ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2022-49-2-24-32 Обзорная статья / Review article

К вопросу анализа существующих методов доступа штатных пользователей к информационным ресурсам автоматизированных систем органов внутренних дел

В.А. Вольф[1], В.С. Наседкина[1], А.Д. Попов[1], Е.А. Рогозин[1], В.А. Хвостов[2]
[1] Воронежский институт МВД России,
[1]394065, г. Воронеж, пр. Патриотов, 53, Россия,
[2]Воронежский университет инженерных технологий,
[2]394036, г. Воронеж, проспект Революции, д. 19, Россия

Резюме. Цель. В настоящее время доступ к информационному ресурсу АС ОВД реализован через подсистему управлению доступом СЗИ на основе мандатного и дискреционного методов разграничения доступа, разработанных в 70-х годах прошлого столетия, и требующих улучшения. Целью исследования является анализ существующих методов и выбор на этой основе оптимального метода доступа штатных пользователей к информационным ресурсам автоматизированных систем ОВД. **Метод**. Системный анализ, метод теории графов, и вербальное (словесное) моделирование. **Результат**. Раскрыт новый аспект метода доступа штатных пользователей к информационным ресурсам автоматизированных систем ОВД, основанный на применении иерархических метрик семантической близости. **Вывод**. Применение метода, основанного на семантической близости, значительно сокращает обработку большого количества информации, соответственно, повышая производительность автоматизированных систем.

Ключевые слова: автоматизированные системы, системы защиты информации, метод доступа

Для цитирования: В.А. Вольф, В.С. Наседкина, А.Д. Попов, Е.А. Рогозин, В.А. Хвостов. К вопросу анализа существующих методов доступа штатных пользователей к информационным ресурсам автоматизированных систем органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(2):24-32. DOI:10.21822/2073-6185-2022-49-2-24-32

To the question of analysis of existing methods of access of regular users to information resources of automated systems of internal affairs bodies

V.A.Wolf [1], V.S. Nasedkina[1], A.D. Popov[1], E.A. Rogozin[1], V.A. Khvostov[2]
[1]Voronezh Institute of the Ministry of Internal Affairs of Russia,
[1]53 Patriotov Str., Voronezh 394065, Russia,
[2]Voronezh University of Engineering Technologies,
[2]19 Revolution Ave., Voronezh 394036, Russia

Abstract. Objective. Currently, access to the information resource of the ATS AS is implemented through the access control subsystem of the information security facility based on the mandatory and discretionary methods of access control developed in the 70s of the last century and requiring improvement. The purpose of the study is to analyze existing methods and, on this basis, select the optimal method for regular users to access information resources of automated systems of internal affairs bodies. **Method.** System analysis, graph theory method, and verbal (verbal) modeling. **Result.** A new aspect of the method of access of regular users to information resources of automated ATS systems, based on the use of hierarchical metrics of semantic proximity, is disclosed. **Conclusion.** The use of a

method based on semantic proximity significantly reduces the processing of a large amount of information, respectively, increasing the performance of automated systems.

Keywords: automated systems, information security systems, access method

For citation: V.A.Wolf , V.S. Nasedkina, A.D. Popov, E.A. Rogozin, V.A. Khvostov. To the question of analysis of existing methods of access of regular users to information resources of automated systems of internal affairs bodies. Herald of the Daghestan State Technical University. Technical Science. 2022; 49 (2): 24-32. DOI: 10.21822 /2073-6185-2022-49-2-24-32

Введение. В настоящее время доступ к информационным ресурсам автоматизированных систем ОВД в соответствии с документацией Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [1-3] осуществляется через подсистему управления доступом системы защиты информации (СЗИ).

В зависимости от класса защищенности определяется количество функционала в этой системе, то есть чем выше класс защищенности, тем больше функционала содержится в подсистеме управления доступом существующих СЗИ.

