В докладе В.М. Федоров, Д.П. Рублев (ЮФУ, г. Таганрог), Е.М. Панченко (НИИ Физики ЮФУ, г. Ростов-на-Дону) «Сегментация виброакустических сигналов, возникающих при нажатии/отпускании клавиш клавиатуры» рассмотрена проблема сегментации виброакустических сигналов, возникающих при наборе данных на клавиатуре. Предложены алгоритмы сегментации сигналов на основе дискретного вейвлет-преобразования и условия превышения порога пиками сигнала для идентификации принадлежности фрагмента виброакустического сигнала нажатию либо отпусканию клавиши. Точность идентификации, по заявлению авторов, составила более 96 %.

В докладе Т.А. Гришечкина, О.Б. Макаревич, ЮФУ, г. Таганрог «Выявление вредоносных узлов в сетях ad hoc при различных типах атак» показано применение методики выявления вредоносных узлов в сети ad hoc с кластерной архитектурой. Описывается поведение вредоносных узлов со стороны различных типов атак, которые они могут осуществлять. Кроме того, приводятся примеры поведения узлов при межкластерном взаимодействии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Материалы XIII Международной научно-практической конференции «Информационная безопасность». Ч. I. – Таганрог: Изд-во ЮФУ, 2013. – 276 с.
2. Материалы XIII Международной научно-практической конференции «Информационная безопасность». Ч. II. Материалы III Всероссийской молодежной конференции «Перспектива-2013». – Таганрог: Изд-во ЮФУ, 2013. – 252 с.

Статью рекомендовал к опубликованию к.т.н. М.Ю. Руденко.

Брюхомицкий Юрий Анатольевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: bya@tgn.sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Макаревич Олег Борисович – e-mail: mak@tsure.ru; тел.: 88634312018; кафедра безопасности информационных технологий; зав. кафедрой.

Bryukhomitsky Yuriy Anatoly – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University” e-mail: bya@tgn.sfedu.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; associate professor.

Makarevich Oleg Borisovich – e-mail: mak@tsure.ru; phone: +78634312018; the department of security in data processing technologies; head of the department.

УДК 004.056.5, 004.89

А.М. Цыбулин, М.Н. Свищева

СИСТЕМНЫЙ ПОДХОД К ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ БОРЬБЫ С ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТЬЮ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОРГАНИЗАЦИИ

Предлагается системный подход к повышению эффективности борьбы с инсайдерской деятельностью пользователей. Контролируется эффективность работы пользователей с любой информацией в течение рабочего времени. Оценка эффективности работы персонала имеет своей целью сопоставить реальное содержание, качество, объемы и интенсивность труда персонала с установленными нормами. Для противодействия утечкам информации по вине внутренних нарушителей разработан программный комплекс, кото-

рый позволяет выявить потенциально опасные действия пользователей, оценить эффективность выполнения ими должностных обязанностей и предотвратить утечку конфиденциальной информации. Изложены результаты апробации данного программного комплекса. Проведенные экспериментальные исследования показали, что программный комплекс достоверно определяет пользователей, которые нарушают установленную политику безопасности, и предложенные им рекомендации позволяют повысить эффективность их работы. Эффективность работы удалось повысить на 12 %, за счет блокирования инсайдерской деятельности пользователей.

Атака; инсайдерская деятельность; информационная безопасность; инвентаризация; эффективность работы пользователя.

A.M. Tsybulin, M.N. Svishcheva

SYSTEMS APPROACH TO IMPROVE THE EFFICIENCY AGAINST INSIDER USERS IN THE ORGANIZATION'S INFORMATION SYSTEMS

Systematic approach to improving the effectiveness of a struggle against insider activities of the users is suggested in this article. The effectiveness of users' work with any information during working hours is controlled. Employee performance evaluation aims to compare the actual content, quality, volumes and intensity of work of the personnel with the established norms. To counter the information leaks through the fault of insiders software complex that enables to identify a potentially hazardous actions of users, to evaluate the effectiveness of their functions implementation and to prevent leakage of confidential information has been developed. The results of this software package approbation are presented. The experimental researches have shown, that the program complex reliably identifies users who violate the established security policy and its proposed recommendations allow improving the efficiency of their work. Efficiency was increased by 12 %, by blocking the insider activities of users.

