УДК 004.056.53

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА ИДЕНТИФИКАЦИИ ПРОФИЛЯ ПОЛЬЗОВАТЕЛЯ В ПРОЦЕССЕ АКТИВНОГО МОНИТОРИНГА СЕТЕВЫХ РЕСУРСОВ

Цветков А.А.[1], Надеждин Е.Н.[2]

[1]*Шуйский филиал ФГБОУ ВПО «Ивановский государственный университет», г. Шуя Ивановской обл., Россия (155908, Ивановская область, г. Шуя, ул. Кооперативная, д.24), e-mail: tsvetkov.a.a@yandex.ru*
[2]*ФГАУ ГНИИ ИТТ «Информатика», г. Москва, Россия (125009, Москва, Брюсов переулок, д. 21, стр. 2),), e-mail: en-hope@ya.ru*

Разработан вычислительный алгоритм, позволяющий эффективно идентифицировать профиль активного пользователя корпоративной вычислительной сети, основанный на анализе данных, полученных в результате проведения активного мониторинга состояния сетевых ресурсов. Авторский алгоритм идентификации профиля пользователя разработан в целях выявления путей корректировки системы информационной безопасности и выявления потенциальных инсайдеров компьютерной сети в интересах своевременного предотвращения совершения возможных деструктивных действий. В статье описаны основные результаты проведенной экспериментальной работы, свидетельствующие об эффективности применения данного алгоритма при осуществлении ряда мероприятий по выявлению потенциально опасных сотрудников организации. Кроме того, в работе сформулированы общие рекомендации по реализации алгоритма идентификации профиля пользователя в процессе проведения активного мониторинга, направленные на совершенствование механизмов защиты корпоративной информации.

Ключевые слова: активный мониторинг ресурсов, корпоративная вычислительная сеть, профиль пользователя, алгоритм идентификации.

IMPLEMENTATION OF IDENTIFICATION THE USER PROFILE ALGORITHM IN THE COURSE OF THE ACTIVE MONITORING OF NETWORK RESOURCES

Tsvetkov A.A.[1], Nadezhdin E.N.[2]

[1]*Shuya branch of Ivanovo State University, Shuya, Ivanovo region, Russia (155908 Ivanovo region, Shuya, Cooperativnaya street, 24), e-mail: Tsvetkov.a.a@yandex.ru*
[2]*State Institute of Information Technologies and Telecommunications, Moscow, Russia ((125009, Moscow, Bryusov Lane, house 21, structure 2), e-mail: en-hope@ya.ru*

It is developed the computing algorithm to effectively identify a network user profile, the algorithm based on the analysis of the data obtained as a result of active monitoring of the network resources condition. The author's algorithm of the user's profile identification is designed to identify the ways to adjust the information security system and identify potential insider of the computer network in order to timely prevent the commission of potentially disruptive actions. The article describes the main results of the carried-out experimental operation which shows the effectiveness of this algorithm in the implementation of a number of measures to identify potentially dangerous employees. In addition, in the paper the general recommendations about carrying out the algorithm of the user's profile identification in the process of active monitoring are formulated, the recommendations aim to improve the mechanisms for the protection of corporate information.

Keywords: the active monitoring of resources, corporate computer network, user profile, identification algorithm.

Быстрое развитие информационной инфраструктуры проектно-конструкторских организаций потребовало адекватного усовершенствования механизмов сетевого администрирования, включая процедуры контроля сетевой активности сотрудников. В таких условиях актуальной задачей становится идентификация профиля активного пользователя корпоративной вычислительной сети (КВС). Этому способствует учащение случаев утечки информации в крупных фирмах, ведущих разработку инновационных IT-проектов и, следовательно, обладающих важными конкурентными преимуществами на рынке

информационных технологий. Как показали наши исследования [2, 4], проведение мониторинга действий пользователей может позволить вовремя идентифицировать потенциального злоумышленника и предотвратить возможные деструктивные действия.

Целью статьи является разработка вычислительного алгоритма идентификации профиля пользователя и обоснование рекомендаций по его реализации при осуществлении активного мониторинга ресурсов КВС.