На основе общепринятых подходов принято считать, что защищённой системой является система, в которой поддерживается определенный уровень конфиденциальности (исключение несанкционированного доступа к защищаемой информации), целостности (исключение возможности модифицировать защищаемую информацию) и доступности [4, 8].

Постановка задачи. Для более эффективного и безопасного обращения штатных пользователей кафедр, рассмотреных на примере ВИ МВД необходимо:

1. Проанализировать существующие методы доступа к информационным ресурсам АС ОВД;
2. На основе результатов анализа определить основные имеющиеся недостатки у каждого анализируемого метода доступа;
3. Путем сравнения основных недостатков и положительных моментов, с точки зрения применения этих методов, выбрать наилучший по определенному критерию, который необходимо обосновать.

Проведенный анализ открытых источников показал, что первостепенной задачей в области защиты информации (ЗИ) в АС ОВД является именно защита от несанкционированного доступа (НСД) к информационным ресурсам.

Методы исследования. Для формализованного описания требований, предъявляемых к СЗИ, применяются соответствующие модели разграничения доступа.

Основными являются [5]:

1. Модель дискреционного разграничения доступа, примером служит модель Хааррисона Руззо-Ульмана.
2. Модель мандатного разграничения доступа, классическим примером является модель Белла-Лападула.
3. Ролевая модель разграничения доступа, включающая в себя признаки, как мандатной, так и дискреционной модели.

В основе любой модели разграничения доступа лежат такие понятия, как объект доступа и субъект доступа. В качестве объекта может выступать документ, файл, архив и др.; субъектом, как правило, являются пользователи системы.

Дискреционная модель разграничения доступа. Сущность дискреционного метода разграничения доступа заключается в проверке прав доступа субъекта к объекту, в момент открытия субъектом этого объекта.

Матрица доступа является основой дискреционного метода. Строки матрицы соответствуют субъектам ($S_{1\ldots4}$), а столбцы матрицы – объектам ($O_{1\ldots4}$). То есть, права доступа субъекта к объекту определяются элементами матрицы (рис. 1).

Главным недостатком матрицы доступа является ее большая размерность, которая влияет на время вычисления уровней доступа. То есть, чем больше записей в матрице, тем больше нужна производительность компьютерной системы.

Более того, все взаимосвязи и ограничения необходимо учитывать вручную, что порядком усложняет администрирование. Права доступа субъекта к объекту являются статичными, то есть независимо от изменения состояния компьютерной системы, права доступа субъекта останутся неизмененными, что также принимается как недостаток рассматриваемого метода разграничения доступа.

объект / субъект	O_1	O_2	O_3	O_4
S_1	read			
S_2				print
S_3		read	execute	
S_4	read write		read write	

Рис. 1. Матрица доступа
Fig. 1. Access Matrix

В методе дискреционного разграничения доступа не осуществляется проверка безопасности выполнения действий субъекта (разрешение доступа субъекта S к объекту O), что не позволяет обеспечивать защиту от утечки конфиденциальной информации. Другими словами, если субъект S_1, являясь владельцем базой данных, наделяет правом чтения субъекта S_2, то фактически субъект S_2 становится владельцем всей защищаемой информацией.

Модель мандатного разграничения доступа. Классическая модель Белла–Лападулы впервые была использована в 70-х годах прошлого века и по настоящее время является основной моделью многоуровневого разграничения доступа, применяемой в большинстве СЗИ, в том числе и на объектах информатизации ОВД [7-9].

Структурно-функциональная модель мандатного разграничения доступа представлена на рис. 2.

