УДК 004.056.52

МОДУЛЬ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ КАК ДОПОЛНИТЕЛЬНЫЙ ЭЛЕМЕНТ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ТОРГОВОЙ ОРГАНИЗАЦИИ

Дубровин А.С.[1], Губин И.А.[2]

[1] ФКОУ ВПО «Воронежский институт Федеральной службы исполнения наказаний», Воронеж, Россия (394076, Воронеж, ул. Иркутская, 1а), e-mail:asd_kiziltash@mail.ru
[2] ФГБОУ ВПО «Воронежский государственный педагогический университет», Воронеж, Россия (394043, Воронеж, ул. Ленина, 86), e-mail:gubin24@yandex.ru

Предлагается решение задачи по оперативному разделению доступа к информации сотрудников торговой организации при инициации режима коммерческой тайны (РКТ). Выделены определенные свойства рассматриваемой автоматизированной информационной системы торговой организации. Согласно нормативным актам, дается описание режима коммерческой тайны и информации, составляющей коммерческую тайну. Частично раскрывается суть эталонной модели защищённой автоматизированной системы (ЭМЗАС). Предлагается использование менеджера ресурсов, расположенного на восьмом уровне ЭМЗАС, в качестве архитектурной основы разделения доступа к конфиденциальной информации. Сервис контроля целостности информации (СКЦИ) предлагается рассматривать не только как элемент организационно-технологического управления автоматизированной системы, но и как эффективный инструмент контроля доступа к информационным ресурсам. В публикации представлена схема и дается описание функционирования СКЦИ при введении РКТ. Результатом исследования является эффективная модель использования ресурсов СКЦИ для решения задачи по разделению привилегий доступа.

Ключевые слова: автоматизированная информационная система, дискреционный доступ, защита информации, коммерческая тайна, менеджер ресурсов, контроль целостности, торговая организация, эталонная модель защищенной автоматизированной системы.

MODULE TRADE SECRET AS AN ADDITIONAL ELEMENT OF INFORMATION PROTECTION SYSTEMS TRADE ORGANIZATION

Dubrovin A.S.[1], Gubin I.A.[2]

[1] Voronezh Institute of the Russian Federal Penitentiary Service, Voronezh, Russia (394076, Voronezh, street Irkutskaya, 1a), e-mail: asd_kiziltash@mail.ru
[2] Voronezh State Pedagogical University, Voronezh, Russia (394043, Voronezh, street Lenina, 86), e-mail: gubin24@yandex.ru

Offer a solution to the problem of the operational separation of access to information by the dealer at the initiation of a commercial secret (ICS). Allocated certain properties considered an automated information system trade organization. According to regulations, describes the regime of trade secrets and information that falls under this concept. Partially reveals the essence of the standard model secure automated system (SMSAS). Proposes the use of a resource manager, located on the eighth level SMSAS as architectural framework separation of classified information. Service integrity monitoring information (SIMI) proposed to consider not only as an element of organizational and technological management of automatedsystem, but also as an effective tool for controlling access to information resources. The publication is a diagram and a description of the functioning of the introduction SIMIICS. The result of this study is to model the effective use of resources SIMI to the task of separation of access privileges.

Keywords: automated information system, discretionary access, data protection, trade secrets, the resource manager, integrity control, trade organization, a reference model for a secure automated system.

Торговая организация (ТО) – организация различных организационно-правовых форм, осуществляющая торговую деятельность, включая необходимые средства и работников с распределением ответственности, полномочий и взаимоотношений (ГОСТ 51303-2013).

Автоматизированная информационная система (АИС) – это система, состоящая из персонала и комплекса средств автоматизации его деятельности, необходимого для выполнения его функций при помощи информационных технологий (ГОСТ 34.003-90).

Для ТО АИС является основой деятельности, так как включает в себя контроль над финансовыми потоками, товарными запасами, документами. В силу развития конкуренции и увеличения угрозы несанкционированного доступа к данным, руководство ТО уделяет особое внимание понятию «Коммерческая тайна». В соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» представим определения:

Коммерческая тайна (КТ) – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

Доступ к информации, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Обладателем информации, составляющей КТ в рассматриваемой ТО, является орган правления. Работники организации, получившие доступ к КТ, обязаны: выполнять установленный в организации режим КТ, строго хранить известную им КТ, пресекать действия других лиц, которые могут привести к разглашению тайны. При введении режима коммерческой тайны (РКТ) в рассматриваемой ТО, рекомендуется ограничить доступ к надлежащим информационным массивам до соответствующего распоряжения.

