вис в непрерывном режиме в любой момент времени круглый год.

Литература

1. Everitt B.S., Landau S., Leese M. Cluster Analysis. A Hodder Arnold Publ., 2001, pp. 120–234.
2. Пономаренко В.С., Листровой С.В., Минухин С.В., Знахур С.В. Методы и модели планирования ресурсов в GRID-системах. Украина, Харьков: Издат. дом ИНЖЭК, 2008. 408 с.
3. Стивенс Р., Раго С. UNIX: профессиональное программирование: 2-е изд. СПб: Символ-Плюс, 2007. 1040 с.
4. Стивенс Р., Феннер Б., Рудофф Э.М. UNIX: разработка сетевых приложений: 3-е изд. СПб: Питер, 2007. 1039 с.

References

1. Everitt B.S., Landau S., Leese M. *Cluster Analysis*. A Hodder Arnold Publ., 2001, pp. 120–234.
2. Ponomarenko V.S., Listrovoy S.V., Minukhin S.V. *Metody i modeli planirovaniya resursov v GRID- sistemakh* [Planing methods and models for resourses in GRID-systems]. Ukraine, Kharkov, INZHEK Publ., 2008, pp. 95–102 (in Russ.).
3. Stivens R., Rago S. *UNIX professionalnoye programmirovaniye* [UNIX professional programming]. 2nd ed., St. Petersburg, Simvol-Plyus Publ., 2007, pp. 504–532.
4. Stivens R., Fenner B., Rudoff E.M. *UNIX: razrabotka setevykh prilozheniy* [UNIX developing network applications]. 3rd ed., St. Petersburg, Piter Publ., 2007, pp. 185–222.

УДК 004.05

ЗАЩИТА ИНФОРМАЦИИ В САМООРГАНИЗУЮЩЕЙСЯ ИНФОРМАЦИОННОЙ СИСТЕМЕ БЕЗ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ СРЕДСТВ

В.В. Дрождин, к.т.н., доцент, зав. кафедрой; Р.Е. Зинченко, к.т.н., доцент
(Пензенский государственный университет,
ул. Красная, 40, г. Пенза, 440026, Россия, drozhdin@yandex.ru, rzinchenko@yandex.ru)

Рассматривается обеспечение безопасного доступа в самоорганизующейся информационной системе. Проанализировано текущее состояние информационной безопасности и защиты данных. Для повышения уровня безопасности самоорганизующейся информационной системы предложено использование трех компонентов: взаимодействие информационной системы с системой иерархически связанных пользователей, взаимодействие пользователей с системой через области видимости, регулярная аутентификация пользователей по их поведению.

Взаимодействие информационной системы с системой иерархически связанных пользователей, объединенных в сетевую структуру, с одной стороны, упрощает создание системы и обеспечивает контроль и управление деятельностью подчиненных пользователей вышестоящими пользователями, а с другой – предоставляет возможность системе обратиться за помощью к вышестоящим пользователям в случае возникновения сложной или неопределенной ситуации с конкретным пользователем.

Использование механизма областей видимости для всех пользователей системы позволяет легко формировать пользовательские представления о предметной области и делегировать полномочия вышестоящих пользователей подчиненным пользователям, а самоорганизующаяся информационная система будет обеспечивать корректное функционирование и эффективную обработку данных, соответствующие концептуальной модели предметной области.

Реализация регулярной аутентификации пользователей в самоорганизующейся информационной системе по их поведению позволит более точно идентифицировать каждого пользователя системы и более корректно предоставлять конфиденциальные полномочия.

Таким образом, предложенный подход естественным образом сочетает программные (автоматические) и организационные средства защиты информационной системы.

Ключевые слова: *самоорганизующаяся информационная система, защита информации, аутентификация пользователя, модель предметной области, область видимости.*

DATA PROTECTION IN SELF-ORGANIZING INFORMATION SYSTEM WITHOUT USING SPECIAL FACILITIES

Drozhdin V.V.*, Ph.D. Tech. Sc., associate professor, head of chair;* ***Zinchenko R.E.****, Ph.D. Tech. Sc., associate professor*
(Penza State University, Krasnaya St., 40, Penza, 440026, Russian Federation,
drozhdin@yandex.ru, rzinchenko@yandex.ru)

Abstract. The safe access in self-organizing information system is described. The current state of information security and data protection is shown. To increase a level of safety of self-organizing information system three components are offered: interaction of information system with system of hierarchically connected users, interaction of users with the system via visibility areas, regular users' authentication based on their behavior.