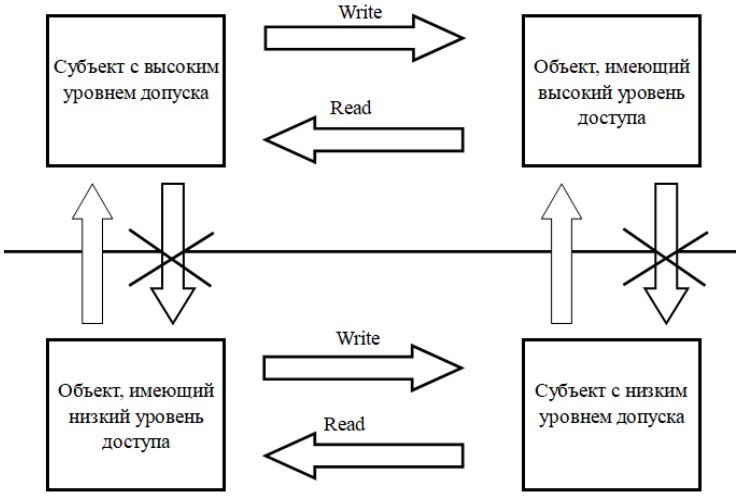

Рис. 2. Структурно-функциональная модель мандатного разграничения доступа
Fig. 2. Structural and functional model of mandatory access control

Основной задачей подсистемы управления доступом пользователей в СЗИ на объектах информатизации ОВД, построенной по мандатному принципу разграничения доступа, является обеспечение конфиденциальности.

Сохранение целостности является не менее важной задачей в обеспечении безопасности информации, однако в рассматриваемой модели вопрос обеспечения целостности защищаемых информационных ресурсов не является приоритетным, и реализуется только как второстепенный признак защиты информации ограниченного доступа [4]. Более того, не исключением является возможность возникновения диссонанса.

Обеспечение безопасности информационных потоков является одной из первостепенных проблем реализации мандатной модели разграничения доступом. Причиной чему является сложность самого процесса выявления запрещенных информационных потоков по памяти, а тем более, по времени.

Частым случаем появления таких потоков является тот факт, что при администрировании СЗИ, построенной на основе мандатной политики безопасности акцент делается на ограничении доступа субъекта с низким уровнем допуска к объекту с высоким уровнем доступа. В то время как малое значение уделяется не менее важной проблеме, связанной с возникновением запрещенных информационных потоков от объектов с большим уровнем конфиденциальности к объектам с меньшим уровнем конфиденциальности.

Решение задач, требуемых коллективного принятия решения в режиме реального времени, подразумевают наличие доступа субъектов, имеющих различные уровни секретности к одним и тем же задачам и функциям системы. Однако, модель на такую сложившуюся ситуацию, не реагирует [7].

К тому же, субъекты заданного уровня секретности одновременно как по времени, так и по задачам и функциям, выполняющимся в реальном масштабе времени, имеют доступ к системе без ограничения, а это является нарушением основных принципов безопасности [8].

Не без внимания остается вопрос изменения классификации сведений, относящихся к какому-либо уровню секретности. Применение мандатной модели разграничения доступа предполагает, что данные, отнесенные к одному из уровней секретности, остаются неизменными, что на практике не является действительным.

Таким образом, применение мандатной модели разграничение доступом более целесообразно для рассматриваемых статическим систем, а для моделей в динамике данный способ требует доработки.

По правилам мандатного разграничения доступа пользователи системы имеет полномочия на чтение тех документов, уровень доступа которых не превышает их уровень допуска, и также, не имеют возможности создавать документы ниже своего уровня допуска [8]. Таким образом, пользователь сталкивается с ситуацией, когда запрещается право чтения документа, который он сам создал, то есть осуществляется санкционированная работа с данными, просмотр которых заращен системой.

Ролевая модель разграничения доступа. Совместила в себе признаки мандатного и дискреционного разграничения доступа, однако ни к одному из них данную модель отнести нельзя. Помимо классических понятий «объект» и «субъект» доступа, появляется такое понятие как «роль».

По своей сути «роль» выступает как набор полномочий, которыми наделен пользователь, в зависимости от выполняемых должностных (обязанностей) задач. Полномочия содержат права осуществлять функционально-логические процедуры над всей совокупностью объектов системы или над определенной их группой.

