DOI: 10.34020/2073-6495-2020-3-231-240
УДК 001.8 + 004.8

СЕТЕВАЯ ЭКСПЕРТНО-АНАЛИТИЧЕСКАЯ ПЛАТФОРМА КАК ИНСТРУМЕНТАЛЬНОЕ СРЕДСТВО ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В РАСПРЕДЕЛЕННОЙ СРЕДЕ

Тобин Д.С.
Санкт-Петербургский Федеральный исследовательский центр РАН,
Академия военных наук Российской Федерации
E-mail: gniiivm-g@yandex.ru

В статье изложены базовые положения организации сетевой экспертно-аналитической платформы поддержки принятия решений как инструментального средства поддержки принятия бизнес-решений и управленческих решений в распределенной среде. Показано, что предлагаемые положения являются универсальными и могут быть использованы при разработке автоматизированных рабочих мест любого должностного лица, принимающего бизнес-решения и управленческие решения по результатам экспертизы их вариантов в распределенной среде с учетом требований обеспечения защиты конфиденциальной информации.

Ключевые слова: поддержка принятия решений, сетевая экспертиза, инструментальная платформа, программно-аппаратный комплекс, распределенная сетевая среда.

NETWORK EXPERT-ANALYTICAL PLATFORM AS A TOOL DECISION SUPPORT DISTRIBUTED ENVIRONMENTS

Tobin D.S.
St. Petersburg Federal Research Center of the Russian Academy of Sciences,
Academy of Military Sciences of the Russian Federation
E-mail: gniiivm-g@yandex.ru

The article outlines the basic principles of organizing a network of expert and analytical decision support platform as a tool for supporting business decision making in a distributed environment. It is shown that the proposed provisions are universal and can be used in the development of automated workplaces of any official making business decisions and managerial decisions based on the results of an examination of their options in a distributed environment, taking into account the requirements for protecting confidential information.

Keywords: decision support, network expertise, tool platform, hardware and software complex, distributed network environment.

Введение. Приоритетным направлением в сфере обеспечения экономической безопасности страны является реализация технологий поддержки принятия оптимальных управленческих и бизнес-решений должностными лицами органов государственного управления [6, 8, 10]. Решение таких задач в настоящем и будущем требует применения специальных информационных технологий, обеспечивающих привлечение к поддержке принятия решений экспертов с помощью специализированных средств функционирования экспертных сообществ в распределенной сетевой среде [1, 2].

Анализ накопленного опыта убедительно свидетельствует о том, что современные информационно-аналитические технологии позволяют создать распределенную сетевую экспертно-аналитическую платформу (СЭАП) поддержки принятия решений, удовлетворяющую требованиям к системам поддержки принятия решений оптимальных управленческих и бизнес-решений должностными лицами органов государственного управления.

Основная часть. СЭАП является инструментальным сетевым средством поддержки принятия решения руководителей в органах государственного управления, которое объединит и обеспечит функционирование экспертных сообществ в распределенной сетевой среде для проведения комплексной экспертизы вариантов решений на всех стадиях их разработки и реализации [3]. Создание СЭАП, отвечающих целям и задачам поддержки деятельности сетевого экспертно-аналитического сообщества органов государственного управления, представляет собой сложный процесс, включающий этапы формирования концепции, проектирования, разработки, внедрения и сопровождения.

СЭАП предоставляет организаторам экспертизы возможность формирования реестра экспертов, выбора метода анализа проекта, выбора метода организации и проведения экспертизы, анализа экспертных оценок, обеспечивает необходимую компьютерную поддержку в проведении экспертного исследования и предназначена для подготовки и проведения экспертизы вариантов решений.