Interaction of information system with the system of hierarchically connected users united in a network structure, on the one hand, simplifies system creation and provides control of subordinated users' activity by higher users. On the other hand,

it gives an opportunity to the system to gain the help of higher users in case of a difficult or uncertain situation with the specific user.

Using the areas visibility mechanism for all users allows to form the user representation of data domain easily and to delegate powers of higher users to the subordinated users, and the self-organizing information system will provide the correct functioning and the effective data processing according to conceptual data domain model.

Regular users' authentication in self-organizing information system based on their behavior will allow to identify each user more precisely and to confer confidential powers more correctly.

Thus, the offered approach combines naturally both program (automatic) and organizational means of information system security.

Keywords: self-organizing information system, information security, user authentication, data domain model, scope.

В современных информационных системах очень важное значение придается безопасности и защите информации.

Защитой данных называется предотвращение доступа к ним со стороны несанкционированных пользователей и обеспечение выполнения пользователями только разрешенных действий. Поэтому систему защиты информации в информационной системе составляют технические, программные и программно-технические средства защиты информации, а также средства контроля эффективности защиты информации.

Основными механизмами защиты информации в *автоматизированных информационных системах* (АИС) являются регистрация и учет пользователей системы, управление доступом пользователей к данным, криптографическая защита данных, обеспечение целостности БД.

Целесообразно, чтобы все меры по обеспечению безопасности АИС выполнялись средствами самой компьютерной системы автоматически.

На основе анализа источников [1, 2] можно сделать вывод, что решение проблемы обеспечения защиты данных идет по пути наращивания количества всевозможных специальных средств, таких как биометрические средства (дактилоскопические считыватели, устройства измерения геометрии ладони, голосовая верификация, считывание радужной оболочки и сетчатки глаза, устройства распознавания подписей), электронные жетоны – генераторы случайных последовательностей, электронные внешние ключи классов Touch Memory и eToken, механические ключи, пластиковые карты различных технологий и др.

Использование указанных средств сопровождается повышением сложности процедур регистрации и входа в систему и ужесточением политик доступа, что чрезвычайно усложняет работу пользователей с АИС и требует большого штата специалистов для обслуживания системы защиты информации.

Рассмотрим преимущества самоорганизующейся информационной системы в обеспечении безопасности и защиты информации.

Прежде всего необходимо отметить, что все указанные проблемы являются следствием того, что в современных информационных системах пользователи рассматриваются как множество независимых друг от друга объектов (рис. 1).

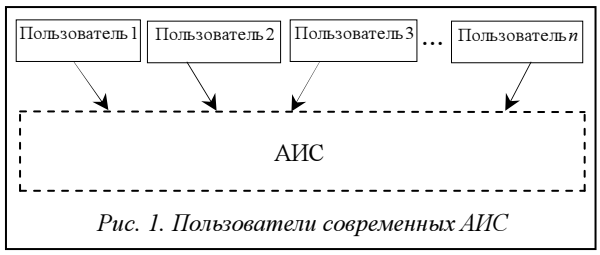

Рис. 1. Пользователи современных АИС

Хотя у разных пользователей разные права, однако с точки зрения АИС они ничем не отличаются друг от друга и не имеют друг к другу никакого отношения. Поэтому для управления доступом пользователей к АИС используются многочисленные внешние средства и искусственные правила, с помощью которых специалисты пытаются решить возникающие проблемы.

Целесообразно признать такое взаимодействие пользователей с АИС крайне непродуктивным, неэффективным и не способствующим качественному решению проблем безопасного доступа и защиты информации, что давно вызывает критику. Еще в 1989 г. авторы работы [3] предлагали взаимодействие АИС с вложенными пользовательскими группами и указывали, что способность классифицировать пользователей в виде иерархии групп является мощным инструментом администрирования больших систем с тысячами пользователей и объектов. Поэтому предлагается новый подход к взаимодействию пользователей с информационной системой, которая должна быть самоорганизующейся.

