Для цитирования: *Алферов В.П., Дровникова И.Г., Обухова Л.А., Рогозин Е.А. Вербальная модель управления слабо уязвимым процессом разграничения доступа пользователей к программным средствам системы электронного документооборота. Вестник Дагестанского государственного технического университета. Технические науки. 2019; 46 (2): 37-49. DOI:10.21822/2073-6185-2019-46-2-37-49*
For citation: *Alferov V.P., Drovnikova I.G., Obukhova L.A., Rogozin E.A. Verbal model of management of a vulnerable process of dedicating the access of users to the software of the electronic document system. Herald of Daghestan State Technical University. Technical Sciences. 2019; 46 (2): 37-49. (In Russ.) DOI:10.21822/2073-6185-2019-46-2-37-49*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 519.7: 004.05
DOI:10.21822/2073-6185-2019-46-2-37-49

ВЕРБАЛЬНАЯ МОДЕЛЬ УПРАВЛЕНИЯ СЛАБО УЯЗВИМЫМ ПРОЦЕССОМ РАЗГРАНИЧЕНИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ПРОГРАММНЫМ СРЕДСТВАМ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Алфёров В.П.[1], Дровникова И.Г.[2], **Обухова Л.А.[4],** ***Рогозин Е.А.[3]***
[1]Воронежский государственный технический университет,
[1]39402, г. Воронеж, Московский пр., 14, Россия,
[2-4]Воронежский институт МВД России,
[2-4]394065, г. Воронеж, пр. Патриотов, 53, Россия,
[1]e-mail:alferov_vladimir@mail.ru, [2]e-mail: idrovnikova@mail.ru,
[3]e-mail: evgenirogozin@yandex.ru, [4]e-mail: obuhova.lyudmila@bk.ru

Резюме. Цель. *Традиционные способы решения проблемы защиты информационного ресурса систем электронного документооборота, базирующиеся на защитных базовых функциях (идентификации, аутентификации и верификации пользователей и др.) имеющихся средств и подсистем информационной безопасности, обладают существенным недостатком — неэффективностью при овладении злоумышленником паролем штатных пользователей. С целью его устранения необходимо разработать новые методы, связанные с управлением слабо уязвимым процессом разграничения доступа пользователей не только к конфиденциальным сведениям, но и к программным средствам системы электронного документооборота.* ***Метод.*** *Одним из способов решения указанной проблемы является применение модифицированного метода «мягкого администрирования», заключающегося в автоматическом формировании списков разрешённых файлов-источников в матрице установления полномочий путём редуцирования списков и сравнения функций целостности файлов с эталонным перечнем для имеющегося пакета программных средств. Это позволяет автоматизировать процесс разработки правил разграничения доступа и обеспечить управление слабо уязвимым процессом разграничения доступа к программным средствам системы электронного документооборота.* ***Результат.*** *Разработана вербальная модель автоматизированного управления слабо уязвимым процессом разграничения доступа к программным средствам системы электронного документооборота и предложена система показателей эффективности функционирования перспективной подсистемы защиты конфиденциальных сведений, характеризующих её как объект управления.* ***Вывод.*** *Представленная вербальная модель предусматривает возможность распределённого управления, при котором администратор защиты непосредственно управляет указанным процессом с помощью удалённого программного средства. Формирование (изменение) матрицы установления полномочий при управлении слабо уязвимым процессом разграничения доступа с помощью перспективной подсистемы защиты конфиденциальных сведений и разработка системы показателей комплексной оценки эффективности её функционирования является одной из важнейших задач защиты информации от несанкционированного доступа, гарантирующей выполнение политики безопасности в течение всего времени эксплуатации защищённой системы электронного документооборота.*

Ключевые слова: *система электронного документооборота, подсистема защиты конфиденциальных сведений, защита информационного ресурса, несанкционированный доступ, разграничение доступа, политика безопасности, матрица установления полномочий*

COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

VERBAL MODEL OF MANAGEMENT OF A VULNERABLE PROCESS OF DEDICATING THE ACCESS OF USERS TO THE SOFTWARE OF THE ELECTRONIC DOCUMENT SYSTEM

Vladimir P. Alferov,[1] Irina G. Drovnikova[2], Lyudmila A. Obukhova[4], Evgenii A. Rogozin[3]
[1]Voronezh State Technical University,
[1]14 Moskovsky Ave., Voronezh 139402, Russia,
[2-4]Voronezh Institute of the Ministry of the Interior of the Russian Federation,
[2-4]53 Patriotov Str., Voronezh 394065, Russia,
[1]e-mail:alferov_vladimir@mail.ru, [2]e-mail: idrovnikova@mail.ru,
[3]e-mail: evgenirogozin@yandex.ru, [4]e-mail: obuhova.lyudmila@bk.ru

Abstract Objectives *Traditional methods for solving the problem of protecting the information resource of electronic document management systems based on protective basic functions (identification, authentication and verification of users, etc.) of available tools and information security subsystems have a significant drawback - inefficiency when an attacker masters the password of regular users. In order to eliminate it, it is necessary to develop new methods related to managing the weakly vulnerable process of delimiting user access not only to confidential information, but also to the software of the electronic document management system.* ***Method*** *One way to solve this problem is to use the modified "soft administration" method, which consists in automatically generating lists of allowed source files in the authorization matrix by reducing the lists and comparing file integrity functions with a reference list for an existing software package. This allows you to automate the process of developing access control rules and provide management of the weakly vulnerable process of access control to software tools of the electronic document management system.* ***Result*** *A verbal model is developed for automated control of a weakly vulnerable process of differentiating access to software tools of an electronic document management system, and a system of performance indicators for the functioning of a promising subsystem for protecting confidential information characterizing it as a control object is proposed.* ***Conclusion*** *The presented verbal model provides for the possibility of distributed control, in which the security administrator directly controls the specified process using a remote software tool. The formation (change) of the authority establishment matrix for managing a weakly vulnerable process of access control using a promising subsystem for protecting confidential information and the development of a system of indicators to comprehensively evaluate the effectiveness of its functioning is one of the most important tasks of protecting information from unauthorized access, guaranteeing the implementation of a security policy throughout the entire operation period secure electronic document management system.*

Keywords: *electronic document management system, confidential information protection subsystem, information resource protection, unauthorized access, access control, security policy, authority establishment matrix*

Введение. Широкое внедрение средств автоматизации различных сфер деятельности человека привело к стремительному развитию электронного документооборота, базирующегося на применении систем электронного документооборота (СЭД), функционирующих в многопользовательском режиме с информационными ресурсами (ИР) различного уровня конфиденциальности. Опыт эксплуатации и разработки СЭД в защищённом исполнении показал, что максимальный вклад в нарушение информационной безопасности (ИБ) данных систем вносят факты несанкционированного доступа (НСД) к их ИР [1 - 5].