Attack; insider activity; information security; inventory; user efficiency.

Результаты глобального исследования утечек корпоративной информации и конфиденциальных данных в 2012 г. «Аналитического Центра InfoWatch» показывают, что в мире зафиксировано и обнародовано в системах массовой информации 934 случая утечки конфиденциальных данных. Превышен на 16 % аналогичный показатель 2011 г. Отметим только два факта: до 38 % снизились случайные утечки; с 9 % до 29 % повысилась доля утечек в госкомпаниях и муниципальных учреждениях.

Эти результаты позволяют сделать вывод, что отсутствовал системный подход при проектировании систем защиты информации. Они были в основном ориентированы на защиту каналов связи и инфраструктуры. Основная цель системы защиты – это защита данных вне зависимости от их физического местонахождения.

Системный подход к информационной безопасности требует определения ее субъектов, средств и объектов, источников опасности, направленности опасных информационных потоков и принципов обеспечения информационной безопасности.

Объектом информационной безопасности является информация (данные), информационные системы различного масштаба и назначения, которые обрабатывают, получают, передают и хранят информацию.

Субъектами информационной безопасности следует считать пользователей, которые в рамках информационной системы работают с информацией, органы и структуры, которые занимаются ее обеспечением.

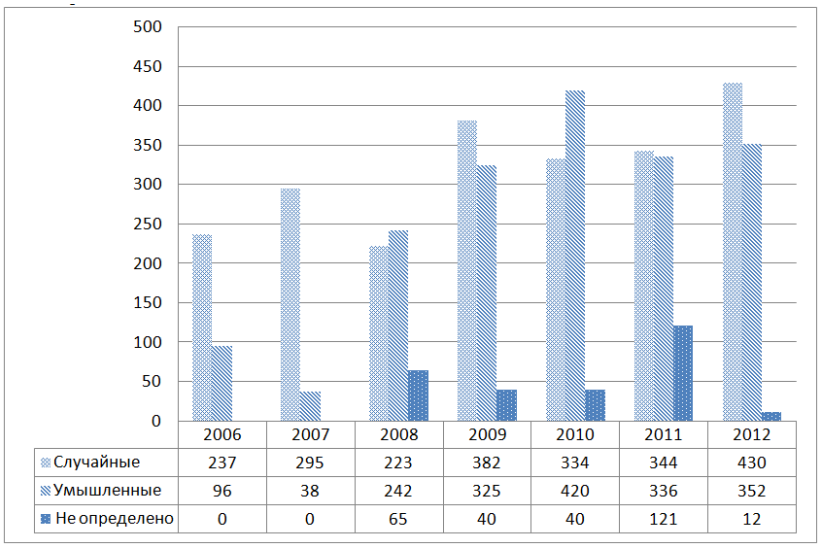
Средства обеспечения информационной безопасности – это средства, с помощью которых осуществляются меры по защите информации, систем управления, связи, компьютерных сетей, недопущению подслушивания, маскировке, предотвращению хищения информации и т.д.

Источники опасности подразделяются на умышленные и на случайные. Умышленные воздействия (программные, технические и т.д.) осуществляются сознательно и целенаправленно, эти воздействия проводятся злоумышленниками и пользователями инсайдерами. Случайные воздействия (программные, технические и т.д.) осуществляются не сознательно, реализуются законными пользователями.

К принципам обеспечения информационной безопасности относятся: законность, баланс интересов личности, общества и государства, комплексность, системность, интеграцию с международными системами безопасности, экономическую эффективность и т.д.

Доля умышленных и случайных утечек информации от собственных пользователей в количественном и качественном (по сумме ущерба) значительно превосходит другие утечки.

Распределения случайных и умышленных утечек данных по каналам за 2012 г. на основании аналитического отчета российской компании InfoWath представлены на рис. 1 [1].



	2006	2007	2008	2009	2010	2011	2012
Случайные	237	295	223	382	334	344	430
Умышленные	96	38	242	325	420	336	352
Не определено	0	0	65	40	40	121	12

Рис. 1. Динамика соотношения случайных и умышленных утечек, 2006–2012 гг.

Анализ диаграмм показывает рост количества случайных и умышленных утечек информации, а значит увеличение доли рабочего времени, которое используют пользователи инсайдеры для передачи этих данных.