Под термином «*мониторинг ресурсов сети*» понимается комплекс процедур, которые предусматривают целенаправленное автоматизированное или автоматическое прямое или косвенное дистанционное «наблюдение» за состоянием ресурсов сети в интересах своевременного обнаружения попытки или факта нарушений установленных прав доступа, других несанкционированных действий пользователей либо обнаружения иных пробелов в безопасности и обеспечивают сбор информации об изменении состояния ресурсов сети [5].

Предлагается итерационный алгоритм идентификации профиля пользователя, который формирует модель профиля активного пользователя, при этом шаг итерации выполняется через временной интервал *T*. Основной задачей алгоритма является классификация всех субъектов сети по группам опасности: безопасный, безвредный, подозрительный, опасный.

Рассмотрим математическую постановку задачи. Пусть в распределенной КВС зарегистрировано *n* пользователей и выбрано для анализа *m* критических событий. Каждой i-й критической ситуации поставлено в соответствие некоторое количество баллов b_i, характеризующее степень опасности данного события. Предположим, что априорно установлены значения K_1, K_2 и K_3 на шкале показателя *K* для разделения пользователей по группам опасности, при этом к безопасным относятся пользователи, набравшие не более K_1 баллов, от K_1+1 до K_2 баллов – безвредные, от K_2+1 до K_3 – подозрительные, более K_3 баллов – опасные. Алгоритм генерирует последовательность результатов $\{x_0, x_1, ..., x_k, ...\}$, $x_i = \{S_i^j\}_{j=1}^n (i = 0, 1, ...)$, где S^j $(j = 1, ..., n)$ называется состоянием пользователя, $\forall j = 1, ..., n$: $S^j \in \{безопасный; безвредный; подозрительный; опасный\}$, между состояниями определена операция отношения $<$. В интересах удобства формализации введём нумерацию групп пользователей: $безопасный = 0$, $безвредный = 1$, $подозрительный = 2$, $опасный = 3$. Изначально предполагается, что все пользователи относятся к категории безопасных: $S_0^j = 0$ $(j = 1, ..., n)$ и $x_0 = \{S_0^1, ..., S_0^n\}$. Значение показателя текущего состояния x_k вычисляется на основании значения предыдущего шага: $x_k = F(x_{k-1})$. Будем считать, что оператор F представляет собой совокупность функций, предназначенных для определения текущего состояния каждого пользователя:

$F = \{f^1, ..., f^n\}$, где $\forall j = 1,...,n \;\; S_k^j = f^j(S_{k-1}^j)$, $f^j = \begin{cases} \text{если } S^j > S_{k-1}^j, \text{то } S_k^j = S^j, \; T^j = 0, \\ \text{если } T^j \geq T^* \text{ и } S_{k-1}^j > 0, \text{то } S_k^j = S_{k-1}^j - 1. \end{cases}$

S^j идентифицируется путем сравнения значения $K = \sum_{i=1}^{m} b_i \cdot k_i^j$ (k_i^j – количество возникших происшествий с номером $i = 1,...,m$ при работе пользователя $j = 1,...,n$) со значениями K_1, K_2 и K_3. Здесь T^j – промежуток времени, в течение которого состояние уровня опасности j-го пользователя оставалось постоянным, T^* – фиксированное значение временного интервала, по истечении которого пользователя можно перевести в группу менее опасных при условии, что в течение этого интервала времени состояние пользователя не менялось.

Для выхода из циклической части алгоритма установим критерий сходимости – $x^* = \lim_{k \to \infty} x_k$, выбор которого производится с учётом требований политики корпоративной безопасности и специфики инфраструктуры организации. В нашем случае в качестве критерия сходимости будем использовать следующее условие, суммирующее изменения за последние s шагов.: $\sum_{l=0}^{s-1} \left| x_{k-s+l+1} - x_{k-s+l} \right| < \varepsilon$, $\left| x_{l+1} - x_l \right| = \sum_{j=1}^{n} \left| S_{l+1}^j - S_l^j \right|$, $\forall l = 0, 1, 2, ...$,

Учитывая введённые обозначения и допущения, алгоритм идентификации профиля активного пользователя может быть описан блок-схемой, представленной на рис. 1. Для предварительной оценки эффективности предложенного подхода к задаче классификации пользователей проведён вычислительный эксперимент, в ходе которого на основе имитационной модели действий пользователя подтверждена вычислительная устойчивость предложенного алгоритма и уточнены значения границ K_1, K_2 и K_3.