Организация и проведение экспертизы вариантов решений с участием лиц, принимающих решения, предполагают [2, 3, 5] реализацию таких этапов:

– непрерывный сбор информации, ее обработка и накопление;

– анализ собранной информации, моделирование и расчет необходимых показателей;

– принятие управленческих решений;

– отработка документов планируемых мероприятий по реализации принятого решения;

– доведение решения до подчиненных;

– реализация принятого решения;

– контроль за ходом реализации решения;

– учет и анализ изменений состояния подчиненных подразделений вследствие реализации принятого решения;

– регулирование отклонений (приведение системы в соответствие установленным требованиям).

Реализацией этих функций является выполнение ряда технологических операций в рамках соответствующих процедур. Очевидно, что выполнение ряда однотипных операций в составе разных процедур целесообразно лишь при условиях изменения входных данных для рассматриваемой операции. Использование результатов выполнения однотипной операции с неизменными исходными данными, учитываемыми при выполнении различных процедур, является одним из путей оптимизации деятельности органов государственного управления и направлением применения новых информационных технологий [4, 9, 11].

С помощью СЭАП обеспечивается возможность автоматизации процессов определения компетенций экспертов, подбор экспертов для проек-

та, ведение базы данных экспертов, формирование групп экспертов в заданной предметной области, формирование по запросу экспертных пулов из базы данных экспертов для проведения сетевой экспертизы, анализировать возможность применения основных методик проведения сетевых экспертиз, проводить сетевую экспертизу вариантов решений, подготовку аналитических данных для формирования вариантов решений, формирования отчетной документации по проведенной экспертизе.

Для начала функционирования СЭАП необходимо сформировать реестр экспертов с возможностью привлечения их различных предметных областей и сфер деятельности. Анализ сфер деятельности российских экспертных сообществ, таких как силовые структуры, бизнес, наука, образование, органы государственного и муниципального управления, показал, что сетевые экспертные сообщества в России стали появляться с 2001 г.

В настоящее время создан и ведется Федеральным государственным бюджетным научным учреждением «Научно-исследовательский институт – Республиканский исследовательский научно-консультационный центр экспертизы» (ФГБНУ НИИ РИНКЦЭ) федеральный реестр экспертов в научно-технической сфере. В реестре эксперты классифицируются по основным приоритетным областям исследований.

На просторах сети «Интернет» активно создаются площадки для формирования баз экспертов по различным областям. На них любой заинтересованный может найти как талантливого рекрутера, который поможет найти нужного эксперта самой узкой специализации, так и самостоятельно выбрать понравившегося эксперта.

В 2018 г. реестр экспертов, сформированный Главным управлением научно-исследовательской деятельности и технологического обеспечения передовых технологий (инновационных исследований) Минобороны России, объединил свыше 250 организаций и более 2600 независимых экспертов. Кроме того, на основе организованного взаимодействия и заключенного соглашения о сотрудничестве с ФГБНУ НИИ РИНКЦЭ появилась возможность привлечения к проведению экспертизы вариантов решений в интересах Минобороны России около 5000 специалистов из Федерального реестра экспертов в научно-технической сфере.

Для развития национального экспертного сообщества требуется, в частности, работа по выстраиванию единой коммуникационной экспертной площадки проведения сетевой экспертизы (СЭ) вариантов решений. С этой целью на СЭАП экспертам необходимо организовать удаленный доступ к исходной информации объекта экспертизы. Перечень объектов, подлежащих обязательной научной и научно-технической экспертизе определяется в соответствии с требованиями [7].

В СЭАП должна быть обеспечена возможность экспертизы программных и инновационных проектов (в том числе междисциплинарных и межведомственных), планируемых к реализации и реализуемых в интересах обеспечения обороны и безопасности страны. Программно-технологическим решением этого вопроса являются технологии виртуализации и контейнеризации, которые дают возможность пользователям СЭАП получать доступ к анализируемому программному обеспечению с любого клиентского устройства в тот момент времени и к тому набору услуг и задач, когда им

это необходимо, без необходимости взаимодействия с разработчиком (см. рисунок).