Самоорганизующейся информационной системой (СИС) называется система, способная активно поддерживать свое существование и обеспечивать решение информационных задач с требуемым качеством в течение длительного времени в условиях существенных изменений внешней среды и внутренней организации системы.

Под существенными изменениями внешней среды понимаются изменения с возникновением ситуаций высокой агрессивности среды (например несанкционированный доступ) либо недостаточности ресурсов (например машинного времени или объема памяти).

В предлагаемом авторами подходе с СИС должна взаимодействовать система иерархически связанных пользователей, объединенных в сетевую структуру (рис. 2).

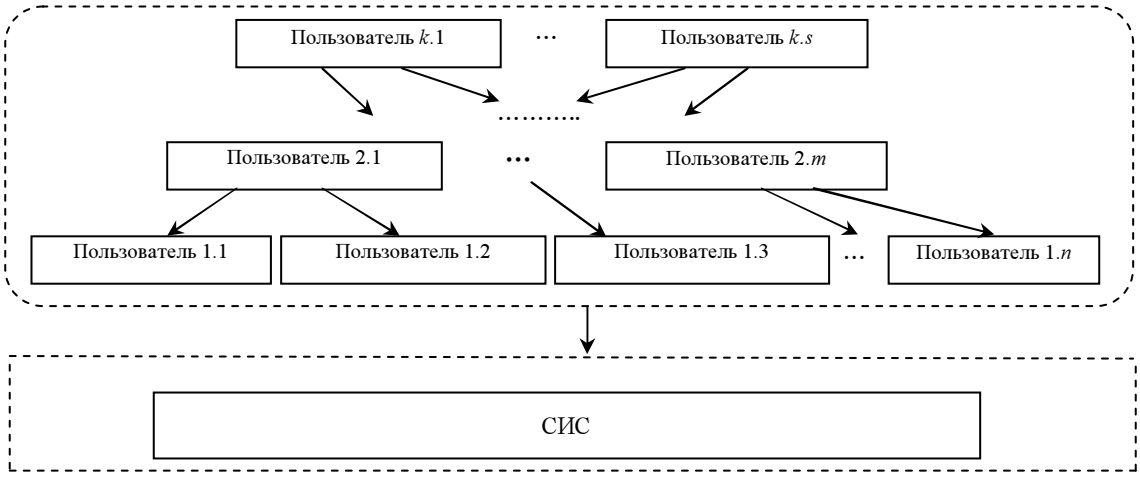

Рис. 2. Взаимодействие с СИС системы иерархически связанных пользователей

Таким образом, СИС организует свое взаимодействие с внешней средой не как с множеством отдельных пользователей, а как с системой взаимосвязанных пользователей. Поэтому каждый пользователь имеет определенную позицию в модели пользователей СИС. Данный подход способствует тому, что вышестоящие пользователи могут контролировать и управлять деятельностью подчиненных пользователей, а система при взаимодействии с конкретным пользователем всегда знает, к кому ей необходимо обратиться при возникновении сложных, неопределенных ситуаций.

В целом взаимодействие СИС с системой пользователей позволяет существенно снизить затраты на ее эксплуатацию, так как наличие иерархических отношений между пользователями позволяет распределить обязанности администрирования системы среди довольно большого числа иерархически привилегированных пользователей. Это делает СИС достаточно прозрачной снизу вверх и реализует возможность естественного контроля вышестоящими пользователями действий нижестоящих пользователей.

Другой особенностью СИС является то, что пользователи получают возможность формировать собственное представление о *предметной области* (ПрО) и решаемых задачах в форме концептуальной модели ПрО [4] и формулируют информационные потребности путем оперирования понятиями. Совместно с иерархическими отношениями между пользователями это позволяет естественным путем реализовать механизм областей видимости для каждого пользователя СИС, что существенно повышает защищенность системы без применения специальных средств защиты.