Апробация разработанной методики проведена на производственном предприятии города Иваново, главный офис которого располагается в Москве. Приведём дополнительные данные о технической базе натурного эксперимента. Связь между головным и региональным офисами осуществлялась с помощью защищенного VPN канала. В локальной компьютерной сети работало 20 серверов: в московском офисе фирмы – сервер сетевого мониторинга The Dude, сервер инвентаризации компьютеров в сети OCS inventory, сервер Hids OSSEC, сервер антивируса Kaspersky, контроллер домена Active Directory, почтовый сервер Postfix, сервер обмена мгновенными сообщениями Jabber, сервер телефонии WellTime, файловый сервер, прокси-сервер ISA и сервер Backup, а в Иванове – сервер базы данных 1С, два сервера приложений Citrix XenApp, сервер Kaspersky, контроллер домена Active Directory, сервер телефонии WellTime, файловый сервер, прокси-сервер ISA и сервер Backup. В Ивановском офисе организации было установлено 197 пользовательских компьютеров, а в московском – 84 рабочие станции (каждый компьютер предназначался для работы одного сотрудника).

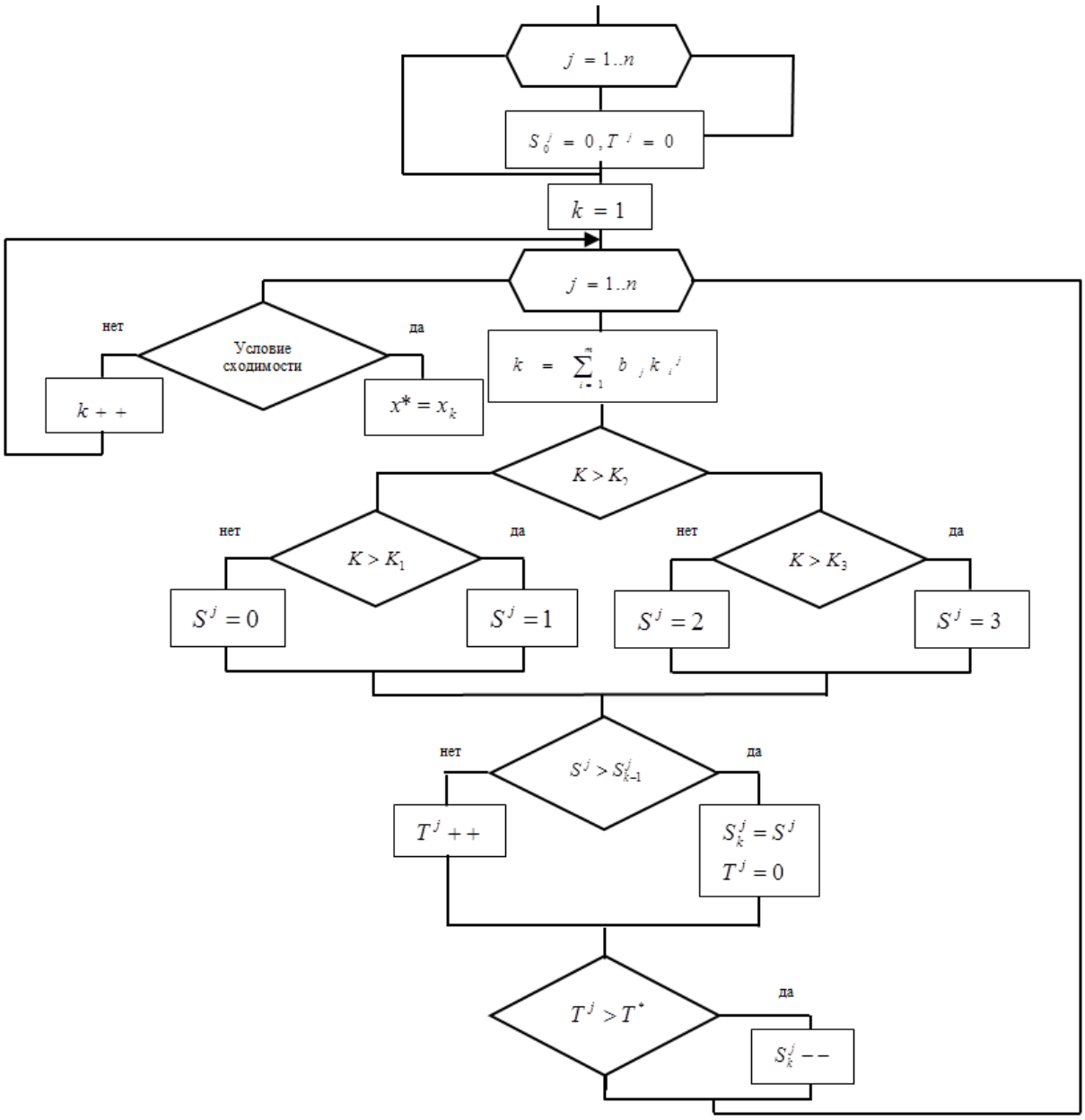

Рис. 1. **Алгоритм идентификации профиля пользователя**

Компьютеры КВС были объединены в домен, согласно ролевой модели управления доступом настроена групповая политика доступа к файлам и Интернет-ресурсам. Прокси-сервер содержал список запрещенных для посещения сотрудниками организации сайтов, на файловом сервере был настроен аудит доступа к файлам и папкам. В период с 10.01.2013г. по 30.12.2013г. нами были собраны логи мониторинга. С прокси-сервера считывались логи сетевой активности пользователей, содержащие в себе сведения о доступе к Интернет-ресурсам. С контроллера домена была получена информация о неудачных попытках авторизации и о сессиях пользователей. Файловый сервер и сервер баз данных предоставляли логи аудита доступа к файлам и папкам. Отчеты об обнаруженных угрозах в сети были считаны с сервера администрирования антивирусов. Промежуток времени просмотра данных мониторинга T был установлен равным одному дню, ежедневно, согласно