Для решения задачи защиты ИР (ЗИР) от НСД в многопользовательских СЭД создаётся подсистема защиты конфиденциальных сведений (ПЗКС) — функциональная подсистема СЭД, организованная как совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) в СЭД для решения задач ЗИР от НСД [6]. Одной из основных функций ПЗКС является разграничение доступа (РД) пользователей и их процессов к ИР СЭД в соответствии с предоставленными им полномочиями. Оно осуществляется с помощью подсистемы РД, одной из ключевых подсистем, входящих в ПЗКС [7]. РД к ИР заключается в

разделении информации, циркулирующей в СЭД, на части и организации доступа к конфиденциальным сведениям (КС) и программным средствам (ПСр) пользователей соответственно их функциональными обязанностям и полномочиям. Указанная функция ПЗКС реализуется с целью защиты КС от нарушителей среди допущенных в систему пользователей в процессе их работы в СЭД.

Для поддержания политики безопасности (ПБ) защищаемой СЭД (интегральной характеристики, описывающей свойства защищённости системы) во времени в условиях постоянно изменяющейся её программной среды (программная среда дополняется новыми компонентами: ПСр, файлами данных, различными процедурами и т.д.) необходимо в процесс защиты информации (ЗИ) перспективной СЭД добавить процедуры управления безопасностью информации СЭД. Проблема управления безопасностью является весьма важной для выполнения ПБ в течение всего времени эксплуатации защищённой СЭД [8 -14].

Постановка задачи. Основные процедуры разработки слабо уязвимого процесса РД к ИР СЭД сводятся к разработке моделей автоматизированного управления РД к их КС, обеспечивающих учёт всех связей и зависимостей, существующих в матрице установления полномочий (МП), и автоматизированного управления РД к ПСр, обеспечивающих включение в состав программной среды СЭД только корректных ПСр. Кроме того, для оценки эффективности функционирования ПЗКС при реализации слабо уязвимого процесса РД к ИР СЭД необходимо сформировать систему показателей оценки эффективности и разработать модели, алгоритмы и программные средства комплексной оценки эффективности функционирования ПЗКС, учитывающие аспекты управления подсистемой РД [15-16].

На основе анализа задач и основных этапов слабо уязвимого процесса РД к ИР СЭД разработана общая структурная схема методического обеспечения автоматизированного управления этим процессом, представленная на рис. 1.

Для повышения защищённости СЭД предлагается реализовать слабо уязвимый процесс РД к ИР СЭД путём автоматизации формирования МП, хранящей информацию о множестве потоков информации легального доступа и множестве файлов-источников для порождения разрешённых ПСр.

Для этого разрабатываются вербальная модель [17] и алгоритм управления РД пользователей, их программ и процессов к КС СЭД (задачи 1 и 3 на рис. 1 соответственно), а также вербальная модель и алгоритм управления РД пользователей к ПСр СЭД (задачи 2 и 4 на рис. 1 соответственно).

Для оценки эффективности функционирования ПЗКС и мероприятий по совершенствованию ЗИР разрабатывается программно-методический комплекс оценки эффективности функционирования ПЗКС в СЭД. С этой целью формируется система показателей эффективности функционирования ПЗКС как объекта управления (ОУ) РД (задача 6 на рис. 1).

Для моделирования количественного показателя эффективности функционирования ПЗКС разрабатывается математическая модель динамики функционирования ПЗКС в СЭД как системе массового обслуживания (задача 5 на рис. 1). Для методического обеспечения комплексной оценки эффективности функционирования ПЗКС разрабатываются математические модели оценки количественного и комплексного показателей (задачи 7 и 8 на рис. 1 соответственно). Далее создаются алгоритмы оценки количественного и комплексного показателей эффективности функционирования ПЗКС (задачи 9 и 10 на рис. соответственно), позволяющие разработать программные комплексы для их оценки. Для апробации методического обеспечения оценки эффективности функционирования ПЗКС в СЭД разрабатывается программное обеспечение (ПО) комплексной оценки эффективности функционирования ПЗКС как ОУ РД (задача 11 на рис. 1) и проводится исследование эффективности её функционирования (задача 12 на рис. 1).

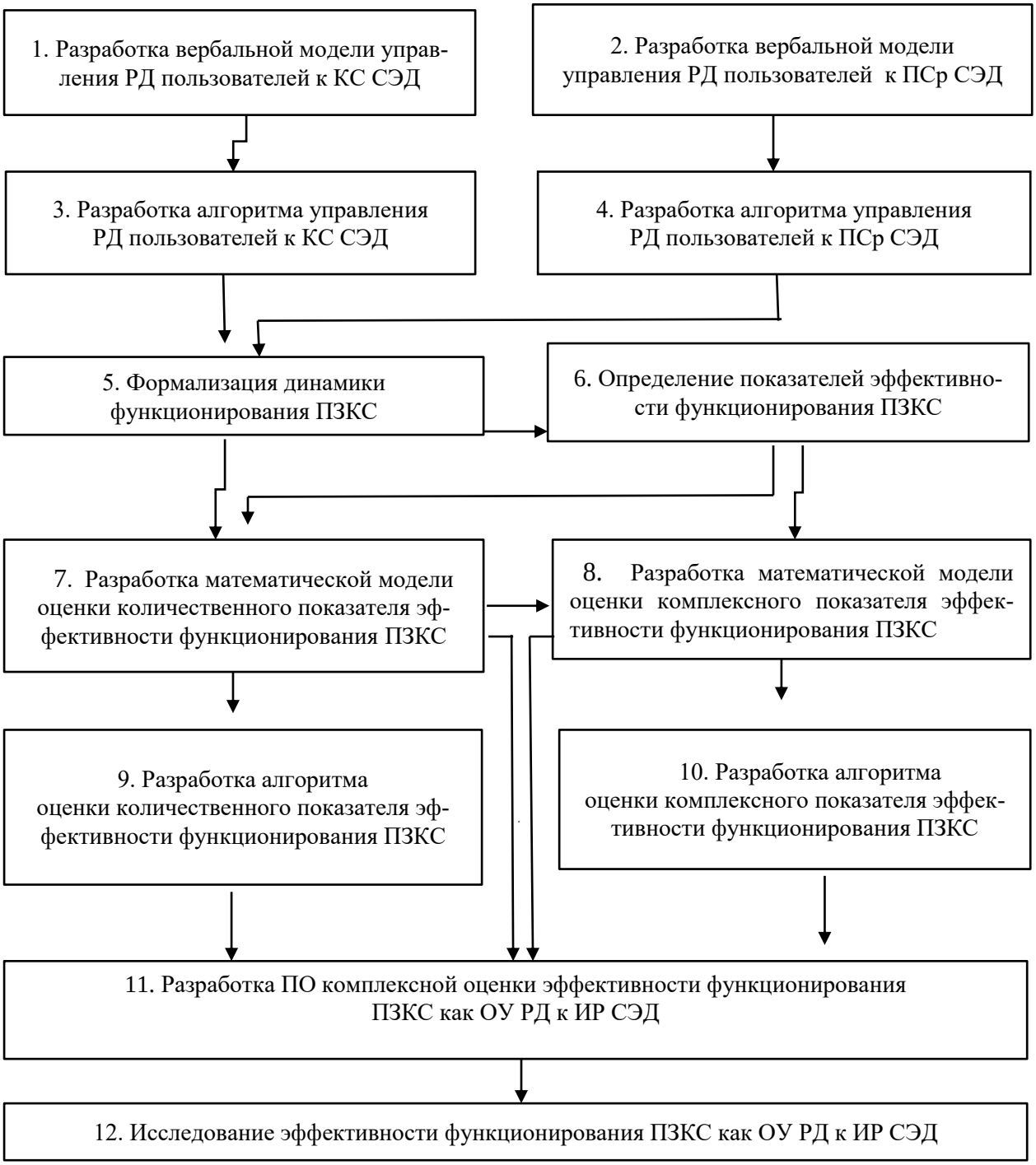

Рис. 1. Общая структурная схема методического обеспечения автоматизированного управления слабо уязвимым процессом разграничения доступа к информационными ресурсами систем электронного документооборота