Предлагаемая архитектура СЭАП предполагает использование:

программного обеспечения с открытым исходным кодом, такого как Kubernetes, Docker, PostgreSQL, технологию блокчейн, а также используемое в ВС VMware ESXi;

существующей инфраструктуры ЗСПД;

гарантированного уровня защиты информации;

одновременной работы с различными ее модулями и компонентами большого количества пользователей.

Предлагаемое решение состоит из следующих основных компонентов: клиент СЭАП на АРМ пользователя, диспетчер подключений (ДП), управляющий модуля (УМ), агент СЭАП внутри виртуального рабочего стола (см. рисунок).

На АРМ пользователя СЭАП устанавливается клиентское ПО, которое представляет графический интерфейс взаимодействия эксперта с инфраструктурой СЭАП. Агент СЭАП на АРМ пользователя занимается настройкой и запуском протокола доставки рабочего стола. Клиент СЭАП работает с ДП по двум каналам: управляющему (авторизация, запрос списка рабочих столов, запрос на подключение к рабочему столу и т.д.) и каналу протокола доставки рабочего стола.

Модуль управления подключениями (МУП) к серверам состоит из двух частей: диспетчера подключений и управляющего модуля.

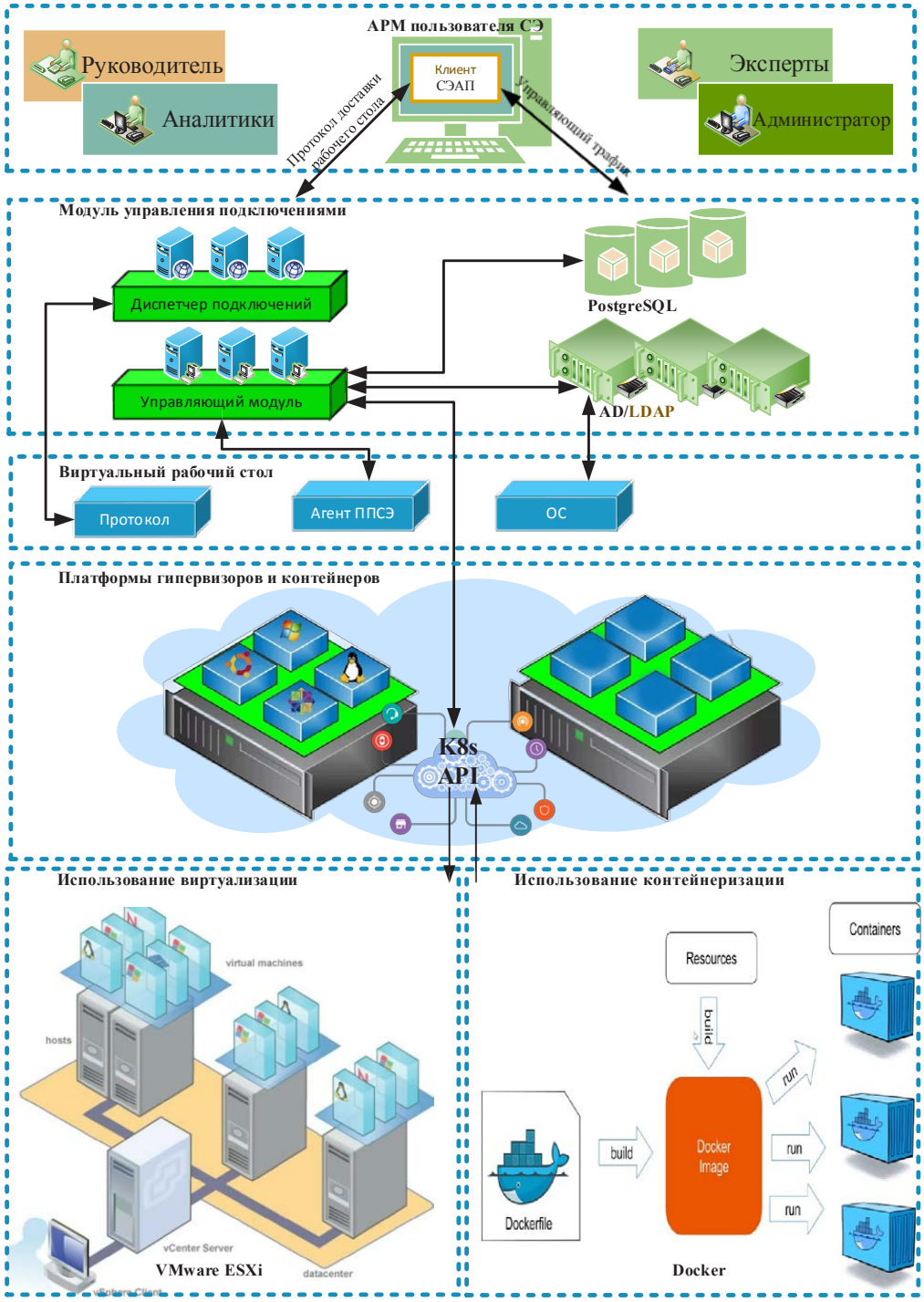
ДП – компонент, терминирующий на себе подключения пользователей. Это прокси, который передает управляющий трафик УМ, а трафик протокола доставки рабочего стола в виртуальный рабочий стол.

