Научная статья
УДК 004.056.52:004.732
https://doi.org/10.24143/2072-9502-2023-1-71-82
EDN JBCFBM

Метод назначения прав доступа к приложениям в корпоративной мобильной сети

Алла Григорьевна Кравец[1]✉, Наталия Анатольевна Сальникова[2]

[1]Волгоградский государственный технический университет,
Волгоград, Россия, AllaGKravets@yandex.ru✉

[1]Университет «Дубна», Дубна, Россия

[2]Волгоградский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ, Волгоград, Россия

Аннотация. Представлено исследование и реализация метода назначения прав доступа к приложениям в корпоративной мобильной сети с разными требованиями по уровню защищенности, который позволит принять во внимание особенности деятельности различных пользователей. Проанализированы существующие решения по назначению прав доступа к приложениям и сервисам внутрикорпоративной сети, обоснована необходимость создания метода, обеспечивающего информационную безопасность при реализации доступа в корпоративных сетях с разными требованиями по уровню защищенности. На основе проведенного анализа тенденций и перспектив развития современных корпоративных мобильных сетей установлено противоречие между требованиями, предъявляемыми к безопасности информации с использованием универсальных мобильных устройств при доступе к защищенным услугам, и техническими возможностями систем защиты информации, обеспечивающих безопасность доступа в корпоративных сетях с разными требованиями по защищенности. Для решения данной задачи реализована многопользовательская система, обеспечивающая работу любой компьютерной техники и мобильных устройств организации, СУБД которой имеет архитектуру «клиент – сервер». Функциональные требования, предъявляемые к разрабатываемому методу, заключаются в том, что он должен обеспечивать возможность выполнения авторизации пользователей, предоставлять администратору возможность управлять правами доступа пользователей к различным приложениям, управлять хранилищем приложений, регистрировать операции, выполняемые пользователем, и вести отчетность. В ходе программной реализации метода назначения прав доступа поэтапно описано проектирование базы данных, построена модель информационных потоков, рассмотрена физическая схема взаимодействия отдельных процедур, на основании которых создана база данных, разработан пользовательский интерфейс с формами, отображающими информацию, хранящуюся в базе данных.

Ключевые слова: права доступа, пользователь, хранение данных, безопасность, защита информации, разграничение полномочий, приложение, корпоративная сеть, Web-сервер

Для цитирования: *Кравец А. Г., Сальникова Н. А.* Метод назначения прав доступа к приложениям в корпоративной мобильной сети // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика 2023. № 1. С. 71–82. https://doi.org/10.24143/2072-9502-2023-1-71-82. EDN JBCFBM.

Original article

Method of assigning access rights to applications in corporate mobile network

Alla G. Kravets[1]✉, Natalia A. Salnikova[2]

[1]Volgograd State Technical University,
Volgograd, Russia, AllaGKravets@yandex.ru✉

[1]Dubna State University, Dubna, Russia

[2]Volgograd Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration, Volgograd, Russia

Abstract. The article focuses on studying and implementing a method of assigning access rights to the applications in a corporate mobile network with different requirements for security, which will allow considering the specific activities of multiple users. The existing solutions for assigning access rights to applications and services of the intranet are analyzed, the need to create a method that ensures information security when implementing access in corporate networks with different requirements for the level of security is substantiated. Due to the results of analysis of trends and development prospects of modern corporate mobile networks there has been found a contradiction between the requirements for information security of universal mobile devices with access to secure services and technical capabilities of information security systems that ensure access security in the corporate networks with different security requirements. To solve the problem, a multi-user system has been implemented that ensures operation of any computer equipment and mobile devices of an organization whose DBMS has a client-server architecture. The functional requirements for the developed method include the ability to perform user authorization, providing the administrator with the ability to manage user access rights to various applications, managing application storage, recording user operations, and keeping records. In the course of the software implementation of the method of assigning access rights, the design of the database is described in stages, a model of information flows is built, a physical diagram of the interaction of individual procedures is considered, on the basis of which the database is created, a user interface with forms that display information stored in the database is developed.

Keywords: access rights, user, data storage, security, information protection, differentiation of powers, application, corporate network, Web server

For citation: Kravets A. G., Salnikova N. A. Method of assigning access rights to applications in corporate mobile network. *Vestnik of Astrakhan State Technical University. Series: Management, Computer Science and Informatics*. 2023;1:71-82. (In Russ.). https://doi.org/10.24143/2073-5529-2023-1-71-82. EDN JBCFBM.

Введение

В процессе проектирования единой корпоративной сети для крупных компаний наиболее сложной проблемой всегда будет управление правами доступа к приложениям и сервисам этой сети. В корпоративных сетях Web-серверы или серверы приложений должны иметь средства управления полномочиями [1]. Для выполнения этого требования применяют конфигурационные файлы, которые можно редактировать с помощью простых текстовых редакторов, для более сложных случаев используют развитый графический интерфейс или средства операционной системы. Встречаются случаи, когда в исходном тексте приложения размещают конфигурацию системы назначения прав доступа, тогда в любом случае изменения настроек системы разграничения прав доступа будет происходить трансформация модулей программного обеспечения [2, 3]. Любые попытки ввода или удаления учетных записей пользователей, публикация или удаление ресурсов приведут к появлению ошибок и необходимости вмешательства администратора в настройки каждой системы для внесения изменений.

Если корпоративная сеть включает в себя небольшой набор приложений, то с проблемой разделения прав доступа можно справляться с помощью собственных встроенных в Web-серверы средств [4]. Например, базы данных с информацией о пользователях можно объединять, применяя собственные разработки или программное обеспечение мета каталогов, тогда Web-серверы и серверы приложений могут хранить информацию о разделении прав доступа к приложениям в том же каталоге [5, 6]. Но с ростом числа используемых приложений эксплуатация системы усложняется, цена реализации резко возрастает и может сравняться со стоимостью переноса ее на новую платформу [7, 8].

Мобильные технологии пришли в бизнес достаточно давно, и работодатели повсеместно применяют их для рабочих целей. Возникающие проблемы в областях безопасности, надежности хранения данных приходится решать постоянно. Для современных компаний существенным риском, безусловно, является высокая вероятность утечки корпоративной информации, что приводит к серьезным потерям в финансовой, экономической, технической областях деятельности компании, а также к потере личной информации сотрудников. Чтобы избежать этих неприятностей, необходимо иметь строгие правила корпоративной безопасности, два из которых должны соблюдаться особенно строго: первое – управление мобильными устройствами (MDM – Mobile Device Management) для обеспечения конфигурирования устройств в соответствии с заданными политиками, второе – разделение деловых и личных данных на мобильных устройствах сотрудников, на которых установлены корпоративные приложения для работы с профессиональным программным обеспечением, электронной почтой, корпоративной службой каталогов. Из практического опыта использования различных корпоративных сетей можно сделать вывод, что основные риски компаний связаны с применением малоэффективных средств защиты информации и разделения прав доступа пользователей к различным приложениям.