Fig. 1. The general structural diagram of the methodological support for the automated management of a weakly vulnerable process of delimiting access to information resources of electronic document management systems

Как показывает общая структурная схема, представленная на рис. 1, одной из важнейших задач управления слабо уязвимым процессом РД к ИР СЭД является разработка вербальной модели управления РД к ПСр СЭД, чему и посвящена данная статья.

Доступ пользователей к ПСр СЭД организуется в соответствии с установленными правилами РД (ПРД), базирующимися на идентификации пользователей по одному или нескольким параметрам аутентификации [18 - 21]. Для осуществления ПРД и выполнения РД пользователя, прошедшего идентификацию, к ПСр СЭД в памяти ЭВМ формируются и хранятся МП, описывающие профили РД каждого пользователя, устройства, программы, процесса и т.д. Уровень доступа к ПСр СЭД соответствует МП и содержит информацию, определяющую порядок организации взаимодействия пользователей, устройств, программ, процессов с СЭД. Кроме таблиц полномочий системой РД определяются время доступа и свойства электронных документов (возможность согласования, применения санкций или наложения резолюции руководства и т.д.).

Управление РД пользователей к ПСр СЭД (управление подсистемой РД) осуществляется с помощью средств ПЗКС и заключается в формировании и изменении файлов МП, содержащих сведения о наборе файлов-источников, необходимых для порождения разрешённых ПСр в соответствии с текущим состоянием ИР СЭД и пользователей. Очевидно, что для обеспечения слабо уязвимого процесса РД к ИР СЭД управление формируется таким образом, чтобы ПБ при преобразованиях МП не нарушалась (т.е. в МП не включались бы файлы-источники некорректных ПСр).

Формирование и изменение МП осуществляется администратором безопасности с помощью ПСр управления (ПСрУ), относящегося к ПЗКС. Система ПСрУ инициирует обмен данными между своими ассоциированными файлами и МП. Права на активирование и администрирование системы ПСрУ предоставляются только администратору СЭД. Корректность управления РД соблюдается, когда разрешённый доступ к МП на запись инициируется только ПСрУ. Для ПСр ЗИР, входящих в состав ПЗКС и непосредственно осуществляющих контроль за процессами порождения разрешённых ПСр в СЭД, предоставляется доступ на чтение к МП. Это позволяет производить поиск файлов-источников и создание на основе найденных в МП эталонов разрешённых ПСр для каждого идентифицированного пользователя.

Дезорганизация корректного управления РД возможна при инициировании некорректного ПСр и вмешательстве некорректного ПСр в процесс функционирования СЭД. Такой процесс аналогичен внесению изменений (редактированию) в МП файла-источника. Следовательно, для гарантированного обеспечения ПБ СЭД целесообразно создание и использование программной среды, исключающей возможность появления в ней некорректного ПСр.

В реальных СЭД практически невозможно поддерживать состояние корректного управления вследствие необходимости регулярного обновления и внесения дополнений в ПСр к программной среде СЭД. В то же время включение в программную среду СЭД комплекса (пакета) ПСр, содержащего некорректное ПСр, противоречит задаче поддержания гарантий заданной ПБ. Таким образом, при администрировании заданной ПБ следует пополнять программный интерфейс СЭД исключительно ПСр, непротиворечащими (корректными) существующим в данной программной среде.

Вместе с тем возможны случаи, когда из-за отсутствия описания какого-либо файла-источника в МП управление и контроль активации ПСр, входящего в состав некоторого программного комплекса, не зависят от администратора. Следовательно, недостатки представления эталонных файлов-источников в МП ПСр ЗИР не позволяют применить порождаемое ПСр, что, несомненно, оказывает влияние на пользовательские свойства СЭД.

Чтобы предотвратить возможное возникновение такого рода ошибок в перечень разрешённых к исполнению файлов-источников целесообразно включать все исполняемые файлы (программные средства). Однако такой подход может привести к избыточной (чрезмерной) защищённости сервиса [21], заключающейся в появлении в процессе добавления в перечень файлов-источников МП файлов, порождённых программной средой и содержащих

разнообразные инструментальные возможности, деструктивно влияющие на СЭД и способные нарушить её корректное межпрограммное функционирование.

Методы исследования. Для решения указанной выше проблемы предлагается использовать метод автоматизированного построения перечня разрешённых файлов-источников в МП. Такой подход является одним из вариантов «мягкого администрирования» [22], заключающегося в отслеживании всех случаев порождения ПСр. В процессе отслеживания в отдельном файле фиксируются все файлы-источники, то есть формируется перечень (список) для проведения «мягкого администрирования». Затем администратор защиты выполняет следующие процедуры:

– осуществляет сортировку файлов-источников (для выявления и удаления повторяющихся);

– осуществляет проверку фактического наличия файлов-источников в СЭД и в случае обнаружения имён несуществующих файлов удаляет эти имена;

– исключает из перечня файлы-источники, порождающие ПСр, имеющие заведомо некорректные свойства (служебные, отладочные средства и т.д.).

По итогам реализации данных процедур администратор формирует перечень файлов-источников, пригодных для использования в процессе формирования МП ПСр ЗИР. Однако такой подход не пригоден для случаев, когда необходимо внести изменения в МП в процессе эксплуатации системы. Причина заключается в возможности нахождении среди пользователей СЭД злоумышленника, имеющего представление о порядке организации защиты с использованием метода «мягкого администрирования». Положим, такой осведомлённый пользователь-злоумышленник в состоянии осуществить НСД к системе и в отрезок времени от снятия перечня «мягкого администрирования» до формирования МП подменить некий файл-источник на другой файл с целью порождения некорректного ПСр. Регистрация такого замаскированного файла в МП приведёт к нарушению условия изолированности среды.

Рассмотренного в примере недостатка не имеет модифицированный метод «мягкого администрирования» [22], применяемый для управления слабо уязвимым процессом РД (изменения МП) при эксплуатации СЭД. Применение данного метода возможно в случае существования эталонного списка файлов-источников для некоторого программного модуля. Основа модифицированного метода заключается вычислении администратором хэш-функции файлов-источников. При регистрации файла-источника в МП последовательно реализуется следующий алгоритм:

– осуществляется проверка на принадлежность файла-источника эталонному списку. При положительном результате проверки — переход к следующему пункту, в противном случае файл пропускается;

– проводятся вычисление хэш-функции файла-источника в реальном времени и проверка на совпадение полученных результатов с вычислениями администратора. При соответствии полученных результатов — переход к следующему пункту, в противном случае файл пропускается;

– формируется файл «СПИСОК», в который заносятся сведения о файлах-источниках для пополнения МП.