алгоритму, уточнялось расположение пользователей по группам опасности. В качестве отслеживаемых критических событий были выбраны следующие: ошибка авторизации (7 баллов опасности), отказ в доступе к сетевым файлам и папкам (7 баллов), удаление общих файлов (20 баллов), отказ в доступе к запрещенным веб-ресурсам (5 баллов), посещение нежелательных сайтов (3 балла), переписка с конкурентами (70 баллов). Для составления таблицы критериев установлены коэффициенты: K_1=10, K_2=25, K_3 =70. Промежуток времени T^* установлен равным двум неделям для всех пользователей, не отнесенных к группе опасных. Если пользователь попадал в группу «опасный», то он подвергался тщательной проверке с привлечением располагаемого административного ресурса службы безопасности.

В результате проведения эксперимента было выявлено 5681 ошибок авторизации, 1729 попыток нарушения прав доступа к общим файлам, 741 удалений файлов, 22230 попыток доступа к запрещенным веб-ресурсам, 68419 посещений нежелательных сайтов. Достаточно большое количество ошибок авторизации можно объяснить несовершенством требований парольной политики, согласно которой установлены жесткие требования к создаваемым паролям, что существенно усложняло процесс их запоминания и практического применения. Значительное количество попыток нарушения прав доступа во многом объяснимо человеческим фактором, вследствие которого сотрудники проявляют «нездоровый интерес» к чужим документам. Посещения сотрудниками нежелательных сайтов и попытки доступа к запрещенным веб-ресурсам могли возникнуть из-за низкого контроля руководства за регламентом рабочего времени и имеющимися возможностями его использования в личных целях. Все случаи несанкционированного удаления рабочих файлов изучались в индивидуальном порядке в целях определения обоснованности таких действий, которые в большинстве случаев идентифицировались как безопасные.

С использованием авторских алгоритмов и рекомендаций в ходе эксперимента было идентифицировано 9 опасных пользователей, требующих более пристального наблюдения за своей деятельностью в КВС. В качестве подозрительных определено 144 пользователя, 123 пользователя проявили себя как безвредные и 5 пользователей сохранили статус безопасных. В ходе специализированной проверки и анализа сетевой активности за 2013 год в организации было выявлено четверо сотрудников-инсайдеров. Приведённые выше данные свидетельствуют о результативности разработанных методик и алгоритмов. На рис. 2 представлен график распределения количества пользователей КВС по группам опасности.