Актуальность данной работы очевидна, поскольку никто не застрахован от утечки корпоративной информации, а руководители крупных корпораций чаще других подвергаются хакерским атакам, и у них особенно высоки риски потери

конфиденциальной информации. Чем выше статус и должность сотрудника, тем выше ценность информации, которую он использует при выполнении своих служебных обязанностей. Применение мобильных устройств в работе напрямую влияет на скорость получения и обработки информации, а значит и служит повышению эффективности результатов работы и качества управления компанией в целом. Политика использования персональных мобильных устройств с разделением уровней прав доступа целиком зависит от полноты предусмотренного заранее списка возможных угроз.

Целью работы является разработка метода назначения прав доступа к приложениям в корпоративных сетях с разными требованиями по уровню защищенности, который позволит принять во внимание особенности деятельности различных пользователей и назначить доступ к необходимым для работы приложениям.

На основе проведенного анализа тенденций и перспектив развития современных корпоративных мобильных сетей установлено противоречие между требованиями, предъявляемыми к безопасности информации с использованием универсальных мобильных устройств при доступе к защищенным услугам, и техническими возможностями систем защиты информации, обеспечивающих безопасность доступа в корпоративных сетях с разными требованиями по защищенности.

Анализ процесса назначения прав доступа в корпоративных сетях

Современные условия организации производства вынуждают большинство компаний применять в своей деятельности информационные технологии, разрабатывать различные высокотехнологичные решения, что обеспечивает их высокую конкурентоспособность на рынке [9, 10].

На сегодняшний день в каждой большой корпорации есть отдел информационных технологий, который занимается поддержкой и развитием IT-инфраструктуры предприятия, сотрудники которого обычно занимаются следующими видами деятельности:

– осуществляют системное администрирование;

– обеспечивают работоспособность внутренних и внешних серверов;

– предоставляют поддержку пользователей.

Рассмотрим более подробно поддержку пользователей.

Специалист по поддержке пользователя отвечает за назначение прав доступа пользователей, проведение диагностики программного и аппаратного обеспечения, предоставляет техническую поддержку и консультации конечным пользователям, несет ответственность за организацию ремонта компьютерной техники, обеспечивает наличие расходных материалов для компьютерной и оргтехники; консультирует пользователей по техническим вопросам [11, 12].

Наиболее трудоемким является процесс, связанный со своевременным назначением прав доступа к приложениям корпоративной сети, поскольку это требует понимания выполняемых функций и задач пользователем в соответствии с должностными инструкциями. Следовательно, происходит значительное расширение должностных обязанностей специалиста по поддержке пользователя [13, 14].

При традиционном подходе к организации прав доступа в системе сотрудники, которые чаще других обращаются к приложениям, должны не только получить учетную запись для каждого из них, но и многократно проходить процедуру авторизации, что вызывает негативную реакцию [15, 16]. Очень часто сотрудники компаний небрежно обращаются со своими паролями, иногда и забывают их. Диаграмма предлагаемой модели работы сотрудников отдела по вопросу принятия и обработки обращений на назначение прав доступа к приложениям мобильной корпоративной сети представлена на рис. 1.

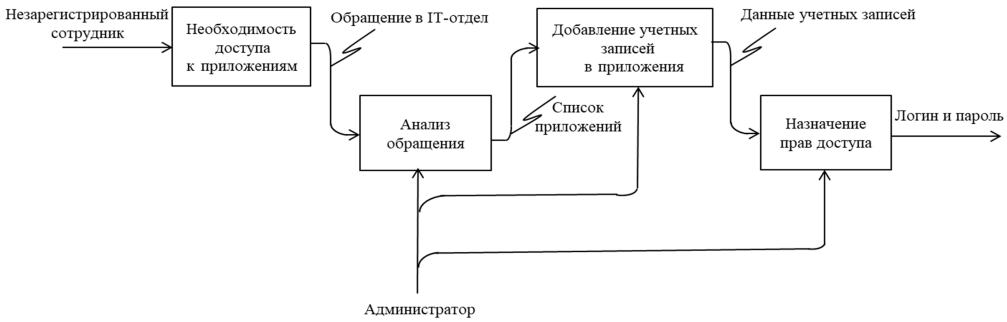

Рис. 1. Структурно-функциональная модель процесса назначения прав доступа к приложениям в корпоративной мобильной сети

Fig. 1. Structural and functional model of assigning access rights to applications in the corporate mobile network

В данный момент деятельность специалиста по поддержке пользователя сводится к получению заявки на разрешения доступа к каждому приложению в отдельности. На следующем этапе происходит анализ обращения и определяется необходимость учетной записи, которая наделяет пользователя логином и паролем для совершения процедуры авторизации в приложении [17, 18]. При выявлении такой ситуации создается учетная запись, которая наделяет пользователя правом доступа. Данная процедура приемлема для небольших компаний, количество сотрудников и приложений в которой ограничено несколькими десятками [19].

Для компаний, численность сотрудников которых превышает данное количество пользователей, у специалиста по поддержке может возникать ряд трудоемких задач:

– при увольнении сотрудника или его переводе из одного подразделения в другое возникает необходимость изменения доступа к различным приложениям;

– при увеличении штата компании процесс создания учетных записей и авторизации занимает большую часть рабочего времени, что препятствует выполнению других обязанностей в рамках занимаемой должности.

Обзор и анализ существующих решений

На сегодняшний день на рынке присутствует множество разнообразных систем разграничения доступа к корпоративным приложениям. Ниже приведен обзор некоторых систем, который дает представление о состоянии данной сферы.

Oracle Mobile Security Suite. Новый комплекс в сочетании с решениями для управления идентификационными данными Identityand Access Management предоставляет интегрированную платформу Oracle, используя которую корпорации могут управлять доступом ко всем используемым в работе приложениям с помощью различных устройств, включая мобильные. Данное решение отвечает современным концепциям COPE (когда устройство принадлежит компании и используется сотрудником для работы и в личных целях) или BYOD (когда устройство принадлежит сотруднику и используется им персонально и в рабочих целях) [20].

Oracle Mobile Security ориентирован на пользователей и отдельные приложения, служит для эффективного и безопасного управления доступом к различным приложениям.