Данный метод, с одной стороны, сохраняет заданную ПБ в СЭД при попадании в программную среду сервиса множества файлов-источников, предназначенных для порождения ПСр. И наоборот, описанные в файле «СПИСОК» файлы-источники гарантируют реализацию полномасштабного пользовательского функционала сервиса. Отметим, что использование модифицированного метода «мягкого администрирования» позволит администратору, отвечающему за безопасность системы, выполнять только процедуры редуцирования (выявление и удаление повторяющихся записей) перечня и проверки соответствия вычисленной в реальном времени хэш-функции файла-источника с эталонным (контроль целостности). Также реализация модифицированного метода «мягкого администрирования»

позволит автоматизировать процесс составления ПРД, что несомненно говорит о ценности описанного выше подхода.

Обсуждение результатов. Порядок формирования (изменения) МП, содержащей описание файлов-источников, необходимых для порождения ПСр, зависит от локализации ПСрУ в СЭД релятивно пользователя. Для случаев, когда ПСрУ принадлежит локальному сегменту (ЛС) СЭД (в смысле принадлежности множеству ПСр ЗИР ЛС СЭД), управление следует считать локальным, а если внешнему сегменту СЭД — удалённым.

При локальном управлении слабо уязвимым процессом РД пользователей к ПСр СЭД (ПСрУ принадлежит ЛС СЭД) формирование (изменение) МП, содержащее описание файлов-источников, необходимых для порождения ПСр, проводится следующим образом. Для всех пользователей сервиса формируются перечни допустимых и необходимых файлов-источников. Для этого выполняется стенографирование используемых файлов-источников, достаточных для инициирования и порождения, разрешённых ПСр для конкретного пользователя. Такое протоколирование осуществляется ПСр ЗИР ЛС под управлением локального ПСрУ.

В процессе протоколирования формируется файл, содержащий полный перечень разрешённых файлов-источников, включая также полные имена локальных файлов-источников и их хэш-функции, для каждого пользователя соответственно. Перед формированием файлов окончательного списка для каждого пользователя осуществляется контроль целостности входящих в эталонный перечень файлов-источников ЛС за счёт вычисления их хэш-функций. Допускается зависимость хэш-функции от коэффициента пользователя, но в таком случае администратор должен располагать значениями этого коэффициента для всех пользователей СЭД.

В случае несоответствия вычисленного в реальном времени хеш-значения эталонному проверяемый на достоверность файл-источник редуцируется из перечня. В итоге формируются файлы результирующего перечня разрешённых и используемых файлов-источников для каждого пользователя СЭД, на основе которых с помощью локального ПСрУ формируется (изменяется) локальная МП.

Особенностью формирования (изменения) МП, содержащей описание файлов-источников, необходимых для порождения ПСр при удалённом управлении слабо уязвимым процессом РД (ПСрУ принадлежит внешнему сегменту СЭД), является транспортировка файлов исходного списка во внешний сегмент с целью уменьшения возможных каналов НСД к файлам ЛС. При этом с помощью процедуры протоколирования также составляются списки разрешённых для каждого пользователя СЭД и используемых файлов-источников. Процедура создания и содержание файлов списков файлов-источников для каждого пользователя СЭД аналогична рассмотренной выше. Созданные в ЛС файлы исходного списка файлов-источников для каждого пользователя СЭД передаются в доступный администратору внешний сегмент при помощи локального ПСр ЗИР.

После передачи файлов перечней во внешний сегмент осуществляется контроль целостности включённых в него файлов-источников ЛС, в результате которого формируются файлы итогового перечня разрешённых и используемых файлов-источников для каждого пользователя СЭД. Процедуры проверки целостности файлов-источников и формирования файла окончательного списка аналогичны рассмотренным выше. Файлы окончательного списка разрешённых и используемых файлов-источников для каждого пользователя СЭД могут изменяться только локальным ПСр ЗИР. На основе этих файлов с помощью удалённого ПСрУ формируется (изменяется) МП.

При распределённом управлении слабо уязвимым процессом РД с помощью двух ПСрУ — локального и удалённого, администратор управляет защитой со своего рабочего места, которое является внешним сегментом СЭД относительно пользователя. При этом администратор защиты непосредственно управляет РД с помощью удалённого ПСрУ, которое имеет канал управления локальным ПСрУ и доступность удалённой МП (в случае её использования). Тогда возможна коррекция прав пользователя (сводящаяся к коррекции МП)

во время начала работы пользователя в системе. Доступ администратора к ресурсам ЛС СЭД осуществляется через локальное ПСрУ и технически легко реализуемо. Особенность формирования (изменения) МП, содержащей описание файлов-источников, необходимых для порождения ПСр при распределённом управлении слабо уязвимым процессом РД, заключается в том, что оно зависит от локализации элементов МП и в общем случае представляет собой функциональное объединение рассмотренных выше конфигураций управления.

На основе анализа особенностей функционирования различных конфигураций управления РД составим схему управления слабо уязвимым процессом РД с помощью перспективной ПЗКС при РД пользователей к ПСр СЭД. В качестве перспективной СЭД примем распределённую СЭД, в которой управление осуществляется с места администратора, а объект управления находится на общем ресурсе хранения (файл-сервере) [6]. Особенность управления РД данной конфигурации приведена выше. Управление слабо уязвимым процессом РД перспективной ПЗКС СЭД заключается в формировании (изменении) МП, содержащей описание используемых файлов-источников, необходимых для порождения разрешённых ПСр, для пользователей СЭД. Блок-схема модели автоматизированного управления слабо уязвимым процессом РД к ПСр СЭД с точки зрения описания файлов-источников приведена на рис. 2.

Данная схема носит наиболее общий характер и обеспечивает возможность распределённого управления слабо уязвимым процессом РД, когда администратор защиты непосредственно управляет РД при помощи удалённого ПСрУ, имеющего канал управления локальным ПСрУ и доступ к удалённой МП.

При этом управление ПСр ЗИР (ПСр протоколирования, транспортировки и т.д.) и доступ к ресурсам ЛС СЭД осуществляется администратором через локальное ПСрУ. При удалённом управлении администратор имеет доступ к информации о файлах-источниках ЛС только из файла «СПИСОК*», хранящегося во внешнем сегменте СЭД, доступном администратору с помощью удалённого ПСрУ.

Актуальной задачей, требующей эффективного решения для обеспечения выполнения заданной ПД в процессе эксплуатации СЭД в защищённом исполнении, является комплексная оценка эффективности функционирования ПЗКС как ОУ слабо уязвимым процессом РД пользователей к ИР СЭД. Важность указанной задачи подтверждается требованиями стандарта ГОСТ Р ИСО/МЭК 15408-2-2013 [23] и Руководящих документов Гостехкомиссии России [24-28]. Анализ использования существующих показателей оценки эффективности функционирования ПЗКС применительно к специфике организации управления процессами ЗИР в СЭД показывает их неадекватность реальным свойствам ПЗКС как ОУ слабо уязвимым процессом РД [6].