Предлагается системный подход к повышению эффективности борьбы с инсайдерской деятельностью пользователей. Контролируется эффективность работы пользователей с любой информацией в течение рабочего времени.

Оценка эффективности работы персонала имеет своей целью сопоставить реальное содержание, качество, объемы и интенсивность труда персонала с установленными нормами.

При оценке эффективности работы пользователя проводится анализ его действий. Для каждого пользователя предполагается наличие шаблона эталонных действий с файлами и каталогами, к которым пользователь имеет доступ, шаблона необходимого программного и аппаратного обеспечения на компьютере пользователя для выполнения им своей работы. Для оценки осуществляется контроль текущих действий и сравнение с эталонным шаблоном. Таким образом, анализ дей-

ствий пользователя позволяет оценить распределение рабочего времени, выявить среди них несанкционированные и перекрыть потенциально возможные каналы утечки информации.

В среднем пользователь при восьмичасовом рабочем дне согласно ст. 108 Трудового Кодекса Российской Федерации имеет право на перерывы для отдыха и питания от 30 минут до 2 часов, то есть время отдыха пользователя может занимать до 25 % всего рабочего времени [2].

При оценке эффективности работы каждого пользователя оценивается, сколько времени он тратит на выполнение своих должностных обязанностей и соответствует ли данная величина нормативам.

При оценке эффективности *E* предполагается наличие некоторого эталонного образца работы пользователя, сравнивая с которым можно сделать вывод об эффективности работы пользователя и его проблемных характеристиках работы [3].

Эталонная модель эффективности E_n работы каждого пользователя в информационной системе представляется в виде следующего кортежа:

$$E_n = (Q_n, C_n, P_n, T_n), \quad (1)$$

где Q_n – требования к количеству выполненных работ, C_n – требования к качеству выполненных работ, P_n – требования к операциям и действиям пользователя, T_n – требования к длительности рабочего времени пользователя. Аналогичным образом описывается текущая эффективность работы i-го пользователя E_{ti}, параметры $Q_{ti}, C_{ti}, P_{ti}, T_{ti}$ характеризуют текущие значения:

$$E_t = (Q_t, C_t, P_t, T_t). \quad (2)$$

Путем сопоставления кортежа (1) и кортежа (2) получаем следующий кортеж:

$$E = (Q, C, P, T).$$

Расчет показателей эффективности осуществляется следующим образом:

1. Оценка полезности использования рабочего времени (в процентах):

$$T = \frac{T_t}{T_n} * 100\ \%,$$

где T_t – время, затраченное пользователем на выполнение своих должностных обязанностей, T_n – нормативное время работы пользователя.

T_t является суммарным временем, затраченным пользователем на работу.

$$T_t = T_e + T_u,$$

где T_e – это полезное время, в течение которого пользователь решал функциональные задачи; T_u – это бесполезное время, в течение которого пользователь работал как инсайдер, решал другие задачи.

Все множество действий, выполняемых пользователем, разделяется на два подмножества: разрешенных и запрещенных операций.

Тогда общее бесполезное время определяется как:

$$T_u = \sum_{i=1}^{n} k(i) * T_i,$$

где n – общее количество задач, которые должен решить пользователь в ходе работы,

$$k(i) = \begin{cases} 1, & \text{если дейсвие является не разрешенным для пользователя} \\ 0, & \text{если действие ясляется разрешенным для пользователя} \end{cases}$$

Время, затраченное на работу, определяется как:

$$T_e = T_n - T_u.$$

2. Относительное количество выполненных работ за время T_t:

$$Q = \frac{Q_t}{Q_n} * 100\ \%,$$

где Q_t – текущее количество выполненных работ, Q_n – требуемое количество выполненных работ;

3. Относительное качество выполненных работ за время T_t:

$$C = \sum_{i=1}^{Q} \frac{C_{t_i}}{C_n} * 100\ \%,$$

где C_n – требуемое качество выполненных работ, C_t – текущее качество выполненных работ;

4. Требования к операциям и действиям пользователя за время T_t:

$$P_n = \begin{cases} 0, \text{не обнаружены запрещенные действия} \\ 1, \text{обнаружены запрещенный действия} \end{cases}.$$