Комплекс предоставляет собой безопасную рабочую среду, которая позволяет изолировать и защищать корпоративные приложения и данные от других приложений и данных на устройстве, а политики контролируют перемещение данных в рабочую область и из нее. Безопасный доступ к сторонним приложениям, добавленным в безопасную рабочую область, осуществляется за счет инструментов контейнеризации приложений. Политики безопасности сохраняют конфиденциальность персонального контента и приложений пользователя на одном и том же клиентском устройстве за счет разделения корпоративной и персональной информации. Oracle Mobile Security обеспечивает пользователю безопасное рабочее пространство, мобильный сервер доступа безопасности и единую административную консоль. Oracle Mobile Security располагает единой административной консолью, механизмом однократной регистрации, туннельным сетевым соединением для каждого защищенного приложения и функцией шифрования хранимых данных. Структура комплекса представлена на рис. 2.

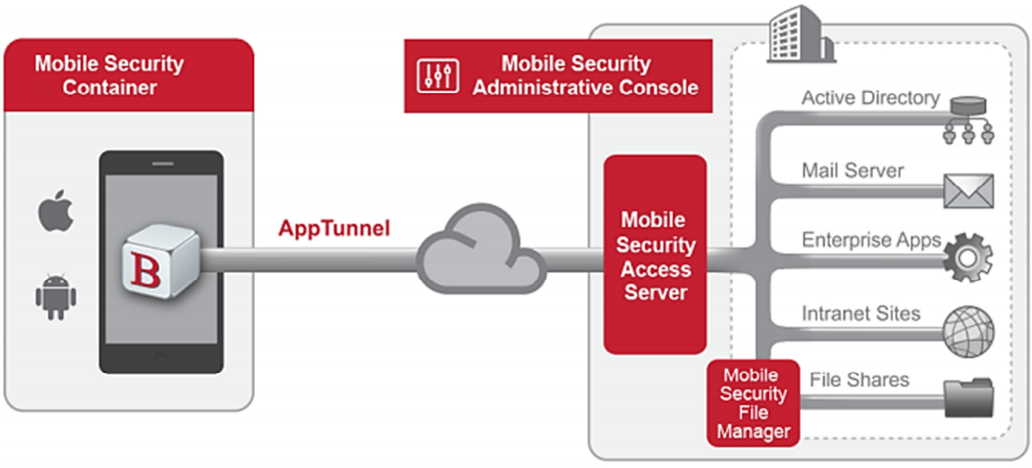

Рис. 2. Структура Oracle Mobile Security Suite

Fig. 2. Structure of Oracle Mobile Security Suite

Основное назначение Oracle Mobile Security Suite – управление мобильной безопасностью. Его основные инструменты управления и контроля:

– режим Geo-Fencing, который служит для ограничения прав доступа в зависимости от геолокации;

– управление политиками использования приложений для предотвращения утечки данных, особенно ограничение функций копирования/вставки/печати;

– построение безопасных сетевых туннелей для приложений, которые предоставляют защиту информации без использования VPN-подключений через виртуальные частные сети;

– предоставление возможности дистанционного удаления корпоративной информации сотрудника при его увольнении.

MS Azure Active Directory. Azure Active Directory (Azure AD) помогает управлять облачными приложениями, локальными приложениями и ресурсами с помощью корпоративных групп. Ресурсы могут как относиться к каталогу (например, разрешения на управление объектами с помощью ролей в каталоге), так и не относиться (например, приложения SaaS, службы Azure, сайты SharePoint и локальные ресурсы) [21].

Azure AD позволяет предоставлять доступ к корпоративным ресурсам, предоставляя права доступа одному пользователю или группе Azure AD. Используя группы, владелец ресурса (или владелец каталога Azure AD) может назначить набор разрешений на доступ всем членам группы, а не предоставлять права по отдельности. Владелец ресурса или каталога может также предоставить права на управление списком членов кому-либо другому, например руководителю отдела или администратору службы технической поддержки, позволяя этому лицу добавлять и удалять участников по мере необходимости. Структура Azure AD представлена на рис. 3.

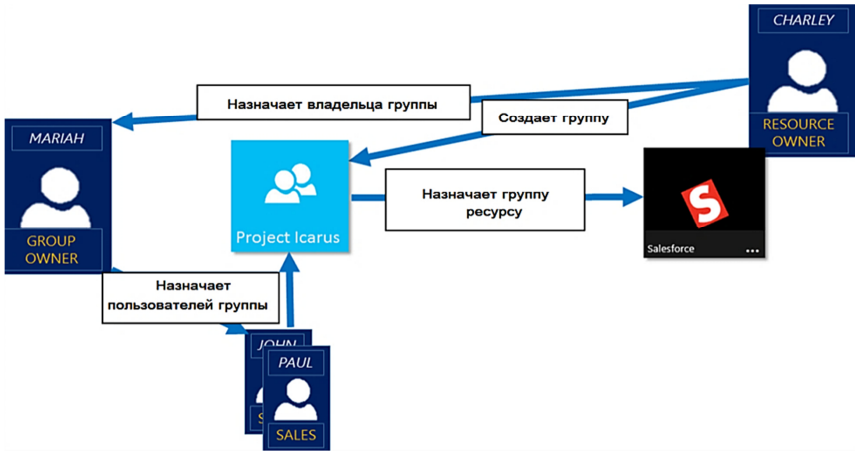

Рис. 3. Структура Azure AD

Fig. 3. Structure of Azure AD

Существует 4 способа назначить пользователям права доступа к ресурсу:

– прямое назначение: владелец ресурса непосредственно назначает пользователя ресурсу;

– назначение группы: владелец ресурса назначает ресурсу группу AzureAD, которая автоматически предоставляет всем своим членам доступ к этому ресурсу. Членством в группе управляют как владелец группы, так и владелец ресурса, что позволяет каждому из них добавлять и удалять членов группы;

– назначение на основе правил: владелец ресурса создает группу и с помощью правила определяет, какие пользователи назначены определенному ресурсу. Правило основывается на атрибутах, назначенных отдельным пользователям. Владелец ресурса управляет правилом, определяя, какие атрибуты и значения необходимы для предоставления доступа к ресурсу;

– назначение внешним источником: доступ предоставляется внешним источником, таким как локальный каталог или приложение SaaS. В этой ситуации владелец ресурса назначает группу для предоставления доступа к ресурсу, а членами группы управляет внешний источник.

Cisco DNA Center. Cisco DNA Center – это новая архитектура для корпоративных сетей для поддержки роста бизнеса и внедрения инноваций. Ключевым принципом системы является автоматизация и надежность за счет применения специализированных систем управления развертывания инфраструктуры. К преимуществам таких решений однозначно можно отнести глубокую интеграцию с обслуживаемым решением и, как следствие, богатые возможности настройки. Также они позво-

ляют поддерживать высокое качество приложений и обеспечивать их безопасность [22].