Цель исследования

1. Учитывая особенности и специфику АИСТО предполагается разработать механизм оперативного разделения доступа к критически важной информации, представляющей коммерческую тайну. Введение режима коммерческой тайны реализовать в составе механизма функционирования сервиса контроля целостности информации (СКЦИ), максимизирующего защищённость информации при обеспечении достаточной оперативности выполнения функциональных задач АИСТО.

Материал и методы исследования

Материал исследования основан на использовании литературных источников, представленных в конце данной статьи. Общей методологической основой проведенного исследования является системно-концептуальный подход.

Результаты исследования и их обсуждение

В соответствии с [1], всегда присутствует угроза несанкционированного доступа и потери данных за счет несовершенности структуры самой АИС. В связи с этим целесообразно применять концепцию эталонной модели защищенной автоматизированной системы (ЭМЗАС).

Согласно [4], все многообразие угроз безопасности АИС организации можно представить в виде целой связки ключей и отмычек, а систему защиты информации от несанкционированного доступа (СЗИ НСД) организации как сейф, в котором содержатся данные. Можно подобрать ключ – получить пароль и доступ к данным. Если умело использовать отмычку, то получиться открыть сейф, взломав пароль.

Недостатки стандартных моделей были устранены путём разработки нового математического аппарата моделирования СЗИ НСД – ЭМЗАС. Необходимо все процессы доступа к ресурсам распределить по уровням эталонной модели, в итоге получим защищенную модель АИС организации с минимальным уровнем уязвимости. Рассмотрим восьмой уровень ЭМЗАС, который называется «Менеджерский». Он определяет доступ прикладного компонента сервера АИС, авторизованного некоторым образом, к менеджерам ресурсов данного сервера.

Предполагается, что в общем случае информация, располагающаяся на данном сервере, может находиться под управлением различных менеджеров ресурсов, поэтому на данном уровне уместнее всего расположить субъекты полного разграничения данных всего сервера. Субъект менеджера ресурсов «Общие данные» и субъект менеджера ресурсов «Специализированные данные» будут разграничивать информацию на условно допустимую для разглашения и максимально неприемлемую для обнародования (конфиденциальную – используемую только руководством) (рис. 1).

Разработаем основные положения, обуславливающие функционирование АИСТО в РКТ:

1. Режим коммерческой тайны инициируется органом правления, и снятие РКТ так же возможно только с его постановления. Служащие, занимающие высокопоставленные и руководящие должности, после инициализации РКТ не допускаются к информации, находящейся под управлением менеджера ресурсов «Специализированные данные».