Действия пользователя в ходе работы можно оценить исходя из содержания журналов безопасности Windows 7 и используемого оборудования пользователем. Для формирования эталонного значения данного параметра проводится инвентаризация программных и аппаратных средств, которая определяет их исходные свойства, а так же определяется перечень программ и ресурсов, необходимых пользователю для выполнения работ [4]. Таким образом, действия пользователя P_n описываются в виде кортежа:

$$P_n = (S, H, S_w, H_w, I),$$

где S – перечень программного обеспечения, установленного на рабочем компьютере пользователя, H – перечень аппаратного обеспечения и его конфигурация, установленного на рабочем компьютере пользователя, S_w – перечень программного обеспечения, необходимого для работы пользователю, H_w – перечень аппаратного обеспечения, необходимого для работы пользователю, I – перечень информационных ресурсов, необходимых пользователю для работы и создаваемых в ходе работы.

Таким образом, эффективность работы пользователя может быть определена на основе сравнения текущих значений параметров кортежа E_t (2) с эталонными значениями кортежа E_n (1).

Задача оценки эффективности E_t является многокритериальной оптимизационной задачей следующего вида: max T_e, max Q, max C, min P.

Сведем ее к однокритериальной оптимизационной задаче, выделив в качестве основного показателя E. Остальные переводятся в разряд ограничений:

$$\max E,$$

при ограничениях:

$$\begin{cases} \mathrm{C} \geq 1 - \mathrm{C}_{\text{д}}, \\ Q \geq 1 - Q_{\text{д}}, \\ P \to 0, \\ T \geq T_{\text{д}}. \end{cases}$$

Данная задача эквивалентна следующей задаче:

$$\min T_u,$$

при ограничениях

$$\begin{cases} \mathrm{C} \geq 1 - \mathrm{C}_{\text{д}}, \\ Q \geq 1 - Q_{\text{д}}, \\ P \to 0. \end{cases}$$

где T_u – бесполезное время, в течение которого пользователь решал другие задачи, $Q_{\text{Д}}$, $C_{\text{Д}}$, $T_{\text{Д}}$ – допустимое относительное отклонение соответственно количество и качество выполненных работ, n – количество бесполезных работ.

Предложенная математическая модель позволяет оценить эффективность работы i-го пользователя.

Для реализации разработанной математической модели был разработан программный комплекс [5, 6], архитектура которого представлена на рис. 2.

Он включает в себя клиентскую и серверную части. Клиентская часть устанавливается на машину пользователя и осуществляет сбор характеристик работы контролируемого пользователя. В состав клиентской части входят следующие модули: «Инвентаризация программных ресурсов», «Инвентаризация аппаратных ресурсов», «Ввод характеристик работы пользователя», «Определение доступных пользователю ресурсов», «Аудит текущих действий пользователя», «Работа с базой данных результатов проверок», «Связь с сервером».