Cisco DNA Center – это революционная архитектура для любого современного предприятия, обеспечивающая поддержку сети на основе намерений, простое и быстрое управление сетью, увеличение времени безотказной работы сети, эффективный мониторинг, также позволяет выполнять установку и обновление устройств за считанные минуты, подключать к сети новые удаленные офисы, при этом сохраняя низкие эксплуатационные расходы.

Cisco DNA Center поддерживает работу в сети на основе намерений, за счет чего снижается нагрузка на сетевых инженеров. Благодаря логичным рабочим процессам проектирование, предоставление и настройка политик упрощаются, вследствие чего развертывание новых устройств происходит за очень короткое время, а время безотказной работы сети увеличивается многократно.

Благодаря эффективной функции мониторинга можно очень быстро и эффективно отслеживать состояние сети, устранять неполадки сети за считанные минуты, обнаруживать и устранять угрозы даже в зашифрованном трафике с помощью технологии машинного обучения. С помощью DNA Center можно создавать виртуальные сети как способ значительно повысить эффективность использования доступных ресурсов.

В Cisco DNA Center интегрированы современные решения для обеспечения информационной и сетевой безопасности. Программные и аппаратные компоненты на всех уровнях архитектуры оснащены специализированными средствами контроля доступа и обнаружения угроз. Структура Cisco DNA Center представлена на рис. 4.

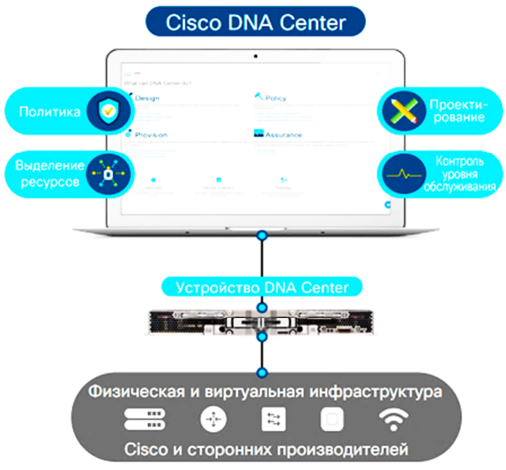

Рис. 4. Структура Cisco DNA Center

Fig. 4. Structure of Cisco DNA Center

G Suite Google. G Suite Google предлагает функции управления мобильными устройствами, в частности для администрирования корпоративных мобильных устройств, обеспечения их безопасности и их отслеживания. Устанавливаются правила, с помощью которых сотрудники могут работать с ресурсами компаний как на личных устройствах, так и на устройствах, предоставленных работодателями [23].

Предоставляется два уровня управления: базовый и расширенный. Набор доступных параметров зависит от используемого режима. Некоторые расширенные функции, например аудит устройств и установка правил, доступны не во всех версиях.

В базовом режиме управления можно выполнять следующие действия:

– устанавливать правила, требующие настроить блокировку экрана или пароль, для защиты корпоративных данных на устройствах;

– удалять корпоративные данные с потерянных или украденных устройств;

– предоставлять пользователям доступ к рекомендуемым корпоративным приложениям для устройств Android;

– публиковать и распространять частные приложения;

– просматривать список устройств с доступом к корпоративным данным в консоли администратора Google.

Если необходимо расширить набор функций для контроля устройств с доступом к корпоративным данным, можно использовать расширенный режим управления, который позволяет:

– устанавливать режим требования назначения пароля повышенной надежности;

– предоставлять пользователям доступ к расширенному набору корпоративных приложений, работающих под операционными системами Android и iOS;

– на устройствах, работающих под Android, использовать рабочие профили для разделения личных и корпоративных данных;

– закрывать доступ к некоторым настройкам и функциям устройств, например, чтобы сотрудники не могли подключаться к Wi-Fi или мобильным сетям, делать скриншоты и т. д.;

– отслеживать работу сотрудников, нарушающих установленные правила, получать отчеты об их работе.

Сравнительный анализ систем разграничения доступа к корпоративным приложениям

Сравнительный анализ систем разграничения прав доступа к корпоративным приложениям приведен в таблице.

Сравнительный анализ систем разграничения прав доступа к корпоративным приложениям

Comparative analysis of systems of differentiating access rights to corporate applications

Функция	Анализируемые системы			
	Oracle Mobile Security Suite	MS Azure Active Directory (Azure AD)	Cisco DNA Center	G SuiteGoogle
Бесплатная версия	–	–	–	+
Удобный интерфейс	+	+	+	+
Открытый код	–	–	–	–
Поддержка шифрования данных	+	+	+	+
Дополнительные плагины	+	–	+	–
Поддержка нескольких языков	+	+	+	+

После проведения анализа существующих систем было принято решение производить разработку метода назначения прав доступа к приложениям в корпоративной сети собственными силами, без привлечения платного программного обеспечения. Это обусловлено тем, что уже существующие разработки имеют либо ограниченный функционал, которого недостаточно для реализации всех функций, либо избыточный, т. е. финансы, затраченные на приобретение готового решения, останутся не использованными в полном объеме. При приобретении готового программного обеспечения необходимо выделять ресурсы на обучение персонала для подготовки, наладки и поддержания стабильной работы приобретаемого продукта. Также в связи с санкционной политикой иностранных компаний по использованию результатов интеллектуальной деятельности и с целью повышения безопасности доступа к приложениям в корпоративных сетях необходимо разработать уникальный метод назначения прав с разными требованиями по уровню защищенности.

Проектирование и разработка метода назначения прав доступа к приложениям в корпоративной мобильной сети

Для решения данной задачи используется многопользовательская система, обеспечивающая работу любой компьютерной техники и мобильных устройств организации, СУБД которой имеет архитектуру «клиент – сервер».

Клиент-серверные СУБД при работе пересылают минимально необходимые объемы информации между клиентом и сервером, но при этом основная вычислительная нагрузка ложится на сервер. Клиент выполняет минимальные функции предварительной обработки информации при пересылке ее серверу, его основная функция заключается в организации доступа к серверу [24].

Клиент-серверные СУБД, по сравнению с файл-серверными СУБД, имеют значительное преимущество, т. к. менее требовательны к пропускной способности, особенно при выполнении поиска в базе данных по заданным параметрам пользователя. Сервер, помимо хранения централизованной базы данных, обеспечивает выполнение основного объема обработки данных. Запрос на данные, выдаваемый клиентом, порождает поиск и извлечение данных на сервере. Извлеченные данные, которые обычно на несколько порядков меньше по объему, чем весь массив данных, хранимый на сервере, транспортируются по сети от сервера к клиенту. Результат выполнения запроса отображается пользователю.

В качестве рабочей СУБД выбрана MS Access. В качестве языка программирования и среды разработки выбран Embarcadero RAD studio.