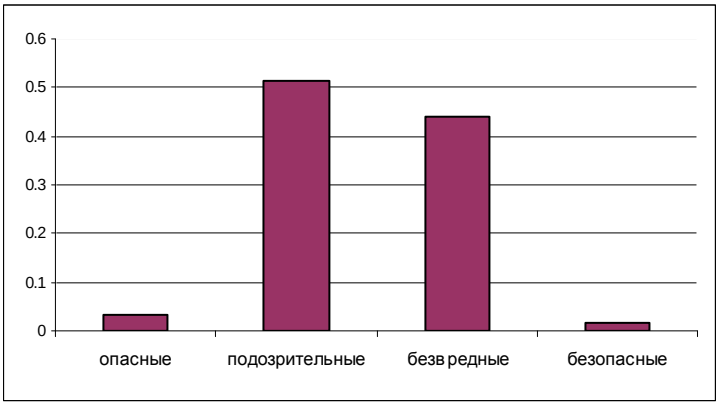

Рис. 2. **Распределение количества пользователей по группам опасности**

Проведенное исследование позволило сформулировать следующие рекомендации по организации активного мониторинга для целей идентификации профиля пользователя:

1. Для централизованного сбора и обработки информации о действиях пользователей в КВС целесообразно установить сервер мониторинга, работающий в круглосуточном режиме. Для оптимизации плана размещения инструментов мониторинга при выборе местоположения данного сервера необходимо руководствоваться двумя критериями: а) минимальной удалённостью сервера от основных устройств, мониторинг которых необходимо производить; б) ёмкостью интернет-канала между сервером мониторинга и станциями с клиентами, которые будут к нему подключаться. Синтез рациональной программы активного мониторинга компонентов КВС может быть сведен к постановке и решению известной комбинаторной задачи дискретной оптимизации – задачи коммивояжера.

2. Целесообразно одновременное проведение двух параллельных процессов – общего и событийного мониторинга. Общий мониторинг должен проводиться с некоторой периодичностью, определяемой параметрами сети, и включать следующие последовательные действия: тестирование физической доступности оборудования; проверка работоспособности критических служб и сервисов, запущенных в сети; проверка состояния всех компьютеров в сети и состояния баз данных. Событийный мониторинг проводится при появлении определенных событий, возникающих как при работе пользователей, так и сетевого оборудования и внешних систем.

3. Согласно особенностям работы фирмы, необходимо определить, какие сведения требуются для адекватной идентификации профиля пользователя сети, а именно: какие логи мониторинга должны быть собраны. Как правило, имеет смысл считывать логи сетевой активности пользователей с прокси-сервера, информацию о неудачных попытках авторизации с контроллера домена, логи аудита доступа к файлам и папкам с файлового

сервера и сервера баз данных, а также отчеты об обнаруженных угрозах в сети с сервера администрирования антивирусов.

4. Для анализа данных собираемые сведения удобно аккумулировать в базе данных, состоящей из шести модулей (таблиц) (см. рис. 3): таблица объектов (object), таблица субъектов (subject), таблица групп (risk_groups), таблица событий (dig_events), таблица происшествий (events) и таблица статистики (statistics).