УМ служит для авторизации АРМ пользователей. После получения от пользователя СЭАП через ДП УМ проверяет, разрешено ли этому АРМ подключение. Если АРМ отсутствует в базе, то оно будет занесено в базу со статусом «ожидает разрешения», после чего администратор безопасности должен принять решение на подключение или блокировку этого АРМ. При выявлении атаки или перебора паролей пользователем, система блокирует АРМ потенциально опасного пользователя. Для работы с пользователями приоритетно использование LDAP/Kerberos – каталога (ОС Astra Linux) либо Active directory (ОС Microsoft Windows), где для групп, в которые они входят, назначаются списки доступных рабочих столов с предустановленным ОПО и СПО с возможностью получения доступа к анализируемому программному обеспеченью.

Объединяющим объектом этих систем является пул ресурсов VMware и Docker – логический сегмент ресурсов, в рамках которых выделены CPU, RAM и дисковая емкость. Пулы рабочих столов живут в рамках данных объектов – пулов ресурсов.

На ДП настраивается политика унификации пользователей в СЭАП в зависимости от роли пользователя в СЭ (одна из четырех политик аутентификации): по паре логин-пароль; по сертификату; двухфакторная аутентификация; или логин-пароль, или сертификат.

Участникам СЭ конфигурируются разные групповые политики для работы с ДП.



Программно-технологическое решение для СЭАП

Для обеспечения отказоустойчивости в клиенте СЭАП указывается список серверов для подключения к ДП, соответственно запросы пользователя выполняются по заданному списку.

Для балансировки нагрузки на ДП необходим балансировщик, который пулирует соединения пользователей на разные сервера ДП. А чтобы это можно было делать эффективнее, через API можно получать коэффициент текущей загруженности ДП по шкале от 0 до 1.

Запросы пользователя СЭАП на подключение к виртуальному рабочему столу по управляющему каналу передаются управляющему модулю и обратно пользователю СЭ. Трафик протокола доставки рабочего стола перенаправляет трафик от пользователя напрямую в удаленный рабочий стол.

PostgreSQL – сертифицированная конфигурационная база для обработки запросов пользователей и хранения данных системы.

Агент СЭАП – ключевой компонент по управлению и подготовке виртуального рабочего стола. Устанавливается на этапе подготовки шаблона виртуального рабочего стола АРМ эксперта, после чего может обновляться из веб-панели администратора безопасности. Агент СЭАП выполняет функции: присваивания виртуальным рабочим столам имен по заданной маске и подготавливает подключение. Перед каждым подключением пользователя агент СЭАП получает от УМ команду на подготовку виртуального рабочего стола, которая включает: настройку серверной части протокола доставки виртуального рабочего стола по полученным от УМ политикам; добавление пользователя в локальную группу безопасности (руководитель, группа руководства, сетевые эксперты, администратор безопасности); настраивает порты в firewall для организации подключения с ДП.