Построение модели информационной системы начинается с описания функционирования системы в целом. Рассмотрим процессы, которые происходят при взаимодействии в корпоративных сетях. Если пользователь хочет получить права доступа, он должен обратиться напрямую к администратору, который, проанализировав должностные инструкции и направления работы пользователя, либо добавит данные по пользователю в модуль, либо откажет в этом, если для выполнения работы не требуется работа с приложениями корпоративной мобильной сети. Если пользователь хочет авторизоваться в сети, он вводит логин и пароль в Web-интерфейсе модуля, после чего получает список доступных приложений. Администратор может добавлять, удалять, редактировать и просматривать базу данных.

Функциональные требования, предъявляемые к разрабатываемому методу, заключаются в том, что он должен обеспечивать возможность выполнения авторизации пользователей, предоставлять администратору возможность управлять правами доступа пользователей к различным приложениям, управлять хранилищем приложений, регистрировать операции, выполняемые пользователем, и вести отчетность.

Из диаграммы, представленной на рис. 5, видно, что процесс назначения прав доступа должен сводиться к анализу обращений пользователей и регистрации их при помощи модуля назначения прав доступа.

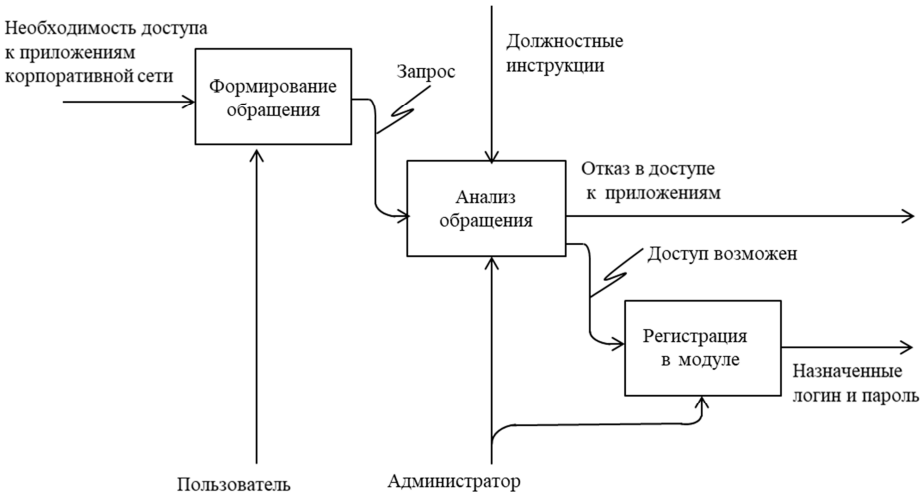

Рис. 5. Диаграмма декомпозиции процесса назначения прав доступа

Fig. 5. Diagram of decomposition of assigning access rights

Алгоритм реализации метода назначения прав доступа к приложениям корпоративной мобильной сети

Предлагаемый метод регламентирует последовательность процесса обращения за доступом к приложениям. Пользователь напрямую обращается к администратору, который проводит анализ должностных инструкций сотрудника и либо выдает права доступа к необходимым приложениям корпоративной мобильной сети, либо отказывает в их получении. Для авторизации в сети необходимо вводить логин и пароль, после этого сотрудник получает доступ к нужным приложениям. Контроль работы осуществляет администратор, который может редактировать базу данных. На рис. 6 представлен алгоритм метода по принятию и обработке обращений на назначение прав доступа к приложениям мобильной корпоративной сети.

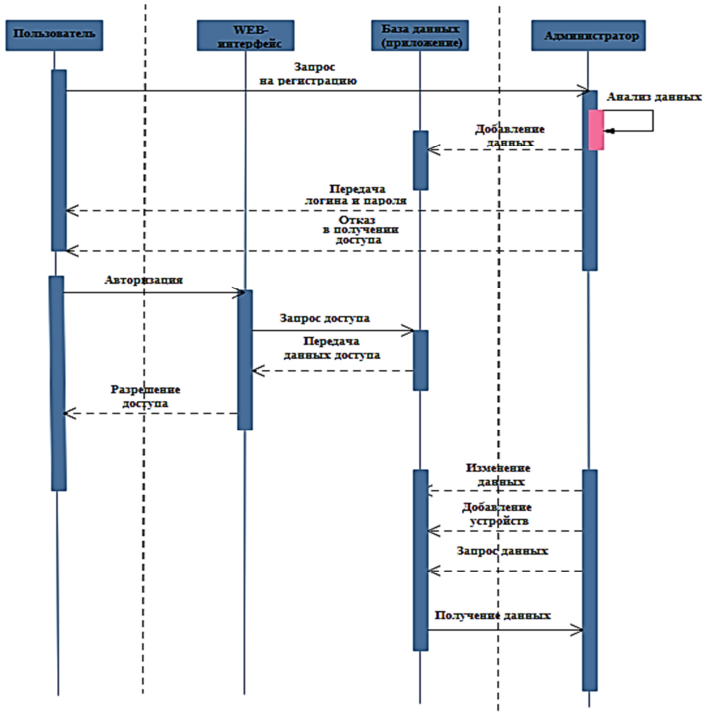

Рис. 6. Алгоритм метода назначения прав доступа к приложениям мобильной корпоративной сети

Fig. 6. Algorithm of assigning access rights to mobile corporate network applications

Концепция программной реализации метода назначения прав доступа к приложениям мобильной корпоративной сети

При выполнении программной реализации предлагаемого метода назначения прав доступа к приложениям необходимо учитывать, чтобы система обеспечивала выполнение следующих функций:

– при входе в систему администратор и сотрудники должны выполнить авторизацию в пользовательском интерфейсе;

– администратор осуществляет управление пользователями: сопровождает, добавляет и редактирует информацию сотрудников (логин, пароль и др.);

– администратор организует, добавляет и редактирует список корпоративных приложений в хранилище;

– администратор отслеживает работу мобильных приложений: распределяет права доступа к приложениям, ограничивает вход мобильным устройствам в корпоративную сеть или к различным приложениям;

– ведение отчетности: регистрация операций, выполненных пользователями.

Входные данные вводятся администратором и должны включать:

– информацию о пользователе − всю необходимую информацию о пользователе мобильных устройств и приложений (логин, пароль, …);

– информацию о мобильном устройстве − всю необходимую информацию о мобильном устройстве (название, ID, IMEI, модель, …);

– список приложений и всю необходимую информацию о приложениях (название, описание, версия, …).

На рис. 7 представлена инфологическая модель данных [25].