Для каждого пользователя на уровне концептуальной модели предметной области определяется подмодель, называемая областью видимости данного пользователя (рис. 3). Учитывая, что БД СИС создает и поддерживает самостоятельно на основе концептуальной модели ПрО, доступ пользователей к данным и их обработка полностью определяются областью видимости. Данный подход позволяет обеспечить одно из важнейших требований [1] к защите информации: пользователи будут получать доступ только к той информации и с теми возможностями по ее обработке, которые соответствуют их функциональным обязанностям.

Область видимости для каждого пользователя определяется его вышестоящим пользователем. Поэтому в СИС осуществляется реализация концепции доступа, которую можно определить как «все запрещено». В соответствии с расширением функциональной деятельности и решаемых задач будет изменяться и область видимости пользователя.

В случае подчинения некоторого пользователя нескольким вышестоящим пользователям его подмодель ПрО представляется совокупностью взаимосвязанных секций, которые будут доступны соответствующим вышестоящим пользователям. Контроль деятельности подчиненных пользователей вышестоящими пользователями осуществляется правом на просмотр и модификацию любых действий, выполненных подчиненными пользователями. Поэтому, если какой-либо пользователь пытается выполнить в системе действие, которое им ранее не выполнялось, СИС инициирует запрос к вышестоящему пользователю на разрешение этих действий.

Вследствие такого функционирования у пользователей будет больше доверия к системе, что обеспечит более интенсивное взаимодействие системы пользователей и СИС и создаст реальные условия для их коэволюции и возникновения системы принципиально нового типа. Новая система будет являться суперсистемой и включать СИС и систему пользователей как равноправные подсистемы.

Существенной проблемой в рамках организации защиты данных в АИС является аутентификация пользователей, заключающаяся в умении