Управлением системой занимается администратор безопасности. Он может ввести виртуальных рабочих столов в домен, осуществить настройку firewall, управлять групповыми политиками, проводить настройку разрешений на использование периферийных устройств, локальных дисковых ресурсов, переводить рабочие столы экспертов в режим обслуживания, принудительно отключить пользователя СЭАП от рабочего стола, подключиться в сессию пользователя для оказания технической поддержки, управлять питанием виртуальных рабочих столов, отправлять сообщения пользователям.

Во время запуска АРМ пользователя СЭ собирается информация о физической конфигурации и формируется HWID (Hardware ID – идентификатор АРМ).

При подключении к ДП происходит авторизация устройства доступа: Клиент ПО СЭАП передает HWID и информацию о пользователе, Управляющий модуль производит авторизацию АРМ пользователя согласно настроенной политике.

При первом входе в систему пользователю СЭАП предлагается смена пароля, также как и если бы он был просрочен.

При обработке конфиденциальной информации необходимо шифрование сертифицированными протоколами ФСБ как управляющего трафика, так и трафика протокола доставки рабочего стола.

Протокол доставки виртуального рабочего стола – исполнительный механизм, доставляющий картинку на АРМ пользователя СЭ. От возможностей данного протокола зависит набор сервисов, которые будут работать.

При этом настраивается протокол пользователей СЭАП и на АРМ, и в виртуальном рабочем столе, используя агента СЭАП.

В свою очередь разработчики СЭАП объединят ресурсы в единый пул с возможностью динамического перераспределения ресурсов в зависимости от количества экспертов. Администраторы безопасности осуществят разграничение прав доступа к необходимой информации и организуют учет событий в платформе. Объем информации, предоставляемой конкретному эксперту, будет контролироваться и сможет быть изменен по требованию эксперта при предварительном согласовании с руководителем (заказчиком) экспертизы. Эксперты при использовании технологий виртуализации и контейнеризации получают быстрый и надежный доступ к услугам при заданном уровне безопасности информации. При этом вычислительные мощности серверного оборудования будут использоваться наиболее эффективно.

Базовыми технологиями математического обеспечения СЭАП должны стать современные технологии экспертно-аналитической обработки информации: умные сети (Smart Grid); искусственные нейронные сети и генетические алгоритмы; ситуационное управление; семантическое моделирование; агентные вычисления; кибербезопасность [6].

Процедура контроля функционирования СЭАП реализуется последовательностью выполнения операций сбора, обработки и учета информации, анализа и постановки задачи с последующим принятием управленческого решения [3, 4].

Модель процедуры контроля подготовки к принятию решений представляется в виде совокупности вербального, математического и информационного слоев, объединяющих соответствующие уровни представления модели.

Вербальный слой модели описывает процедуру контроля как совокупность технологических операций и как перечень задач, решаемых в рамках каждой из операций.

Математический слой представляет собой формальные постановки задач контроля, а также решения этих задач с использованием соответствующего математического аппарата. В этом же слое осуществляется выбор параметров и назначение переменных в соответствии с информационным слоем, описывающим предметную область процедуры контроля.

Информационный слой обеспечивает информационную основу для решения задач в составе технологических операций. Уровни представления входной, выходной и нормативно-справочной информации являются основой для применения в разработанной модели процедуры контроля моделей данных и соответствующих информационных технологий.

Модель процедуры контроля выполнения мероприятий по управлению войсками является составной, объединяя модели агрегированных состояний объекта контроля и идентификации информационных состояний СЭАП.