Для оценки изменения эффективности функционирования ПЗКС при реализации слабо уязвимого процесса РД к ИР СЭД необходимо сформировать систему показателей комплексной оценки эффективности функционирования ПЗКС, учитывающую специфику управления подсистемой РД.

Для решения указанной задачи предлагается использовать систему показателей эффективности функционирования ПЗКС [6].

Под системой показателей эффективности функционирования ПЗКС при управлении слабо уязвимым процессом РД к ИР СЭД понимается совокупность показателей, в полной мере количественно выражающая пригодность ПЗКС при заданных параметрах её функционирования в данной СЭД удовлетворять предъявляемым к ней требованиям в заданной ситуации. Структурная схема предлагаемой системы показателей представлена на рис. 3. Система имеет иерархическую структуру, в соответствии с которой все показатели делятся на комплексный (нулевой) показатель и элементарные показатели (показатели 1 - 3), определяющие количественные значения для соответствующих характеристик эффективности функционирования ПЗКС.

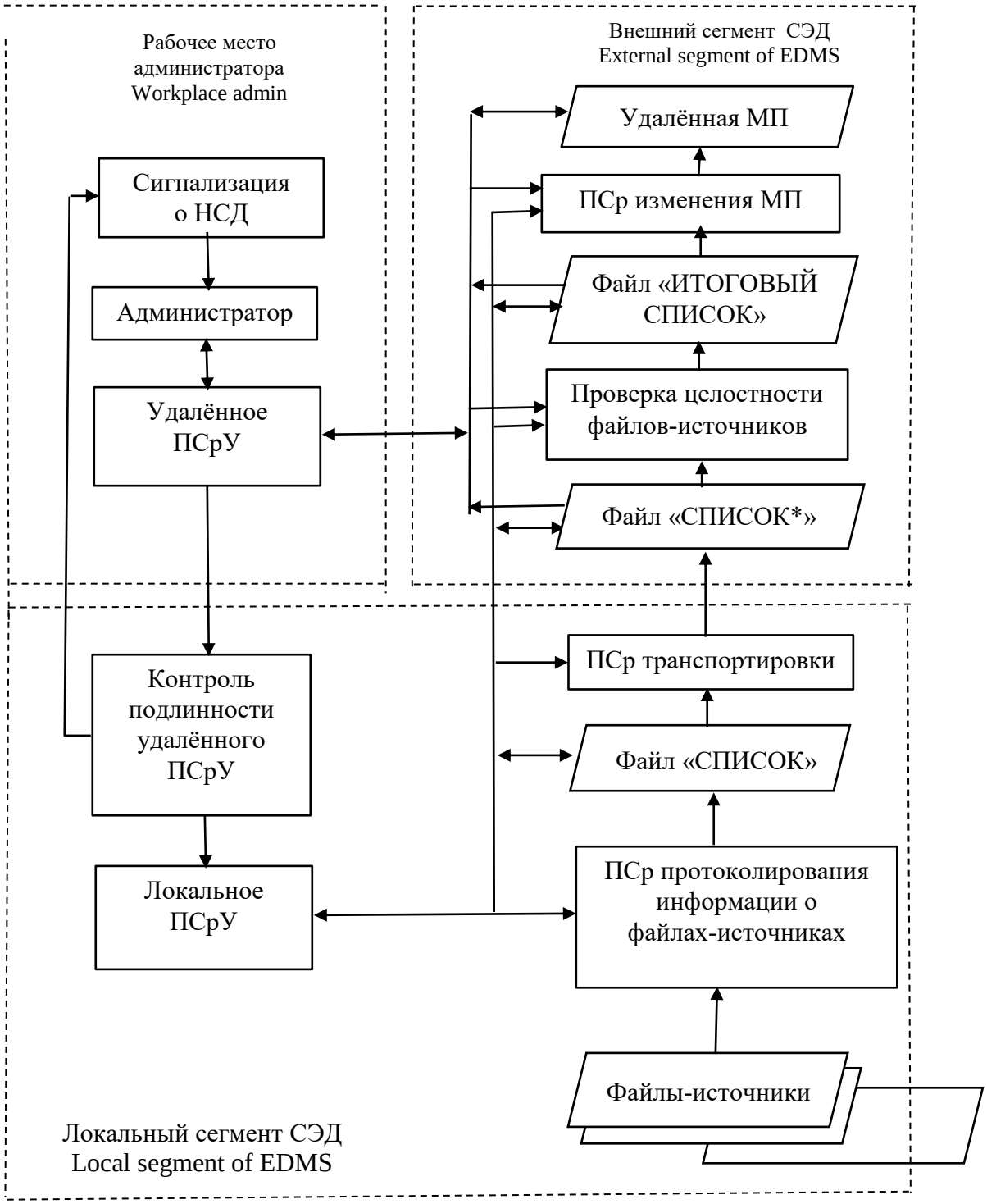

Рис. 2. Блок-схема вербальной модели автоматизированного управления слабо уязвимым процессом разграничения доступа к программным средствам систем электронного документооборота

Fig. 2. The block diagram of the verbal model of automated control of a weakly vulnerable process of differentiating access to software tools of electronic document management systems

Предлагается ввести следующие характеристики эффективности функционирования ПЗКС: функциональная защищённость, своевременность реализации ЗИР и эксплуатируемость. Основной из указанных характеристик является функциональная защищённость, определяющая возможность ПЗКС при установленных параметрах функционирования поддерживать достаточный уровень ИБ в СЭД.

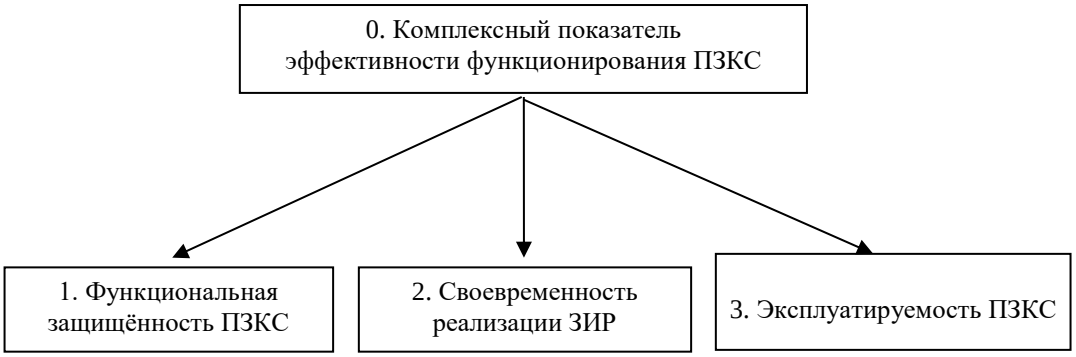

Рис. 3. Структурная схема показателей эффективности функционирования подсистемы защиты конфиденциальных сведений
Fig. 3. The structural diagram of performance indicators of the subsystem for protecting confidential information

Указанные характеристики при необходимости оцениваются количественными показателями, которые в дальнейшем можно использовать для комплексной оценки эффективности функционирования ПЗКС как ОУ слабо уязвимым процессом РД в СЭД.