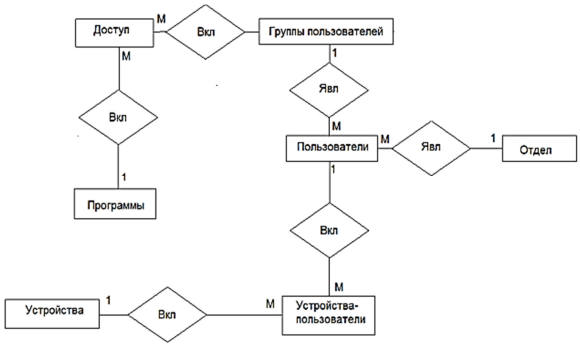

Рис. 7. Инфологическая модель данных: 1-M – связь «один-ко-многим»; Явл – отношение «Состоит из»

Fig. 7. Infological model of data: 1-M – connection «one-to-many»; Явл – relation «Consist of»

В ходе анализа предметной области были выделены следующие сущности:

– сущность «Устройства» (код, IMEI, название устройства, IP адрес, версия ОС, дата регистрации);

– сущность «Отдел» (код, наименование отдела);

– сущность «Пользователи» (код, фамилия, имя, логин, пароль, код группы, e-mail, комментарий, код отдела);

– сущность «Группы пользователей» (код, имя группы, комментарий);

– сущность «Программы» (код, имя программы, ссылка на программу, версия программы, дата добавления, описание);

– сущность «Устройства-пользователи» (код, код устройства, код пользователя);

– сущность «Доступ» (код, код группы, код программы).

Главное окно программы (рис. 8) состоит из следующих элементов:

– вкладка просмотра сведений о пользователях;

– вкладка просмотра сведений о группах пользователей;

– вкладка просмотра сведений о программах.

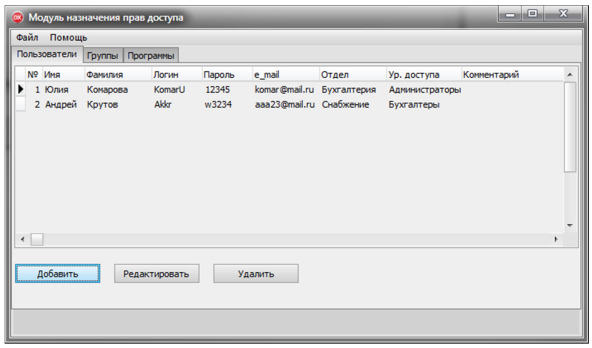

Рис. 8. Экранная форма главного окна программы

Fig. 8. Screen chart of the main program window

Главное меню (см. рис. 8) обеспечивает добавление новых данных о пользователях, о рабочих группах, об используемых программах и приложениях, а также предоставляет возможность редактирования внесенных данных.

Заключение

При выполнении данного проекта проведен анализ деятельности сотрудников отдела, ответственных за решение вопросов назначения прав доступа к приложениям; определены входные, постоянные и выходные данные; рассмотрены функции и назначение отдельных компонентов проектируемого программного обеспечения; выполнен анализ существующих разработок, обзор имеющихся систем и выбор концепции программной реализации предложенного метода; произведен выбор СУБД и среды разработки пользовательского интерфейса; исследованы и обоснованы проектные решения.

В ходе программной реализации метода назначения прав доступа поэтапно описано проектиро-

вание базы данных, построена модель информационных потоков, рассмотрена физическая схема взаимодействия отдельных процедур, на основании которых создана база данных, разработан пользовательский интерфейс с формами, отображающими информацию, хранящуюся в БД. Формы обеспечивают возможность ввода, вывода данных, их редактирования, обработки и хранения данных о пользователях корпоративной мобильной сети (сотрудниках компании) и мобильных приложениях, с последующим назначением прав доступа сотрудникам к использованию приложений.

Список источников

1. Гнеушев В. А., Кравец А. Г., Козунова С. С., Бабенко А. А. Моделирование сетевых атак злоумышленников в корпоративной информационной системе // Промышленные АСУ и контроллеры. 2017. № 6. С. 51–60.

2. Буй Нгок Зыонг. Управление и анализ качества мобильного доступа к корпоративным информационным ресурсам: дис. … канд. техн. наук. Волгоград, 2017. 136 с.

3. Kravets A. G., Salnikova N. A., Mikhnev I. P., Orudjev N. Y., Poplavskaya O. V. Web Portal for Project Management in Electronics Design Software Development // 2019 International Seminar on Electron Devices Design and Production, SED 2019 – Proceedings (Prague, 23–24 апреля 2019 г.). Institute of Electrical and Electronics Engineers, 2019. P. 8798472.

4. Болотин П. Управление правами доступа в корпоративных Web-системах. URL: http://www.iksmedia.ru/articles/23910-Upravlenie-pravami-dostupa-v-korpor.html (дата обращения: 14.01.2022).

5. Kravets A., Salnikova N., Dmitrenko K., Lempert M. Industrial Cyber-Physical Systems: Risks Assessment and Attacks Modeling // Studies in Systems, Decision and Control. 2020. V. 260. C. 197–210.

6. Bolshakov A. A., Klyuchikov A. V. Decision Support System for Selecting Designs of Autostereoscopic Displays // Cyber-Physical Systems: Design and Application for Industry 4.0 (Studies in Systems, Decision and Control). 2021. V. 342. P. 73–88.

7. Kravets A. G., Skorobogatchenko D. A., Salnikova N. A., Orudjev N. Y., Poplavskaya O. V. The traffic safety management system in urban conditions based on the C4.5 algorithm // Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 – Proceedings (1, Moscow, 14–16 march 2018). Moscow, 2018. P. 1–7. DOI: 10.1109/MWENT.2018.8337254.

8. Kizim A. V., Matokhina A. V., Vayngolts I. I., Shcherbakov M. V. Intelligent Platform of Monitoring, Diagnosis and Modernization of Technical Systems at Various Stages of Life Cycle // Proceedings of the 5th International Conference on System Modeling and Advancement in Research Trends (SMART 2016). 2016. V. 5. P. 145–150.

9. Мобильные устройства в корпоративной сети: управление и контроль. URL: https://www.kaspersky.ru/blog/mobil-ny-e-ustrojstva-v-korporativnoj-seti-upravlenie-i-kontrol/14809/ (дата обращения: 14.01.2022).

10. Kravets A. G., Salnikova N. A., Shestopalova E. L. Development of a Module for Predictive Modeling of Technological Development Trends // Studies in Systems, Decision and Control. 2021. V. 350. P. 125–136.

11. Чан В. Ф., Щербаков М. В., Нгуен Т. А., Скоробогатченко Д. А. Метод сбора и слияния разнотипных данных в проактивных системах интеллектуальной поддержки принятия решений // Нейрокомпьютеры: разработка, применение. 2016. № 11. С. 40–44.