Модель агрегированных состояний объекта контроля позволяет определять минимальный состав комплекса проверок при выполнении процеду-

ры контроля экспертизы вариантов решений. Модель не оперирует с множеством входных воздействий, вызывающих переход объекта контроля из одного состояния СЭАП в другое, а работает с множеством признаков (состояний), описывающих реакцию объекта на эти воздействия.

Модель идентификации информационных состояний объекта контроля задает множество его агрегированных состояний и определяет вероятностную меру и возможные переходы между ними с описанием механизма этих переходов. В рамках этой модели идентификацию информационных состояний выполнения плана мероприятий по управлению войсками можно рассматривать как управляемый дискретный многошаговый процесс стохастического типа.

В отличие от «традиционных» систем специфика СЭАП накладывает определенные ограничения на формальное представление входных и выходных сигналов системы, признаков агрегированных состояний, построение агрегированной модели объекта контроля. При практическом применении предлагаемых решений целесообразно использовать логические характеристики (параметры и переменные) и образы объекта контроля с последующим решением задач распознавания образов.

Разрабатываемая СЭАП может быть использована как инструментальное сетевое средство поддержки принятия решения для руководителей ОВУ в интересах обеспечения обороны и безопасности страны. СЭАП свяжет и обеспечит функционирование экспертных сообществ в распределенной сетевой среде, для проведения комплексной экспертизы проектов. Доступ будет обеспечен с их АРМ в назначенный момент времени, к заранее установленному набору услуг и поставленным задачам. Разработчики, используя технологии виртуализации и контейнеризации, обеспечат участников СЭ новым уровнем доступности к информации проекта и простоты ее анализа. Использование технологий виртуализации и контейнеризации позволит повысить уровень управляемости инфраструктурой СЭАП и ее масштабируемости в зависимости от объекта экспертизы, уменьшить общие накладные расходы на построение IT-инфраструктуры органов военного управления.

Заключение. Предлагаемые решения являются универсальными и могут быть использованы при разработке автоматизированных рабочих мест любого должностного лица органа государственного управления – участника процесса принятия бизнес-решений и управленческих решений в распределенной среде. Уровень контроля, направление работы и степень детализации контролируемых характеристик определяются составом и содержанием информационного слоя модели.

Литература

1. *Армашова-Тельник Г.С.* Проблематика принятия управленческих решений в условиях цифровизации экономики России // Инновационная наука. 2020. № 4. С. 96–100.
2. *Богомолов А.В., Климов Р.С.* Автоматизация обработки информации при проведении коллективных сетевых экспертиз // Автоматизация. Современные технологии. 2017. Т. 71. № 11. С. 509–512.

3. *Волосенков В.О., Морозов А.В., Бужлаков С.Н., Мажара И.В*. Способ оценивания защищенности информационных ресурсов автоматизированных систем управления специального назначения // I-methods. 2019. Т. 11. № 3. С. 1–6.
4. *Голосовский М.С*. Модель жизненного цикла разработки программного обеспечения в рамках научно-исследовательских работ // Автоматизация и современные технологии. 2014. № 1. С. 43–46.
5. *Губанов Д.А., Коргин Н.А., Новиков Д.А., Райков А.Н*. Сетевая экспертиза. М.: Эгвес, 2010. 170 с.
6. *Массель А.Г., Бахвалов К.С*. Применение интеллектуальных технологий для решения проблемы научного обоснования стратегических решений по цифровой трансформации энергетики // Информационные и математические технологии в науке и управлении. 2019. № 1 (13). С. 47–60.
7. Модельный закон «О научной и научно-технической экспертизе». Принят на XXII пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ (постановление № 22-17 от 15 ноября 2003 г.).
8. *Наумов В.В*. Актуальные вопросы построения комплекса моделей и методов информационно-аналитической поддержки системы управления специального назначения // I-methods. 2019. Т. 11. № 2. С. 1–9.
9. *Сизоненко А.Б., Булгаков О.М., Клюев С.Г*. Модель защищенной подсистемы контроля документных систем на основе технологии «блокчейн» // Моделирование, оптимизация и информационные технологии. 2018. Т. 6. № 2 (21). С. 293–300.
10. *Сильников М.В., Ямпольский С.М., Шаламов А.С., Злобин С.М., Гарькушев А.Ю*. Концептуальные основы информационно-аналитического обеспечения органов управления военной организацией государства // Известия Российской академии ракетных и артиллерийских наук. 2016. № 4 (94). С. 9–15.
11. *Федоров М.В., Калинин К.М., Богомолов А.В., Стецюк А.Н*. Математическая модель автоматизированного контроля выполнения мероприятий в органах военного управления // Информационно-измерительные и управляющие системы. 2011. Т. 9. № 5. С. 46–54.