Вывод. Предложена реализация управления слабо уязвимым процессом РД к ИР СЭД путём автоматизации формирования МП, хранящей информацию о множестве файлов-источников, необходимых для порождения разрешённых ПСр в соответствии с текущим состоянием ИР СЭД и пользователей.

Разработана вербальная модель автоматизированного управления слабо уязвимым процессом РД пользователей к ПСр перспективной СЭД, предусматривающая возможность распределённого управления, при котором администратор защиты непосредственно управляет указанным процессом с помощью удалённого ПСрУ, имеющего канал управления локальным ПСрУ и доступ к удалённой МП.

Обеспечение формирования (изменения) МП для штатных пользователей при управлении слабо уязвимым процессом РД с помощью перспективной ПЗКС СЭД, а также разработка системы показателей комплексной оценки эффективности функционирования ПЗКС, учитывающих специфику управления подсистемой РД, является одной из важнейших задач защиты информации от НСД пользователей в процессе их работы в защищённой СЭД, гарантирующей выполнение ПБ в течение всего периода эксплуатации системы.

Библиографический список:

1.Шаньгин В.Ф. Защита информации в компьютерных системах и сетях: учеб. пособие / В.Ф. Шаньгин. — М.: ДМК Пресс, 2012. 592 с.

2. Методы и средства оценки защищённости автоматизированных систем органов внутренних дел: монография [Электронный ресурс] / Е.А. Рогозин [и др.]; под ред. проф. Е.А. Рогозина. — Воронеж: Воронеж. ин-т МВД России, 2017. 88 с.

3.Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота: монография / И.И. Застрожнов [и др.]. — Воронеж: Воронеж. гос. техн. ун-т, 2015. 106 с.

4. Авсентьев О.С. Методика управления защитой информационного ресурса системы электронного документооборота / О.С. Авсентьев, И.Г. Дровникова, И.И. Застрожнов, А.Д. Попов, Е.А. Рогозин // Труды СПИИРАН. № 2 (57) (2018). С.-Пб.: СПИИРАН, 2018. 2018. № 2(57). С. 188-210. DOI 10.15622/sp.57.8.

5. Дровникова И.Г. Вербальная модель управления разграничением доступа пользователей к конфиденциальным сведениям систем автоматизированного документооборота / И.Г. Дровникова, В.П. Алфёров // Охрана, безопасность, связь — 2017: сб. ст. Междунар. науч.-практич. конф. В. 3. Ч. 3. (Воронеж, 16 ноября 2017 г.). Воронеж: ВИ МВД России, 2018. С. 77-80.

6. Дровникова И.Г. Концептуальная модель управления защитой информационного ресурса системы электронного документооборота / И.Г. Дровникова, И.И. Застрожнов, Е.А. Рогозин // Вестник Воронежского института МВД России. 2016. № 2. С. 147-154.

7.Застрожнов И.И. Методологические основы безопасности использования информационных технологий в системах электронного документооборота: монография / И.И. Застрожнов, Е.А. Рогозин, М.А. Багаев. — Воронеж: ИПЦ «Научная книга», 2011. 252 с.

8. Дровникова И.Г. Методика проектирования систем информационной безопасности в автоматизированных системах [Электронный ресурс] / И.Г. Дровникова, А.А. Никитин, Е.А. Рогозин // Интернет-журнал «Технологии техносферной безопасности». 2016. Выпуск № 4 (68) (август). http:// ipb.mos.ru/ttb/2016-4.

9. Дровникова И.Г. Разработка метода «мягкого администрирования» для организации управления подсистемой разграничения доступа в автоматизированных системах / И.Г. Дровникова, Д.А. Кабанов // Вестник Воронежского института МВД России. 2014. № 4. С. 269-276.

10. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. М.: ГЛТ, 2016. 586 с.

11. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры: учеб. пособие / А.А. Малюк М.: Горячая линия — Телеком, 2018. 314 с.

12. Бабаш А.А. Актуальные вопросы защиты информации: монография / А.А. Бабаш [и др.]. — М.: Риор, 2017. 111 с.

13. Даниленко А.В. Безопасность систем электронного документооборота. Технология защиты электронных документов / А.В. Даниленко. М.: Ленанд, 2015. 232 с.

14. Марков А.С. Методы оценки несоответствия средств защиты информации / А. С. Марков [и др.]. — М.: Радио и связь, 2012. 192 с.

15. Xiao Y. Handbook of security and neyworks / Y. Xiao [and others]. — Word Scientific Pub Co Inc. 1 edition, 2012. 576 p.

16. Schaefer R. Information Theoretic Security and Privacy of Information Systems / R. Schaefer. — Cambridge University Press, 2017. — 574 p.

17. Sheikh F. Circuits and Systems for Security and Privacy / F. Sheikh [and others]. — CRC Press, 2016. — 400 p.

18. Fields B. Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution / B. Fields. IGI Global, 2018. 648 p.

19. Rudra B. Flexible Network Architectures Security: Issues and Principles / B. Rudra. — Auerbach Publications, 2018. 326 p.

20. Klaic A. Conceptual Modeling of Information Systems within the Information Security Policies / A. Klaic, M. Golub // Journal of Economics / Business and Management. 2013. vol. 1. Issue 4. P. 371-376.

21. Nazareth D. System dynamics model for information security management / D. Nazareth, J. Choi // Information & Management. 2015. Vol. 52. Issue 1. P. 123-134.

22. Рогозин Е.А. Модель функционирования типовой системы защиты информации от несанкционированного доступа в автоматизированных информационных системах ОВД / Е.А. Рогозин, А.Д. Попов // Вестник Воронежского института МВД России. 2016. № 4. С. 122-132.

23. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные компоненты безопасности. [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200105710 (дата обращения 23.11.2018).

24. Защита от несанкционированного доступа к информации. Термины и определения: руководящий документ // сб. руководящих. докум. по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте Российской Федерации. М.: Росс. инженер. Академия, 1998. С. 5-14.

25. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: руководящий документ // сб. руководящих. докум. по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте Российской Федерации. М.: Росс. инженер. Академия, 1998. С. 15-21.

26. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: руководящий документ // сб. руководящих. докум. по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте Российской Федерации. М.: Росс. инженер. Академия, 1998. С. 22-51.

27. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации: руководящий документ // сб. руководящих. докум. по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте Российской Федерации. М.: Росс. инженер. Академия, 1998. С. 52-71.

28. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники: руководящий документ // сб. руководящих. докум. по защите информации от несанкционированного доступа Государственной технической комиссии при Президенте Российской Федерации. — М.: Росс. инженер. Академия, 1998. С. 72-92.