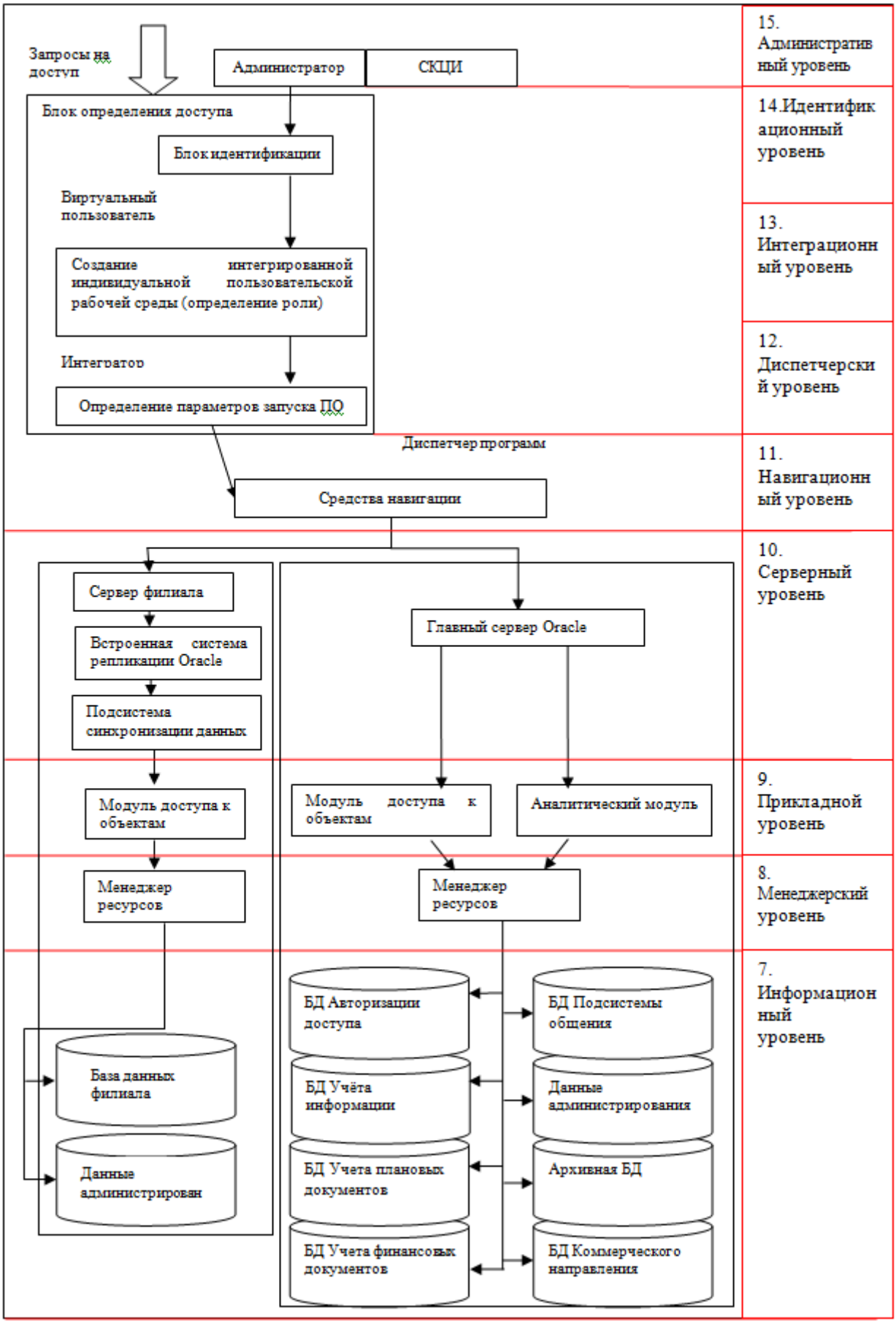

Рис. 1. «Распределение элементов АИСТО по уровням ЭМЗАС»

2. Режим РКТ устанавливается непосредственно администратором АИС при управлении сервисом контроля целостности информации (СКЦИ). Дальнейшее поддержание РКТ будет осуществляться СКЦИ. Выбор СКЦИ в качестве управляющего механизма вполне оправдан, так как процесс проверки информации на целостность неразрывно связан с дискреционными доступами.

3. Доступ к информационным ресурсам ограничивается только использованием совокупности баз данных «Общие данные». Доступ к конфиденциальной информации осуществляется только по мандату органа правления.

Достаточно подробную информацию о СКЦИ можно получить из [2]. Кратко опишем данный механизм организационно-технического управления.

Контроль целостности объекта представляет собой контроль его неизменности [5]. При этом проверяется полное тождество контролируемого объекта и образца (объекта, хранящего исходное состояние контролируемого объекта, которое принимается за эталонное), что обеспечивает полностью достоверный контроль, но использует максимум ресурсов.

Принятие решения осуществляется на основе комплексной оценки качества функционирования СКЦИ как объекта управления с учетом результатов его контроля, реализующего функцию обратной связи управления, для обеспечения и поддержания разумного компромисса между уровнем целостности информации в АИСТО и её эффективностью функционирования по целевому назначению.

СКЦИ представляет собой совокупность различных модулей (рис. 2).

Административный модуль дает возможность руководить работой и осуществлять настройку СКЦИ. Посредством него администратор вводит необходимые для функционирования параметры и осуществляет анализ эффективности работы СКЦИ по выходным данным.

Подсистема контроля качества функционирования обеспечивает расчет текущих важных показателей, таких как скорость функционирования, и итоговые значения объема информации, проверенного на неизменность, и времени, затраченного на это.