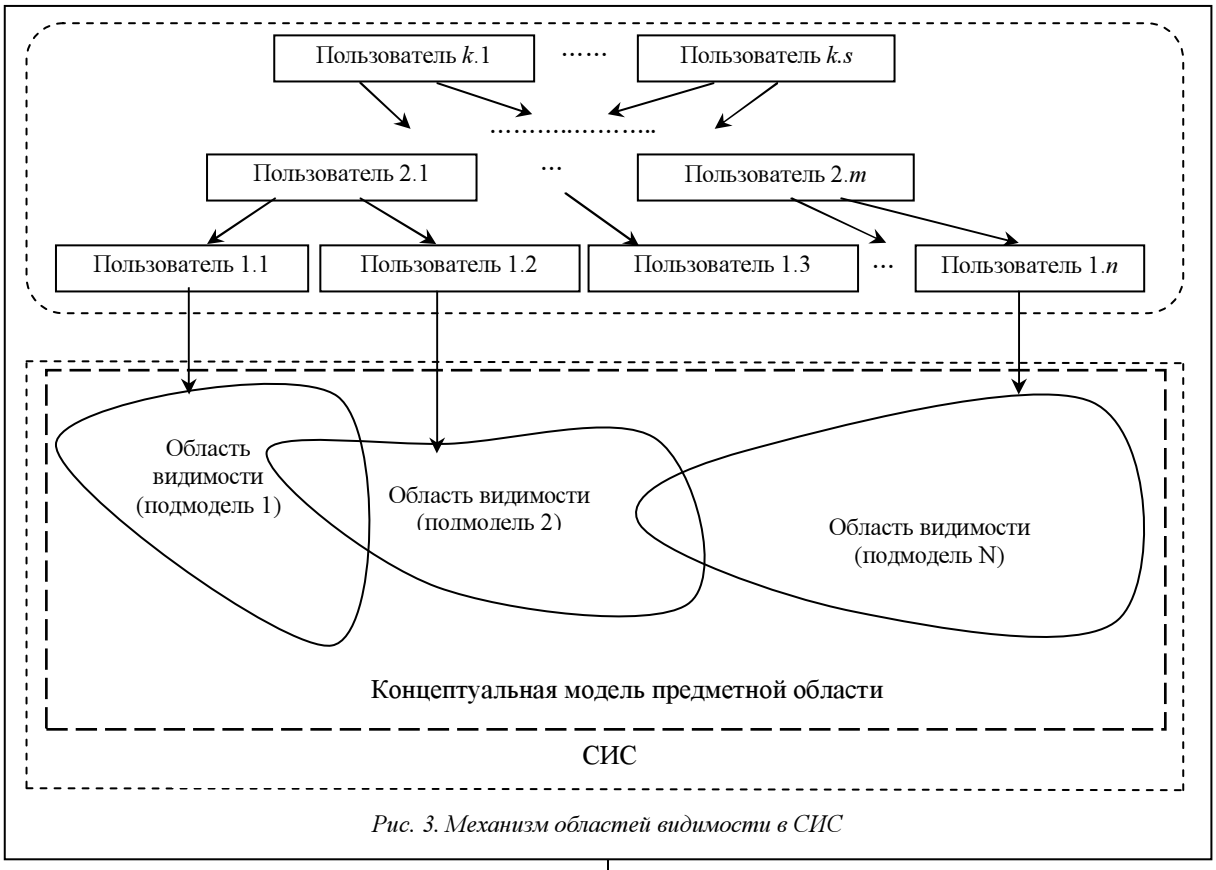

Рис. 3. Механизм областей видимости в СИС

системы опознавать конкретного пользователя. В настоящее время в большинстве случае аутентификация пользователя осуществляется путем ввода пароля. При этом предполагается, что пароль известен только системе и тем лицам, которые имеют право применять данный идентификатор пользователя [5]. Однако на практике это предположение не всегда оказывается истинным. Если какому-либо лицу становятся известны логин/пароль пользователя АИС, то АИС не в состоянии препятствовать действиям данного лица в системе.

В отличие от этого СИС будет обладать способностью опознавать поведение пользователя и в случае обнаружения каких-либо нестандартных, отклоняющихся от обычной практики действий будет сигнализировать об этом вышестоящим пользователям и фиксировать в журналах аудита либо блокировать действия данного пользователя.

В [1, 5] указывается, что во многих системах управления БД поддерживаются дискреционный, мандатный или оба способа управления доступом одновременно. В СИС внутренняя организация управления доступом существенно сложнее, однако для пользователей она естественна и не требует больших усилий.

Кроме этого, в [5] указывается, что в действующем стандарте языка SQL предусматривается поддержка только избирательного метода управления доступом, осуществляемая двумя механизмами:

– механизмом представлений, позволяющим скрывать важные данные от несанкционированных пользователей;

– подсистемой авторизации, предоставляющей возможность привилегированным пользователям избирательно назначать необходимые полномочия менее привилегированным пользователям, а также отзывать предоставленные полномочия в случае необходимости.

В [5] описывается способ защиты данных в прототипе системы University Ingres, заключающийся в том, что любой запрос перед выполнением автоматически модифицировался таким образом, чтобы предотвратить любые возможные нарушения установленных ограничений защиты. Например, если для некоторого пользователя доступны для просмотра в БД только те детали, которые хранятся в Лондоне, то при выполнении им запроса

```
SELECT *
FROM Детали
```

система автоматически преобразует его к виду

```
SELECT *
FROM Детали
WHERE Город = 'Лондон'.
```

Предлагаемый подход конструктивно является усовершенствованием и существенным расширением данной идеи. Источник разграничений доступа – концептуальная модель предметной области, в которой каждому пользователю видна только его часть предметной области. Далее СИС создает

БД, соответствующую концептуальной модели предметной области, а также систему базовых запросов, в которых уже заложены все необходимые ограничения видимости в соответствии с подмоделью ПрО каждого пользователя.

Таким образом, доступ к БД и обработка данных в СИС возможны только через концептуальную модель предметной области и области видимости пользователей, что обеспечивает корректное функционирование системы и автоматическую реализацию мощных механизмов защиты информации. При этом предложенный подход способствует наиболее тесному сотрудничеству пользователей и выполнению ими кооперативных действий, способствующих более высокому темпу развития предприятия и конкурентным преимуществам на рынке.