Bibliography

1. *Armashova-Tel'nik G.S*. Problematika prinjatija upravlencheskih reshenij v uslovijah cifrovizacii jekonomiki Rossii // Innovacionnaja nauka. 2020. № 4. P. 96–100.
2. *Bogomolov A.V., Klimov R.S*. Avtomatizacija obrabotki informacii pri provedenii kollektivnyh setevyh jekspertiz // Avtomatizacija. Sovremennye tehnologii. 2017. Vol. 71. № 11. P. 509–512.
3. *Volosenkov V.O., Morozov A.V., Buzhlakov S.N., Mazhara I.V*. Sposob ocenivanija zashhishhennosti informacionnyh resursov avtomatizirovannyh sistem upravlenija special'nogo naznachenija // I-methods. 2019. Vol. 11. № 3. P. 1–6.
4. *Golosovskij M.S*. Model' zhiznennogo cikla razrabotki programmnogo obespechenija v ramkah nauchno-issledovatel'skih rabot // Avtomatizacija i sovremennye tehnologii. 2014. № 1. P. 43–46.
5. *Gubanov D.A., Korgin N.A., Novikov D.A., Rajkov A.N*. Setevaja jekspertiza. M.: Jegves, 2010. 170 p.
6. *Massel' A.G., Bahvalov K.S*. Primenenie intellektual'nyh tehnologij dlja reshenija problemy nauchnogo obosnovanija strategicheskih reshenij po cifrovoj transformacii jenergetiki // Informacionnye i matematicheskie tehnologii v nauke i upravlenii. 2019. № 1 (13). P. 47–60.
7. Model'nyj zakon «O nauchnoj i nauchno-tehnicheskoj jekspertize». Prinjat na XXII plenarnom zasedanii Mezhparlamentskoj Assamblei gosudarstv-uchastnikov SNG (postanovlenie № 22-17 ot 15 nojabrja 2003 g.).

8. *Naumov V.V*. Aktual'nye voprosy postroenija kompleksa modelej i metodov informacionno-analiticheskoj podderzhki sistemy upravlenija special'nogo naznachenija // I-methods. 2019. Vol. 11. № 2. P. 1–9.
9. *Sizonenko A.B., Bulgakov O.M., Kljuev S.G*. Model' zashhishhennoj podsistemy kontrolja dokumentnyh sistem na osnove tehnologii «blokchejn» // Modelirovanie, optimizacija i informacionnye tehnologii. 2018. Vol. 6. № 2 (21). P. 293–300.
10. *Sil'nikov M.V., Jampol'skij S.M., Shalamov A.S., Zlobin S.M., Gar'kushev A.Ju*. Konceptual'nye osnovy informacionno-analiticheskogo obespechenija organov upravlenija voennoj organizaciej gosudarstva // Izvestija Rossijskoj akademii raketnyh i artillerijskih nauk. 2016. № 4 (94). P. 9–15.
11. *Fedorov M.V., Kalinin K.M., Bogomolov A.V., Stecjuk A.N*. Matematicheskaja model' avtomatizirovannogo kontrolja vypolnenija meroprijatij v organah voennogo upravlenija // Informacionno-izmeritel'nye i upravljajushhie sistemy. 2011. Vol. 9. № 5. P. 46–54.