Подсистема принятия решений вычисляет, на основании полученных параметров от подсистемы контроля и от администратора, оптимальное значение важного параметра динамической эффективности Y_{opt}, значение которого и определяет эффективный характер функционирования СКЦИ.

Подсистема управляющих воздействий, учитывая ограничивающий параметр $K_{\max i}$, рассчитывает случайным образом параметр K_i, отвечающий за полноту проверки на каждом уровне ЭМЗАС.

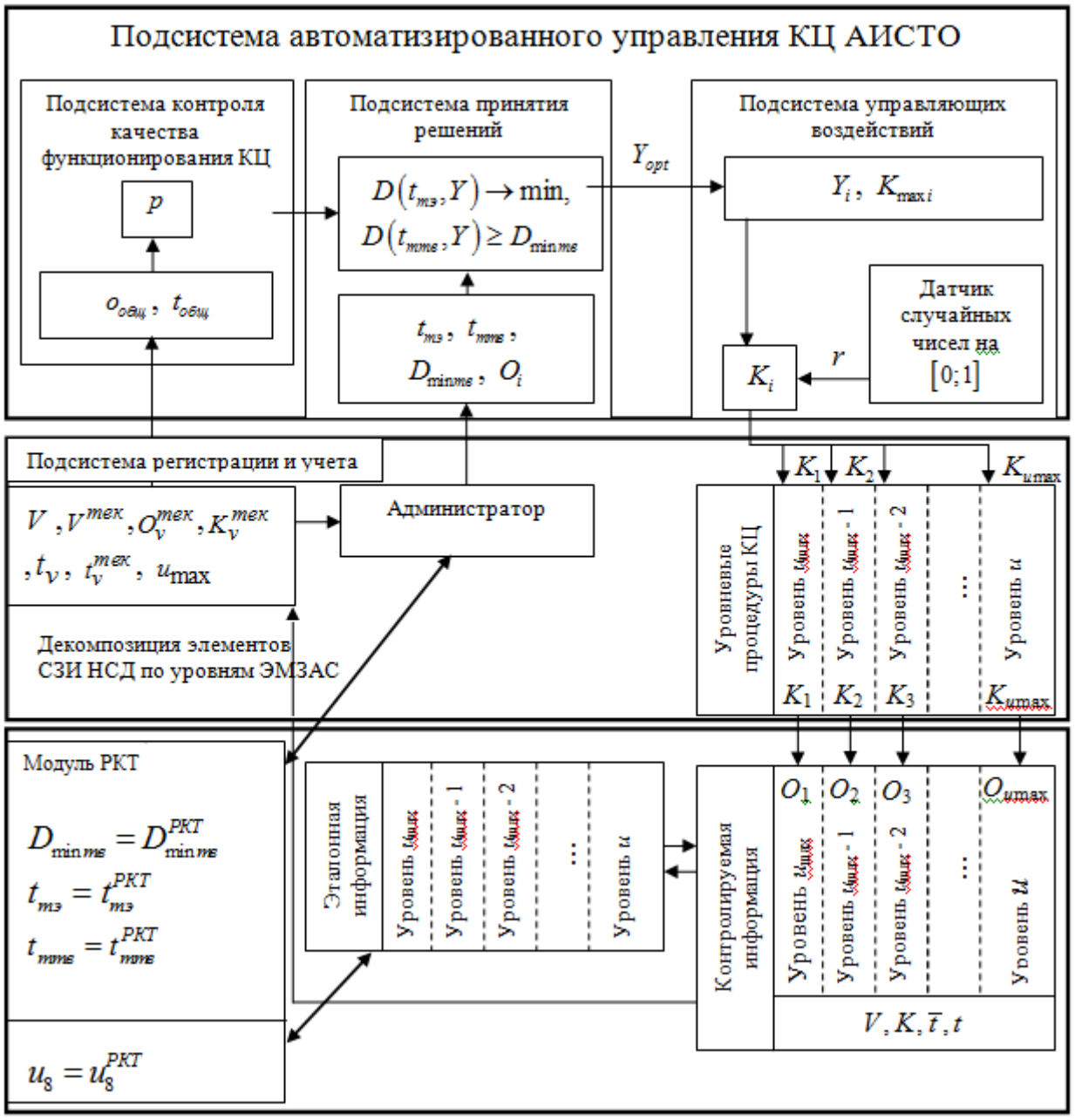

Рис. 2. «Структурная схема управления СКЦИ АИСТО»