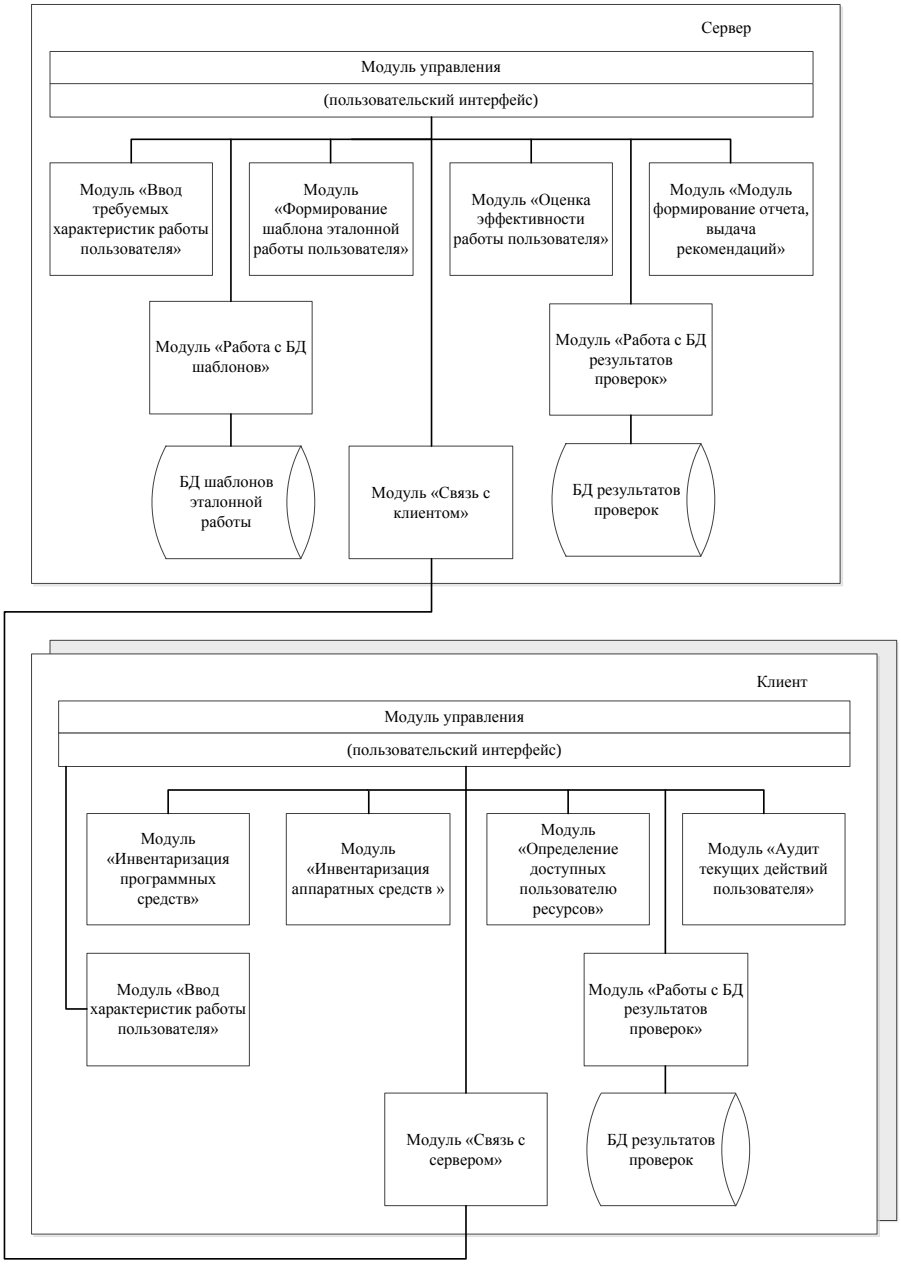


Рис. 2. Архитектура программного комплекса для оценки эффективности работы персонала

В состав серверной части входят следующие модули: «Ввод требуемых характеристик работы пользователя», «Формирование шаблона эталонной работы пользователя», «Оценки эффективности работы пользователя», «Формирование отчета, выдача рекомендаций», «Работа с базой данных шаблонов», «Работа с базой данных результатов проверок», «Связь с клиентом».

Все модули реализованы в виде интеллектуальных агентов, которые основе своих знаний проводят анализ эффективности работы пользователей и выявляют какую часть рабочего времени они использовали на инсайдерские действия.

Для апробации программного комплекса были проведены экспериментальные исследования в рамках опытной эксплуатации в ООО «Региональный аттестационный центр». Задачами четырех экспериментальных исследований являлось:

1) формирование шаблона эталонной работы пользователя;
2) оценка эффективности работы пользователя;
3) выдача рекомендаций для повышения эффективности работы персонала;
4) анализ результатов экспериментальных исследований.

Были проведены 4 эксперимент.

Эксперимент 1 «Формирование шаблона и оценка эффективности работы пользователя, не нарушающего политику безопасности организации».

Пользователь должен за 8 часов рабочего времени должен выполнить 100 документов с заданным качеством «Хорошо». Перерывы на отдых должны составлять не более 2 часа. При этом не модифицировать программного и аппаратного обеспечения ИС и не использовать запрещенные операции.

Задача: проверка работоспособности разработанного программного комплекса, а также проверка достоверности оценки эффективности работы пользователя, не нарушающего политику безопасности организации.

Эксперимент 2 «Формирование шаблона и оценка эффективности группы пользователей, при условии, что отдельные пользователи нарушают политику безопасности».

Время наблюдения и требования к работе пользователей аналогичны первому эксперименту. Пользователи совершали следующие нарушения:

- User1 – установка нового программного обеспечения;
- User2 – запуск запрещенных приложений;
- User3 – замена компонентов аппаратного обеспечения;
- User4 – отсутствуют нарушения;
- User5 – отсутствуют нарушения.