References:

1. Shan'gin V.F. Zashchita informatsii v komp'yuternykh sistemakh i setyakh: ucheb. posobiye / V.F. Shan'gin. — M.: DMK Press, 2012. 592 s. [Shangin V.F. Information Protection in computer systems and networks: proc. benefit / V.F. Shangin. — M.: DMK Press, 2012. 592 p. (in Russ)].
2. Metody i sredstva otsenki zashchishchonnosti avtomatizirovannykh sistem organov vnutrennikh del: monografiya [Elektronnyy resurs] / Ye.A. Rogozin [i dr.]; pod red. prof. Ye.A. Rogozina. — Voronezh: Voronezh. in-t MVD Rossii, 2017. 88 s. [Methods and tools for assessing the security of automated systems of bodies of internal Affairs: monograph [Electronic resource] / E.A. Rogozin [and others]; under the editorship of Professor E.A. Rogozin. Voronezh: Voronezh. Ministry of internal Affairs of Russia, 2017. 88 p. (in Russ)].
3. Metody i sredstva otsenki effektivnosti podsistemy zashchity konfidentsial'nogo informatsionnogo resursa pri yeyo proyektirovanii v sistemakh elektronnogo dokumentooborota: monografiya / I.I. Zastrozhnov [i dr.]. — Voronezh: Voronezh. gos. tekhn. un-t, 2015. 106 s. [Methods and means of assessing the effectiveness of the subsystem of protection of confidential information resource in its design in electronic document management systems: monograph / I.I. Zastrozhnov [and others]. Voronezh: Voronezh. state tech. UN-t, 2015. 106 p. (in Russ)].
4. Avsent'yev O.S. Metodika upravleniya zashchitoy informatsionnogo resursa sistemy elektronnogo dokumentooborota / O.S. Avsent'yev, I.G. Drovnikova, I.I. Zastrozhnov, A.D. Popov, Ye.A. Rogozin // Trudy SPIIRAN. № 2 (57) (2018). S.-Pb.: SPIIRAN, 2018. 2018. № 2(57). S. 188-210. DOI 10.15622/sp.57.8. [Avxentiev O.S. The management of protection

information resource electronic document management system / O.S. Avxentiev, I.G. Drovnikova, I.I. Zastrozhnov, A.D. Popov, E.A. Rogozin // Proceedings of SPIIRAS. № 2 (57) (2018). S.-Pb.: Spiran, 2018. 2018. № 2 (57). P. 188-210. DOI 10.15622 / sp.57.8 (in Russ)].

5. Drovnikova I.G. Verbal'naya model' upravleniya razgranicheniyem dostupa pol'zovateley k konfidentsial'nym svedeniyam sistem avtomatizirovannogo dokumentooborota / I.G. Drovnikova, V.P. Alforov // Okhrana, bezopasnost', svyaz' — 2017: sb. st. Mezhdunar. nauch.-praktich. konf. V. 3. CH. 3. (Voronezh, 16 noyabrya 2017 g.). Voronezh: VI MVD Rossii, 2018. S. 77-80. [Drovnikova I.G. Verbal control model differentiation of user access to confidential information of automated document management / I.G. Drovnikova, P.V. Alferov // Protection, security, communications — 2017: collection of articles]. scientific-practical conf. V. 3. Part 3. (Voronezh, 16 November 2017). Voronezh: VI Ministry of internal Affairs of Russia, 2018. P. 77-80 (in Russ)].
6. Drovnikova I.G. Kontseptual'naya model' upravleniya zashchitoy informatsionnogo resursa sistemy elektronnogo dokumentooborota / I.G. Drovnikova, I.I. Zastrozhnov, Ye.A. Rogozin // Vestnik Voronezhskogo instituta MVD Rossii. 2016. № 2. S. 147-154. [Drovnikova I.G. A conceptual model for managing information resource of an electronic document management system / I.G. Drovnikova, I.I. Zastrozhnov, E.A. Rogozin // Bulletin of Voronezh Institute of MIA Russia. 2016. № 2. P. 147-154 (in Russ)].
7. Zastrozhnov I.I. Metodologicheskiye osnovy bezopasnosti ispol'zovaniya informatsionnykh tekhnolo-giy v sistemakh elektronnogo dokumentooborota: monografiya / I.I. Zastrozhnov, Ye.A. Rogozin, M.A. Bagayev. — Voronezh: IPTS «Nauchnaya kniga», 2011. 252 s. [Zastrozhnov I.I. Methodological basis for the safe use of information technologies in electronic document management systems: monograph / I.I. Zastrozhnov, E.A. Rogozin, M.A. Bagayev. Voronezh: CPI «Scientific book», 2011. 252 p. (in Russ)].
8. Drovnikova I.G. Metodika proyektirovaniya sistem informatsionnoy bezopasnosti v avtomatizirovannykh sistemakh [Elektronnyy resurs] / I.G. Drovnikova, A.A. Nikitin, Ye.A. Rogozin // Internet-zhurnal «Tekhnologii tekhnosfernoy bezopasnosti». 2016. Vypusk № 4 (68) (avgust). http:// ipb.mos.ru/ttb/2016-4. [Drovnikova I.G. Methods of designing of information security systems in automated systems [Electronic resource] / I.G. Drovnikova, A.A. Nikitin, E.A. Rogozin // Internet journal «Technologies of technospheric safety». — 2016. Issue № 4 (68) (August). http:// ipb.mos.ru/ttb/2016-4 (in Russ)].
9. Drovnikova I.G. Razrabotka metoda «myagkogo administrirovaniya» dlya organizatsii upravleniya podsistemoy razgranicheniya dostupa v avtomatizirovannykh sistemakh / I.G. Drovnikova, D.A. Kabanov // Vestnik Voronezhskogo instituta MVD Rossii. 2014. № 4. S. 269-276. [Drovnikova I.G. Development of a method for «soft admin» organization control subsystem of access control in automated systems / I.G. Drovnikova, D.A. Kabanov // Vestnik of Voronezh Institute of MIA Russia. — 2014. № 4. P. 269-276 (in Russ)].
10. Buzov G.A. Zashchita informatsii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam / G.A. Buzov. M.: GLT, 2016. 586 c. [Buzov G.A. Protection of limited access information from leakage through technical channels / G.A. Buzov. M.: GLT, 2016. 586 p. (in Russ)].
11. Malyuk A.A. Osnovy politiki bezopasnosti kriticheskikh sistem informatsionnoy infrastruktury: ucheb. posobiye / A.A. Malyuk M.: Goryachaya liniya — Telekom, 2018. 314 s. [Malyuk A.A. Fundamentals of security policy of critical information infrastructure systems: proc. manual / A.A. Malyuk M.: Hot line — Telecom, 2018. 314 p. (in Russ)].
12. Babash A.A. Aktual'nyye voprosy zashchity informatsii: monografiya / A.A. Babash [i dr.]. — M.: Rior, 2017. 111 s. [Babash A.A. Actual questions of information security: monograph / A.A. Babash [and others]. M.: Rior, 2017. 111 p. (in Russ)].
13. Danilenko A.V. Bezopasnost' sistem elektronnogo dokumentooborota. Tekhnologiya zashchity elektronnykh dokumentov / A.V. Danilenko. M.: Lenand, 2015. 232 s. [Danilenko A.V. Security of electronic document management systems. Technology to protect electronic documents / A.V. Danilenko. M.: Lenand, 2015. 232 p. (in Russ)].
    Markov A.S. Metody otsenki nesootvetstviya sredstv zashchity informatsii / A. S. Markov [i dr.]. — M.: Radio i svyaz', 2012. 192 s.
14. Markov A.S. Methods for assessing the mismatch of information security tools / A. S. Markov [et al.]. - M.: Radio and Communications, 2012.192 s. [Markov A.S. Methods of evaluation of information security means. M.: Radio and communication, 2012. 192 p. (in Russ)].
15. Xiao Y. Handbook of security and neyworks / Y. Xiao [and ot.]. Word Scientific Pub Co Inc. 1 edition, 2012. 576 p.
16. Schaefer R. Information Theoretic Security and Privacy of Information Systems / R. Schaefer. — Cambridge University Press, 2017. 574 p.
17. Sheikh F. Circuits and Systems for Security and Privacy / F. Sheikh [and others]. CRC Press, 2016. 400 p.
18. Fields B. Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution / B. Fields. IGI Global, 2018. 648 p.
19. Rudra B. Flexible Network Architectures Security: Issues and Principles /B. Rudra. Auerbach Publications, 2018. 326 p.
20. Klaic A. Conceptual Modeling of Information Systems within the Information Security Policies / A. Klaic, M. Golub // Journal of Economics/ Business and Management. 2013. vol. 1. Issue 4. pp. 371–376.
21. Nazareth D. System dynamics model for information security management / D. Nazareth, J. Choi // Information & Management. 2015. vol. 52. Issue 1. P. 123–134.
22. Rogozin Ye.A. Model' funktsionirovaniya tipovoy sistemy zashchity informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh informatsionnykh sistemakh OVD / Ye.A. Rogozin, A.D. Popov // Vestnik Voronezhskogo instituta MVD Rossii. 2016. № 4. S. 122-132. [Rogozin E.A. Model operation of the standard information system of protection against unauthorized access to automated information systems of the Law Enforces Agencies / E.A. Rogozin, A.D. Popov // Vestnik Voronezhskogo instituta MVD Rossii — Bulletin of the Voronezh Institute of the Ministry of the Interior of Russia. 2016. № 4. pp. 122–132 (in Russ)].
23. GOST R ISO/MEK 15408-2-2013. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. CH. 2: Funktsional'nyye komponenty bezopasnosti. [Elektronnyy resurs]. URL: http://docs.cntd.ru/document/1200105710 (data obrashcheniya 23.11.2018). [GOST R ISO/IEC 15408-2-2013.