12. Котенко И. В., Паращук И. Б. Нечеткое управление информацией и событиями безопасности: особенности построения функций принадлежности // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2021. № 3. С. 7–15. DOI: 10.24143/2072-9502-2021-3-7-15.

13. Югансон А. Н., Заколдаев Д. А. Подход к оценке защищенности встроенного программного обеспечения в условиях нечеткости входной информации // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2020. № 1. С. 50–56. DOI: 10.24143/2072-9502-2020-1-50-56.

14. Нгуен Ле Тхань Тунг, Кравец А. Г., Буй Нгок Зьюнг. Анализ средств и моделей взаимодействия между компонентами в системе управления корпоративной мобильностью // Информационные технологии. 2018. Т. 24. № 1. С. 64–72.

15. Щербаков М. В., Groumpos P. P., Кравец А. Г. A Method and IR4I Index Indicating the Readiness of Business Processes for Data Science Solutions // Creativity in Intelligent Technologies and Data Science. Second Conference, CIT&DS 2017 (Volgograd, Russia, September 12-14, 2017): Proceedings / ed. by A. Kravets, M. Shcherbakov, M. Kultsova, Peter Groumpos. Germany: Springer International Publishing AG, 2017. Ser. Communications in Computer and Information Science. V. 754. P. 21–34.

16. Кравец А. Г., Сальникова Н. А. Разработка модуля назначения прав доступа к приложениям в корпоративной мобильной сети // Математические методы в технологиях и технике. 2022. № 8. С. 85–89. DOI: 10.52348/2712-8873_MMTT_2022_8_85.

17. Котенко И. В., Паращук И. Б. Модель системы управления информацией и событиями безопасности // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2020. № 2. С. 84–94. DOI: 10.24143/2072-9502-2020-2-84-94.

18. Нгуен Ле Тхань Тунг, Кравец А. Г., Буй Нгок Зьюнг. Организация сообщений на основе архитектуры «публикация/подписка» в системе управления корпоративной мобильностью // Вестн. компьютер. и информац. технологий. 2017. № 5 (155). С. 3–12. DOI: 10.14489/vkit.2017.05.pp.003-012.

19. Олейников А. А. Использование метода случайного леса в процессе оценки элементов инфокоммуникационных систем // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2019. № 2. С. 56–65. DOI: 10.24143/2072-9502-2019-2-56-65.

20. Fusion Middleware Administering Oracle Mobile Security Suite. URL: https://docs.oracle.com/cd/E52734_01/omss/MOBAD/toc.htm (дата обращения: 14.01.2022).

21. Сведения о группах и правах доступа в Azure Active Directory. URL: https://docs.microsoft.com/ru-ru/

azure/active-directory/fundamentals/active-directory-manage-groups (дата обращения: 14.01.2022).

22. Cisco DNA Center User Guide, Release 2.3.5. URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/user_guide/b_cisco_dna_center_ug_2_3_5/m_work-with-wireless-2d-and-3d-maps.html?dtid=osscdc000283 (дата обращения: 14.01.2022).

23. Google Workspace. URL: https://gsuite.google.com/features/ (дата обращения: 14.01.2022).

24. Федоренко В. В., Самойленко В. В., Алдущенко Д. В., Емельяненко И. В. Методика моделирования топологии беспроводных сенсорных сетей с учетом межузловых помех // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2020. № 3. С. 34–44. DOI: 10.24143/2072-9502-2020-3-34-44.

25. Королева А. Н. Инфологическая модель данных «сущность-связь». Основные понятия. URL: https://spravochnick.ru/bazy_dannyh/infologicheskaya_model_dannyh_suschnost-svyaz_osnovnye_ponyatiya/ (дата обращения: 14.01.2022).

References

1. Gneushev V. A., Kravets A. G., Kozunova S. S., Babenko A. A. Modelirovanie setevykh atak zloumyshlennikov v korporativnoi informatsionnoi sisteme [Modeling network attacks of intruders in corporate information system]. *Promyshlennye ASU i kontrollery*, 2017, no. 6, pp. 51-60.

2. Bui Ngok Zyong. *Upravlenie i analiz kachestva mobil'nogo dostupa k korporativnym informatsionnym resursam. Dissertatsiia ... kand. tekhn. nauk* [Management and analysis of quality of mobile access to corporate information resources. Diss.... Cand.Tech. Sci.]. Volgograd, 2017. 136 p.

3. Kravets A. G., Salnikova N. A., Mikhnev I. P., Orudjev N. Y., Poplavskaya O. V. *Web Portal for Project Management in Electronics Design Software Development. 2019 International Seminar on Electron Devices Design and Production, SED 2019 – Proceedings (Prague, 23–24 aprelia 2019 g.)*. Institute of Electrical and Electronics Engineers, 2019. P. 8798472.

4. Bolotin P. *Upravlenie pravami dostupa v korporativnykh Web-sistemakh* [Management of access rights in corporate Web systems]. Available at: http://www.iksmedia.ru/articles/23910-Upravlenie-pravami-dostupa-v-korpor.html (accessed: 14.01.2022).

5. Kravets A., Salnikova N., Dmitrenko K., Lempert M. Industrial Cyber-Physical Systems: Risks Assessment and Attacks Modeling. *Studies in Systems, Decision and Control*, 2020, vol. 260, pp. 197-210.

6. Bolshakov A. A., Klyuchikov A. V. Decision Support System for Selecting Designs of Autostereoscopic Displays. *Cyber-Physical Systems: Design and Application for Industry 4.0 (Studies in Systems, Decision and Control)*, 2021, vol. 342, pp. 73-88.

7. Kravets A. G., Skorobogatchenko D. A., Salnikova N. A., Orudjev N. Y., Poplavskaya O. V. The traffic safety management system in urban conditions based on the C4.5 algorithm. *Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 – Proceedings (1, Moscow, 14–16 march 2018 g.)*. Moscow, 2018. Pp. 1-7. DOI: 10.1109/MWENT.2018.8337254.

8. Kizim A. V., Matokhina A. V., Vayngolts I. I., Shcherbakov M. V. Intelligent Platform of Monitoring, Diagnosis and Modernization of Technical Systems at Various Stages of Life Cycle. *Proceedings of the 5th International Conference on System Modeling and Advancement in Research Trends (SMART 2016)*, 2016, vol. 5, pp. 145-150.

9. *Mobil'nye ustroistva v korporativnoi seti: upravlenie i kontrol'* [Mobile devices in the corporate network: management and control]. Available at: https://www.kaspersky.ru/blog/mobil-ny-e-ustrojstva-v-korporativnoj-seti-upravlenie-i-kontrol/14809/ (accessed: 14.01.2022).