Задача: оценка эффективности работы пользователей, а так же рекомендаций, которые выданы пользователю для повышения эффективности его работы.

Эксперимент 3 «Формирование шаблона и оценка эффективности группы пользователей, при условии, что они выполняют предложенные рекомендации, предложенные в эксперименте 2».

Задача: проверка достоверности оценки эффективности работы пользователей, а так же оценка влияния рекомендаций, которые выданы пользователю, на изменение качества его работы; оценка изменений в работе пользователей.

На рис. 3 приведены результаты экспериментальных исследований. Данная диаграмма отражает соответствие характеристик пользователей эталонным значениям до и после применения рекомендаций.

В результате анализа было выявлено, что пользователь 1 установил неразрешенное программное обеспечение, пользователь 2 модифицировал аппаратное обеспечение, пользователь 3 запускал запрещенные для него приложения, а пользователи 4 и 5 выполнял работу несоответствующего качества. Затем пользователям были выданы рекомендации для повышения эффективности их работы. Из приведенных данных видно, что предложенные рекомендации позволили повысить эффективность работы пользователей до заданного уровня.

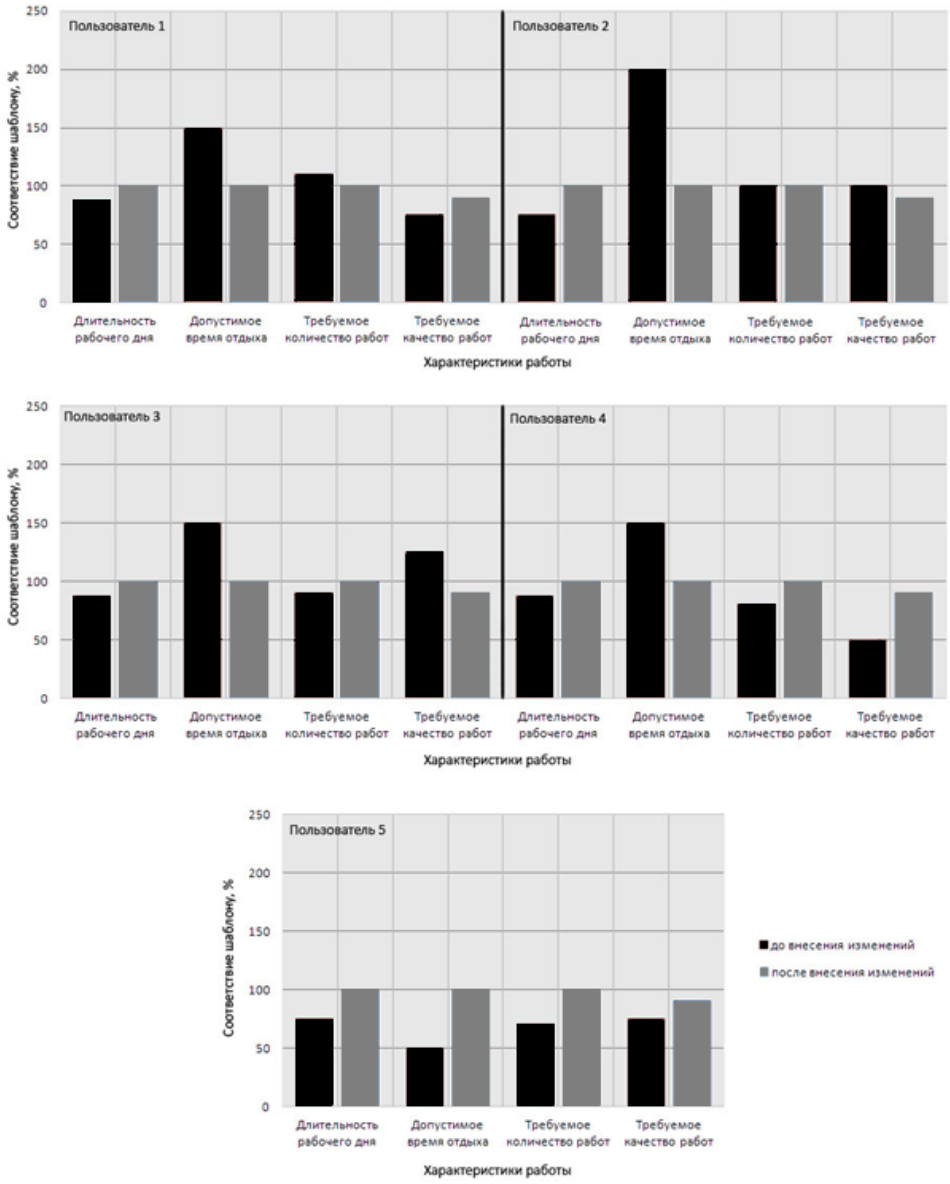


Рис. 3. Результаты экспериментов

Проведенные экспериментальные исследования показали, что программный комплекс достоверно определяет пользователей, которые нарушают установленную политику безопасности и предложенные им рекомендации позволяют повысить эффективность их работы. Эффективность работы удалось повысить на 12 %, за счет блокирования инсайдерской деятельности пользователей.

Практическая значимость заключается в том, что выявляются несанкционированные действия пользователя с данными и блокируются возможные утечки информации. Критерии, лежащие в основе оценки, позволяют каждого пользователя оценить объективно и предложить рекомендации по повышению эффективности его работы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Исследование утечек информации из компаний и госучреждений России 2012 [электронный ресурс] // InfoWatch [Офиц. сайт]. URL: http://www.infowatch.ru/analytics/reports/3073 (дата обращения 03.12.13).
2. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ [электронный ресурс] // КонсультантПлюс. URL: http://www.consultant.ru/popular/tkrf/ (дата обращения 03.12.13).
3. *Тененко М.И., Пескова О.Ю.* Анализ рисков информационной безопасности // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 49-58.
