$. Каждый агент может находиться в двух состояниях:

– выполнение задачи по управлению доступом к соответствующему ресурсу;

– изменение, модификация внутреннего состояния для решения новых задач администратора мультиагентного пространства.

Все манипуляции в рассматриваемой модели выполняют процессы. Обозначим через P множество процессов: $P = \{P_{i1},...,P_{nm}\}$, где n – количество агентов и соответственно компьютеров в вычислительной сети; m – количество задач, решаемых агентом на компьютере n.

В качестве модели программного агента рассмотрим модель в виде фреймовой структуры. В общем случае модель фрейма имеет вид:

$$FR = [(R_1, A_1), (R_2, A_2), ...(R_n, A_n)], \qquad (2)$$

где FR – имя фрейма; R – имя слота; A – значение слота.

На основании модели фрейма (2) может быть представлена концептуальная модель программного агента в терминах <объекты>, <условия>, <действия>, <приоритет>. Каждый слот будет формироваться из четырех атрибутов базовых типов и реализовать процесс Pij по управлению информационным ресурсом Dij на i-м персональном компьютере.

Слот может быть спроектирован при помощи типового набора атрибутов. При этом в качестве базовых могут рассматриваться типы, приведенные в табл. 1.

Рассмотрим пример логической модели программного агента с именем SPY (табл. 2), который выполняет две задачи и, соответственно, состоит из двух слотов. Слот A1 содержит три атрибута. Первый атрибут определяет объект действия – файл с именем polis.doc. Второй атрибут определяет условие, при котором должно состояться выполнение операции, – если размер файла достигнет 50 Кб. Третий атрибут определяет вид операции или вид

Таблица 1

№ п/п	Сущности	Идентификатор	Область действия или набор операций данного типа
1	OBJECT (объекты)	OBG	База данных, файл, папка, диск, PC
2	ACTION (действия)	ACT	Читать, копировать, записать, поиск, наблюдать, защищать, ссылка, сценарий
3	CONDITIO N (условие)	CON	IF-THEN, предикат
4	STATUS (приоритет)	STA	Конфиденциально, очень важно, важно, общий доступ

Таблица 2

Имя программного агента SPY			
Имя слота	Базовые сущности		
A1	OBG: c:\TEMP\POLIS. doc	CON: IF size > 50kb	ACT: COPY to d:\MAIN
A2	OBG: c:\BASE\STUD. mdb		ACT: PROT d:\MAIN\hist. doc

действия – копировать файл polis.doc на диск D:\ в папку MAIN. Слот A2 - выполняет задачу регистрации доступа (время открытия) к файлу базы данных c:\BASE\STUD.mdb, протокол доступа хранит в файле d:\MAIN\hist.doc.

Концепция защиты информации в распределенных базах данных на основе мультиагентной системы может быть представлена в виде многоуровневой иерархической системы [5]. На каждом ее уровне решается определенный класс задач по защите информации. Все агенты в системе подчиняются некоторой иерархии в соответствии с выполняемыми функциями: «рядовые агенты», «агенты-менеджеры», «агенты-администраторы».

Существует несколько уровней защиты информации в информационной системе: уровень организационных мер, сетевой уровень, уровень рабочих станций и серверов сети.

Рассмотрим уровень защиты локальной БД. Его можно разделить на несколько подуровней, первый из которых – защита системы от несанкционированного доступа. Одним из способов защиты системы от несанкционированного доступа может быть метод идентификации индивидуального почерка пользователя при работе с информационной системой или базой данных. В этом случае программному агенту назначаются правила, по которым он разрешает доступ к данным, при соответствии образа пользователя его модели. В противном случае агент блокирует систему. Первичный образ пользователя формируется на основе индивидуальных параметров: скорость нажатия клавиш, последовательность выполнения физических операций пользователем и т.д.

Второй подуровень защиты информации – защита от внешних атак через локальную или глобальную сеть. Мультиагентная система защиты на основе мониторинга системы идентифицирует чужого агента или атаку и уведомляет администратора БД о несанкционированном вторжении.

К третьему подуровню можно отнести защиту от системных сбоев в операционной системе и в системе управления базами данных. В этом случае мультиагентная система осуществляет контроль целостности данных информационной системы. В функции системы защиты может входить задача контроля и анализа выполнения транзакций.

Реализация мультиагентной концепции защиты ресурсов информационной системы позволит значительно повысить надежность ее эксплуатации.

Литература: **1.** *Баранов А.А., Брыжко В.М., Базанок Ю.К.* Права человека и защита персональных данных. К.: Госкомсвязи Украины, 2000. 280 с. **2.** *Богуш В.М., Кудін А.М.* Інформаційна безпека «від А до Я». 3000 термінів та понять. К.: Техніка, 1999. 300 с. **3.** *Задірака В.К., Олексюк О.С.* Методи захисту фінансової інформації: Навчальний посібник. Тернопіль: "Збруч", 2000. 460 с. **4.** *Кульба В.В., Ковалевский С.С., Косяченко С.А., Сиротюк В.О.* Теоретические основы проектирования оптимальных структур распределенных баз данных. Серия «Информатизация России на пороге XXI века»/ М.:СИНТЕГ, 1999. 660 с. **5.** *Пономаренко Л.А, Филатов В.А.* Электронная коммерция / Под ред. А.А.Мазаракн. К.: Київ.нац.торг.-екон.ун-т, 2002. 443 с. **6.** *O'Brien James A.* Management Information Systems: managing information technology in the internetworked enterprise. 4th ed. McGraw-Hill, 1999. 700 p. **7.** *Wooldridge M., Jennings N.R.* Intelligent Agents: Theory and Practice // The Knowledge Engineering Review. 1995. Vol. 10, N 2. P.115-152.

Поступила в редколлегию 16.12.2002

Резенцент: д-р техн. наук, проф. Путятин В.П.

Гвоздинский Анатолий Николаевич, канд. техн. наук, профессор кафедры ИИ ХНУРЭ. Научные интересы: оптимизация процедур принятия решений в сложных системах управления. Адрес: Украина, 61166, Харьков, ул. Акад. Ляпунова, 7, кв. 9, тел.32-69-08.

Филатов Валентин Александрович, канд. техн. наук, доцент кафедры ИИ ХНУРЭ. Научные интересы: разработка и проектирование распределенных информационных систем и баз данных, агентные технологии. Хобби: футбол, автомобили. Адрес: Украина, 61031, Харьков, ул. Ромашкина, №6-а, кв.19, тел. 66-05-86, 40-94-32.

Чалая Лариса Эрнестовна, аспирантка кафедры ИИ ХНУРЭ. Научные интересы: агентные технологии, мультиагентные системы, системы распределенных баз данных. Хобби: чтение. Адрес: Украина, 61001, Харьков, ул. Державинская, 46-а, тел. 40-96-40.