Литература

1. Духан Е.И., Синадский Н.И., Хорьков Д.А. Применение программно-аппаратных средств защиты компьютерной информации: учеб. пособие. Екатеринбург: УГТУ-УПИ, 2008. 182 с.
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: Академия, 2008. 336 с.
3. Gagliardi R., Lapis G., Lindsay B. A flexible and efficient database authorization facility. IBM Res. Rep. RJ6826, San Jose, CA, 1989.
4. Дрождин В.В., Зинченко Р.Е. Информатизация предприятия на основе самоорганизующейся информационной системы // Инновации в управлении и образовании: технико-технологические и методические аспекты: матер. II Междунар. науч.-практич. конф. В 2-х т. Тула, 2009. Т. 2. С. 91–93.
5. Дейт К. Введение в системы баз данных. М.: Вильямс, 2006. 1328 с.

References

1. Dukhan E.I., Sinadskiy N.I., Horkov D.A. *Primenenie programmno-apparatnykh sredstv zashhity kompyuternoy informatsii: ucheb. posobie* [Application of computer information security firmware: tutorial]. Ekaterinburg, Ural. State Tech. Univ. Publ., 2008 (in Russ.).
2. Melnikov V.P., Kleymenov S.A., Petrakov A.M. *Informatsionnaya bezopasnost i zashchita informatsii* [Information security]. Moscow, Akademiya Publ., 2008 (in Russ.).
3. Gagliardi R., Lapis G., Lindsay B. *A flexible and efficient database authorization facility*. IBM Res. Rep. RJ6826, San Jose, CA, 1989.
4. Drozhdin V.V., Zinchenko R.E. *Materialy II Mezhdunar. nauchno-prakticheskoy konf. "Innovatsii v upravlenii i obrazovanii: tekhniko-tekhnologicheskie i metodicheskie aspekty"* [Proc. of the 2nd int. research-to-practice conf. "Innovations in management and education: engineering and methodological aspects"]. Tula, 2009, vol. 2, pp. 91–93 (in Russ.).
5. Date C.J. *Introduction to Database Systems*, 8th Ed. Addison-Wesley, 2003, 1024 p.

УДК 004.896

ИНТЕЛЛЕКТУАЛЬНОЕ УПРАВЛЕНИЕ РОБОТОМ-МАНИПУЛЯТОРОМ НА ОСНОВЕ МЯГКИХ ВЫЧИСЛЕНИЙ

А.В. Николаева, аспирант; С.В. Ульянов, д.ф.-м.н., профессор
(Международный университет природы, общества и человека «Дубна», Институт системного анализа и управления, ул. Университетская, 19, г. Дубна, 141980, Россия, nikolaevaav@lenta.ru, ulyanovsv@mail.ru)

Рассматривается проблема проектирования интеллектуальных систем управления с применением технологий мягких вычислений на примере робота-манипулятора с тремя степенями свободы. Приводится общая методология проектирования робастных баз знаний с использованием специального интеллектуального инструментария – оптимизатора баз знаний на мягких вычислениях. Предложены варианты организации координационного управления: создание единой базы знаний, содержащей информацию о трех звеньях робота-манипулятора, а также метод разделения (декомпозиции) управления – создание независимых баз знаний для индивидуального управления звеньями. Эффективность спроектированных интеллектуальных систем управления с применением технологий мягких вычислений рассматривается в сравнении с системой управления с постоянными параметрами регулирующего звена, определенными с помощью генетического алгоритма. Для оценки работы систем управления введена система критериев качества, учитывающая методы оценки переходных процессов теории автоматического управления, адаптированная для рассматриваемого объекта управления – робота-манипулятора с тремя степенями свободы. Оценка работы систем управления производится по результатам моделирования в среде MatLab/Simulink и по результатам серии экспериментов на физическом макете объекта управления.

Ключевые слова: *интеллектуальная система управления, нечеткий регулятор, база знаний, технологии мягких вычислений.*

INTELLIGENT CONTROL OF A ROBOT MANIPULATOR BASED ON SOFT COMPUTING

Nikolaeva A.V.*, postgraduate student;* ***Ulyanov S.V.****, Dr.Sc. (Physics and Mathematics), professor*
(Dubna Internacional University for Nature, Socitty and Man, Universitetskaya St., 19, Dubna, 141980, Russian Federation, nikolaevaav@lenta.ru, ulyanovsv@mail.ru)

Abstract. The problem of designing control systems using soft computing is described with 3 degrees of freedom manipulator as an example. The article investigates a general methodology of robust knowledge base design using special