4. Методы мониторинга и обеспечения безопасности для поддержания работоспособности корпоративной сети [электронный ресурс] // SecurityLab [Офиц. сайт]. URL: http://www.securitylab.ru/analytics/301808.php (дата обращения 03.12.13).
5. *Никишова А.В.* Архитектура типовой информационной системы для задачи обнаружения атак // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 104-110.
6. *Цыбулин А.М.* Архитектура автоматизированной системы управления информационной безопасностью предприятия // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 58-64.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Цыбулин Анатолий Михайлович – Волгоградский государственный университет; e-mail: anatsybulin@yandex.ru; 400062, г. Волгоград, пр. Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; зав. кафедрой.

Свищева Марина Николаевна – e-mail: marinasvih@gmail.com; кафедра информационной безопасности; аспирантка.

Tsybulin Anatoly Mihaylovich – Volgograd State University; e-mail: anatsybulin@yandex.ru; 100, Universitetsky pr., Volgograd, 400062, Russia; phone: +78442460368; the department of informational security; head of department.

Svishcheva Marina Nikolaevna – e-mail: marinasvih@gmail.com; the department of informational security; postgraduate student.

УДК 004.089

П.М. Иванов, О.Б. Макаревич, З.В. Нагоев

АВТОМАТИЧЕСКОЕ ФОРМИРОВАНИЕ КОНТЕКСТА СИТУАЦИЙ В СИСТЕМАХ ОБВОЛАКИВАЮЩЕЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МУЛЬТИАГЕНТНЫХ КОГНИТИВНЫХ АРХИТЕКТУР*

Цель данной работы состоит в разработке метода формирования контекста текущей ситуации в системах обволакивающей безопасности на основе самоорганизации мультиагентной рекурсивной когнитивной архитектуры. Задача исследования состоит в разработке алгоритма формирования контекста текущей ситуации в распределенной мультиагентной системе принятия решений на основе ее формального описания с помощью рекурсивных детерминированных абстрактных автоматов. Предложено решение задач ситуативного анализа и синтеза интеллектуального поведения в системах обволакивающей безопасности строить на основе самоорганизующихся мультиагентных рекурсивных когнитивных архитектур. Разработана формализация таких архитектур на основе рекурсивных детерминированных абстрактных автоматов. Задача синтеза интеллектуального управления системой обволакивающей безопасности сведена к информированному поиску пути, субоптимального по критерию максимизации энергии, в дереве решений, глубина

* Работа выполнена при поддержке грантов РФФИ №№ 12-07-00744, 13-07-01002, Программы Президиума РАН «Фундаментальные проблемы модернизации полиэтнического региона в условиях роста напряженности» № 32.