Information technology. Methods and means of security. Criteria for evaluating the security of information technology. Part 2: Functional safety components. [Electronic resource.] — URL: http://docs.cntd.ru/document/1200105710 (accessed 23.11.2018) (in Russ)].

24. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Terminy i opredeleniya: rukovodyashchiy dokument // sb. rukovodyashchikh. dokum. po zashchite informatsii ot nesanktsionirovannogo dostupa Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii. M.: Ross. inzhener. Akademiya, 1998. S. 5-14. [Protection against unauthorized access to information. Terms and definitions: guidance document // sat. docum. on protection of information from unauthorized access of the state technical Commission under the President of the Russian Federation. M.: Ross. engineer. Academy, 1998. P. 5-14 (in Russ)].
25. Kontseptsiya zashchity sredstv vychislitel'noy tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii: rukovodyashchiy dokument // sb. rukovodyashchikh. dokum. po zashchite informatsii ot nesanktsionirovannogo dostupa Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii. M.: Ross. inzhener. Akademiya, 1998. S. 15-21. [The concept of protection of computer equipment and automated systems from unauthorized access to information: guidance document // sat. docum. on protection of information from unauthorized access of the state technical Commission under the President of the Russian Federation. M.: Ross. engineer. Academy, 1998. P. 15-21 (in Russ)].
26. Avtomatizirovannyye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii: rukovodyashchiy dokument // sb. rukovodyashchikh. dokum. po zashchite informatsii ot nesanktsionirovannogo dostupa Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii. M.: Ross. inzhener. Akademiya, 1998. S. 22-51. [Automated system. Protection against unauthorized access to information. Classification of automated systems and information security requirements: guidance document // sat. docum. on protection of information from unauthorized access of the state technical Commission under the President of the Russian Federation. — M.: Ross. engineer. Academy, 1998. P. 22-51 (in Russ)].
27. Sredstva vychislitel'noy tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchonnosti ot nesanktsionirovannogo dostupa k informatsii: rukovodyashchiy dokument // sb. rukovodyashchikh. dokum. po zashchite informatsii ot nesanktsionirovannogo dostupa Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii. M.: Ross. inzhener. Akademiya, 1998. S. 52-71. [Computer aids. Protection against unauthorized access to information. Indicators of protection against unauthorized access to information: guidance document // sat. docum. on protection of information from unauthorized access of the state technical Commission under the President of the Russian Federation. M.: Ross. engineer. Academy, 1998. pp. 52-71 (in Russ).]
28. Vremennoye polozheniye po organizatsii razrabotki, izgotovleniya i ekspluatatsii programmnykh i tekhnicheskikh sredstv zashchity informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh sistemakh i sredstvakh vychislitel'noy tekhniki: rukovodyashchiy dokument // sb. rukovodyashchikh. dokum. po zashchite informatsii ot nesanktsionirovannogo dostupa Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii. — M.: Ross. inzhener. Akademiya, 1998. S. 72-92. [Temporary position on the organization of development, production and operation of software and hardware to protect information from unauthorized access to automated systems and computer equipment: guidance document // sat. docum. on protection of information from unauthorized access of the state technical Commission under the President of the Russian Federation. M.: Ross. engineer. Academy, 1998. pp. 72-92 (in Russ)].

Сведения об авторах:

Алфёров Владимир Павлович — соискатель, кафедра конструирования и производства радиоэлектронной аппаратуры.

Дровникова Ирина Григорьевна — доктор технических наук, доцент, профессор, кафедра автоматизированных информационных систем органов внутренних дел

Обухова Людмила Александровна — кандидат технических наук, доцент, кафедра автоматизированных информационных систем органов внутренних дел

Рогозин Евгений Алексеевич — доктор технических наук, профессор, профессор, кафедра автоматизированных информационных систем органов внутренних дел.

Information about the authors:

Vladimir P. Alferov —Applicant, Department of Design and Production of Radio-Electronic Equipment .

Irina G. Drovnikova – Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs.

Lyudmila A. Obukhova – Cand. Sci. (Technical), Assoc. Prof., Department of Automated Information Systems of the Internal Affairs

Evgeny A. Rogozin - Dr. Sci. (Technical), Prof., Department of Automated Information Systems of Internal Affairs.

Конфликт интересов **Conflict of interest.**

Авторы заявляют об отсутствии конфликта интересов. **The authors declare no conflict of interest.**

Поступила в редакцию 10.03.2019. **Received** 10.03.2019.

Принята в печать 30.05.2019. **Accepted for publication** 30.05.2019.