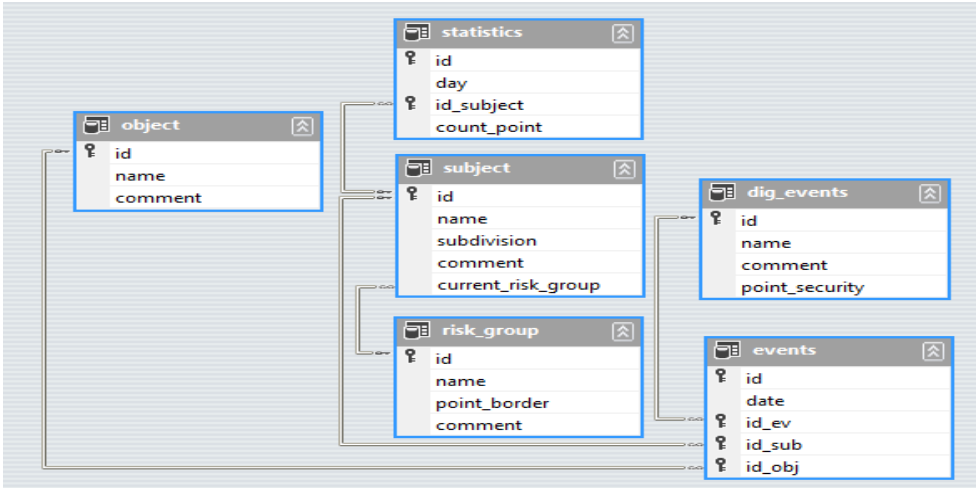

Рис. 3. **Структура базы данных мониторинга (базовый вариант)**

Таблица object предназначена для хранения сведений об объектах мониторинга, на которых могут быть зафиксированы инциденты, таблица subject содержит полную информацию о субъектах сети – имя, подразделение, которое определяет уровень прав доступа данного пользователя, а также информацию о текущем состоянии пользователя в отношении его отнесения к одной из групп опасности (поле current_risk_group), которая соответствует номеру группы опасности в справочной таблице групп risk_groups. Таблица dig_events предназначена для хранения списка критических событий с указанием количества баллов опасности, присваиваемых за возникновение такого события. В таблицу events заносятся сведения обо всех произошедших критических событиях, характеризующихся датой с указанием точного времени, номером события из списка событий в таблице dig_events, номером субъекта (из таблицы subject) и номером объекта (из таблицы object). Таблица statistics несет вспомогательную функцию, она содержит статистику об изменении состояний пользователей, которая требуется в процессе применения алгоритма идентификации профиля пользователя. При этом для информационно-аналитической поддержки мониторинга необходимы дополнительные программные средства, осуществляющие накопление и систематизацию результатов наблюдений за активностью пользователей.

5. С целью оценки эффективности программы мониторинга необходимо установить количественные характеристики свойств мониторинга применительно к определённым условиям его проведения, так называемые показатели эффективности или показатели

качества. На наш взгляд, ключевыми показателями являются скорость проведения активного мониторинга, качество собранной информации и ресурсозатратность. Посредством применения метода экспертных оценок по выделенным показателям необходимо определить качество проведенного мониторинга сети и, как следствие, уровень достоверности сделанных на его основе выводов.

Таким образом, в ходе наших исследований сформулирована задача идентификации профиля активного пользователя на основе данных мониторинга сети, обоснован итерационный алгоритм классификации пользователей по степени опасности, описаны основные результаты его практического применения, а также определены общие рекомендации по проведению активного мониторинга в целях выявления потенциальных инсайдеров.

Список литературы

1. Еремеев В. Б. Разработка математического и программного обеспечения активного мониторинга вычислительной сети // V Всероссийская школа-семинар молодых ученых «Управление большими системами»: Сборник трудов. – Т.2. – Липецк: ЛГТУ, 2008. – С.33-39.
2. Надеждин Е. Н. Методы моделирования и оптимизации интегрированных систем управления организационно-технологическими процессами в образовании: монография / Е.Н. Надеждин, Е.Е. Смирнова. – Тула: Изд-во ТулГУ, 2013. – 250 с.
3. Надеждин Е.Н. Проблемные вопросы управления рисками информационной безопасности в сфере образования // Научный журнал «Научный поиск». Специальный выпуск: Материалы V научной конференции «Шуйская сессия студентов, аспирантов, молодых учёных», 2012. – Научный поиск. - №2,6. – С.50-56.
4. Цветков А. А. Особенности управления механизмами защиты информации на основе данных активного мониторинга состояния защищённости ресурсов // Наука, образование, общество: проблемы и перспективы развития: сб. науч. тр. по мат-лам Междунар. науч.-практ. конф. 28 февраля 2014 г.: в 12 частях. Часть 11; М-во обр. и науки РФ. – Тамбов: Изд-во ТРОО «Бизнес-наука-общество», 2014. – С. 154-156.
5. Цветков А. А. Модель активного мониторинга пользователей корпоративной информационной сети вуза // Информационная среда образования и науки [Электронный ресурс]. – М.: ИИО РАО, 2012. Вып. 9. – URL: http://www.iiorao.ru/iio/pages/izdat/ison/publication/ison_2012/num_9_2012/Cvetkov.pdf (дата обращения: 30.07.2014г.).

Рецензенты:

Куракин Д.В., д.т.н., профессор, советник директора ФГАУ ГНИИ ИТТ «Информатика», г.Москва;

Неустроев С.С., д.э.н., первый заместитель директора ФГАУ ГНИИ ИТТ «Информатика» г.Москва.