Основной модуль СКЦИ рассчитывает количество информации для проведения процесса проверки и сверяет с эталонным значением. Заметим, что данные касательно проверяемой на целостность информации при текущем запуске СКЦИ регистрируются *подсистемой регистрации и учета.*

Модуль РКТ управляется администратором. При инициализации РКТ происходит подмена в реестре эталонных значений: значения восьмого уровня ЭМЗАС, который называется «Менеджерский», заменяются аналогичными, за исключением содержания совокупности «Специализированные данные». Данная замена исключает возможность получить доступ к данной совокупности, так как любой дискреционный доступ к объявленным данным не пройдет проверку СКЦИ. Для возможности использования

защищенных данных предусмотрена процедура по замене эталонной информации специальным значением, дающим возможность определенным авторизациям пользоваться совокупностью «Специализированные данные». Процедура предлагает администратору на установленный срок или до окончания РКТ указать номера легальных авторизаций, для которых доступ будет открыт.

При инициализации РКТ происходит автоматическая замена установленных администратором параметров функционирования СКЦИ: $D_{\min тв} = D_{\min тв}^{РКТ}$, $t_{тэ} = t_{тэ}^{РКТ}$, $t_{mmв} = t_{mmв}^{РКТ}$. Данная процедура призвана увеличить объем информации, контролируемой на неизменность, что увеличит степень защиты от НСД. Параметры функционирования СКЦИ при РКТ должны быть заранее определены и не оказывать существенного влияния на производительность АИС. Заметим, что изменение только вводимых параметров, а не конечных, рассчитываемых СКЦИ в автоматическом режиме, лучшим образом влияет на эффективность функционирования АИСТО.

Заключение

Рассмотренный метод использования СКЦИ в качестве инструмента разграничения доступа предполагает:

1. Экономию вычислительных ресурсов. Дополнительные операции, связанные с введением РКТ, в исполнении СКЦИ окажут незначительное влияние на оценку производительности АИСТО.

2. Уменьшение трудозатрат на реализацию СЗИ НСД. На стадии проектирования СКЦИ применение данной методологии позволит решить многие задачи предоставления полномочий доступа.

3. Анализ и усовершенствование архитектуры СКЦИ, что впоследствии позволит увеличить эффективность данного элемента организационно-технологического управления автоматизированной системы.

Список литературы

1. Губин И.А., Дубровин А.С., Мирошина И.Е. Стохастическое варьирование коэффициентом контроля целостности в эталонной автоматизированной системе обработки данных // Вестник Воронежского института ФСИН России.2012. № 1. С.75-78.

2. Губин И.А.О контроле целостности информационных процессов автоматизированной системы торговой организации // Научные ведомости Белгородского государственного университета.2014. № 22 (165). Вып. 28/1. С. 179-185.

3. Дубровин А.С. Модели и методы комплексного обеспечения надежности информационных процессов в системах критического применения: дис. … д-ра техн. наук. Воронеж, 2011. 433 с.
4. Сумин В.И., Дубровин А.С., Сумин А.И., Губин И.А. Внедрение режимакоммерческой тайны в проектируемую систему защиты информации // Качество в производственных и социально-экономических системах: материалы 2-ой Международной научно-технической конференции. Курск: Юго-Зап. гос. ун-т, 2014. Т. 2. С. 115-118.
5. Сумин В.И., Ильницкий А.В. Построение модели рационального выбора систем принятия решения // Научные ведомости Белгородского государственного университета. 2012. № 19 (138). Вып. 24/1. С. 158-160.

Рецензенты:

Белокуров С.В., д.т.н., доцент, начальник кафедры математики и естественнонаучных дисциплин ФКОУ ВПО Воронежский институт ФСИН России, г. Воронеж;

Душкин А.В., д.т.н., доцент, начальник кафедры управления и информационно-технического обеспечения ФКОУ ВПО Воронежский институт ФСИН России, г. Воронеж.