10. Kravets A. G., Salnikova N. A., Shestopalova E. L. Development of a Module for Predictive Modeling of Technological Development Trends. *Studies in Systems, Decision and Control*, 2021, vol. 350, pp. 125-136.

11. Chan V. F., Shcherbakov M. V., Nguen T. A., Skorobogatchenko D. A. Metod sbora i sliianiia raznotipnykh dannykh v proaktivnykh sistemakh intellektual'noi podderzhki priniatiia reshenii [Method of collecting and merging heterogeneous data in proactive intelligent decision support systems]. *Neirokomp'iutery: razrabotka, primenenie*, 2016, no. 11, pp. 40-44.

12. Kotenko I. V., Parashchuk I. B. Nechetkoe upravlenie informatsiei i sobytiiami bezopasnosti: osobennosti postroeniia funktsii prinadlezhnosti [Fuzzy control of information and security events: features of construction of membership functions]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2021, no. 3, pp. 7-15. DOI: 10.24143/2072-9502-2021-3-7-15.

13. Iuganson A. N., Zakoldaev D. A. Podkhod k otsenke zashchishchennosti vstroennogo programmnogo obespecheniia v usloviiakh nechetkosti vkhodnoi informatsii [Approach to assessing security of embedded software under fuzzy input information]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2020, no. 1, pp. 50-56. DOI: 10.24143/2072-9502-2020-1-50-56.

14. Nguen Le Tkhan' Tung, Kravets A. G., Bui Ngok Zyong. Analiz sredstv i modelei vzaimodeistviia mezhdu komponentami v sisteme upravleniia korporativnoi mobil'nost'iu [Analysis of means and models of interaction between components in corporate mobility management system]. *Informatsionnye tekhnologii*, 2018, vol. 24, no. 1, pp. 64-72.

15. Shcherbakov M. V., Groumpos P. P., Kravets A. G. A Method and IR4I Index Indicating the Readiness of Business Processes for Data Science Solutions. *Creativity in Intelligent Technologies and Data Science. Second Conference, CIT&DS 2017 (Volgograd, Russia, September 12-14, 2017): Proceedings / ed. by A. Kravets, M. Shcherbakov, M. Kultsova, Peter Groumpos*. Germany: Springer International Publishing AG, 2017. Ser. Communications in Computer and Information Science. Vol. 754. Pp. 21-34.

16. Kravets A. G., Sal'nikova N. A. Razrabotka modulia naznacheniia prav dostupa k prilozheniiam v korporativnoi mobil'noi seti [Development of module for assigning access rights to applications in corporate mobile network]. *Matematicheskie metody v tekhnologiiakh i tekhnike,* 2022, no. 8, pp. 85-89. DOI: 10.52348/2712-8873_MMTT_2022_8_85.

17. Kotenko I. V., Parashchuk I. B. Model' sistemy upravleniia informatsiei i sobytiiami bezopasnosti [Model

of information and security event management system]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2020, no. 2, pp. 84-94. DOI: 10.24143/2072-9502-2020-2-84-94.

18. Nguen Le Tkhan' Tung, Kravets A. G., Bui Ngok Zyong. Organizatsiia soobshchenii na osnove arkhitektury «publikatsiia/podpiska» v sisteme upravleniia korporativnoi mobil'nost'iu [Organizing messages based on publish/subscribe architecture in enterprise mobility management system]. *Vestnik komp'iuternykh i informatsionnykh tekhnologii*, 2017, no. 5 (155), pp. 3-12. DOI: 10.14489/vkit.2017.05.pp.003-012.

19. Oleinikov A. A. Ispol'zovanie metoda sluchainogo lesa v protsesse otsenki elementov infokommunikatsionnykh sistem [Using random forest method in process of evaluating elements of infocommunication systems]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2019, no. 2, pp. 56-65. DOI: 10.24143/2072-9502-2019-2-56-65.

20. *Fusion Middleware Administering Oracle Mobile Security Suite.* Available at: https://docs.oracle.com/cd/E52734_01/omss/MOBAD/toc.htm (accessed: 14.01.2022).

21. *Svedeniia o gruppakh i pravakh dostupa v Azure Active Directory* [Information about groups and access rights in Azure Active Directory]. Available at: https://docs.microsoft.com/ru-ru/azure/active-directory/fundamentals/active-directory-manage-groups (accessed: 14.01.2022).

22. *Cisco DNA Center User Guide, Release 2.3.5.* Available at: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/2-3-5/user_guide/b_cisco_dna_center_ug_2_3_5/m_work-with-wireless-2d-and-3d-maps.html?dtid=osscdc000283 (accessed: 14.01.2022).

23. *Google Workspace.* Available at: https://gsuite.google.com/features/ (accessed: 14.01.2022).

24. Fedorenko V. V., Samoilenko V. V., Aldushchenko D. V., Emel'ianenko I. V. Metodika modelirovaniia topologii besprovodnykh sensornykh setei s uchetom mezhuzlovykh pomekh [Methods of modeling topology of wireless sensor networks taking into account internodal interference]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2020, no. 3, pp. 34-44. DOI: 10.24143/2072-9502-2020-3-34-44.

25. Koroleva A. N. *Infologicheskaia model' dannykh «sushchnost'-sviaz'». Osnovnye poniatiia* [Infological model of data 'entity-relationship'. Basic concepts]. Available at: https://spravochnick.ru/bazy_dannyh/infologicheskaya_model_dannyh_suschnost-svyaz_osnovnye_ponyatiya/ (accessed: 14.01.2022).

Статья поступила в редакцию 02.12.2022; одобрена после рецензирования 26.12.2022; принята к публикации 19.01.2023
The article is submitted 02.12.2022; approved after reviewing 26.12.2022; accepted for publication 19.01.2023

Информация об авторах / Information about the authors

Алла Григорьевна Кравец – доктор технических наук, профессор; профессор кафедры систем автоматизированного проектирования и поискового конструирования; Волгоградский государственный технический университет; профессор кафедры системного анализа и управления; Университет «Дубна»; AllaGKravets@yandex.ru

Наталия Анатольевна Сальникова – кандидат технических наук, доцент; доцент кафедры информационных систем и математического моделирования; Волгоградский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ; ns3112@mail.ru

Alla G. Kravets – Doctor of Sciences in Technology, Professor; Professor of the Department of Computer Aided Design and Exploratory Design Systems; Volgograd State Technical University; Professor of the Department of System Analysis and Control; Dubna State University; AllaGKravets@yandex.ru

Natalia A. Salnikova – Candidate of Sciences in Technology, Assistant Professor; Assistant Professor of the Department of Information Systems and Mathematical Modeling; Volgograd Institute of Management – branch of the Russian Academy Presidential Academy of National Economy and Public Administration; ns3112@mail.ru