Основой разграничения доступа является усовершенствованная матрица, задача которой заключается в назначении прав доступа для ролей. В добавлении к этому имеются заранее определенные правила, на основе которых осуществляется назначение роли для каждого пользователя и активирование этих ролей во время начала работы.

Структурно-функциональная модель дискреционного разграничения доступа представлена на рис. 3.

На практике, нередко возникают случаи, в частности в системе ОВД, когда пользователи занимают одну (одинаковую) должность, но при этом каждый из них имеет отличные друг от друга, уникальные права. Подобная ситуация значительно усложняет построение и администрирование ролевой модели разграничения доступа.

Также модели имеют избыточность прав на доступ, и дублирование в предоставлении прав доступа пользователей к объектам. При этом, проектирование защищенной системы с множеством рабочих групп достаточно трудозатратно, и требует применения дополнительных теоретико-графовых алгоритмов и пространственно-векторных моделей [10].

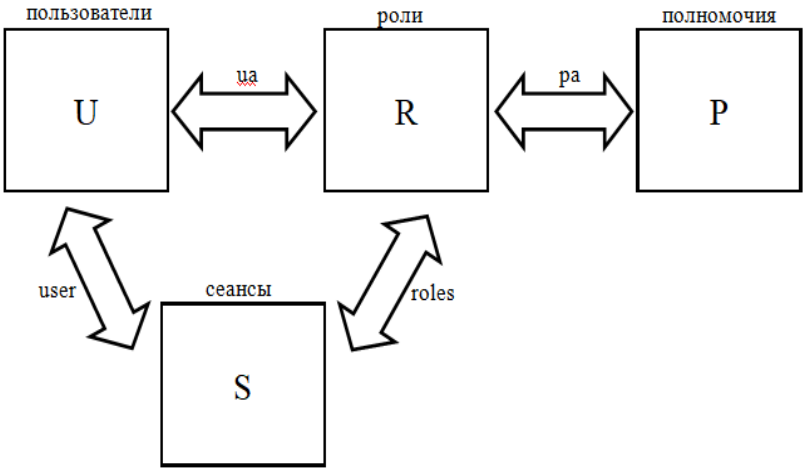

Рис. 3. Структурно-функциональная модель дискреционного разграничения доступа
Fig. 3. Structural and functional model of discretionary access control

Обсуждение результатов. Рассмотренные модели является основополагающими для построения СЗИ, однако нельзя не отметить тот факт, что создание таких моделей и их проработка в СЗИ началась в 1970г., и применяются по настоящее время практически в неизменном виде.

Учитывая динамику развития способов нарушения безопасности информации, возникновения новых угроз НСД к информации. Все это способствует созданию новых критериев разграничения доступа, позволяющих усовершенствовать существующие модели управления доступом, повысить степени защищенности информации, циркулирующей в АС ОВД.

Одним из перспективных аспектов совершенствования существующих методов доступа, учитывая недостатки рассмотренных методов, является метод, основанный на использовании иерархических метрик семантической близости, сущность которого раскрыт в [9].

Такой метод доступа впервые был рассмотрен и в медицинских системах [10] и образовательных системах [9]. В то же время вопросы, связанные с адаптацией данного метода в АС ОВД требуют дальнейшей проработки. Связано с тем, что при доступе в АС ОВД штатные пользователи этих систем осуществляют работу с многоуровневым иерархическим информационным ресурсом, который можно представить в виде модели, (математической модели, вербальной и др.).

Анализ информационного ресурса АС ОВД показал, что структуру этого ресурса и взаимодействующих с ним штатных сотрудников АС ОВД можно формализовать в виде графовой модели (рис. 4) [6].

$$H = (S, E), \quad (1)$$

где

$S = \{s_1, s_2 \ldots s_{12,20}\}$ – элементы (субъекты) информационного ресурса;

$E = \{e_1, e_2, \ldots e_l\}$ – связи между элементами или подмножествами элементов информационного ресурса.

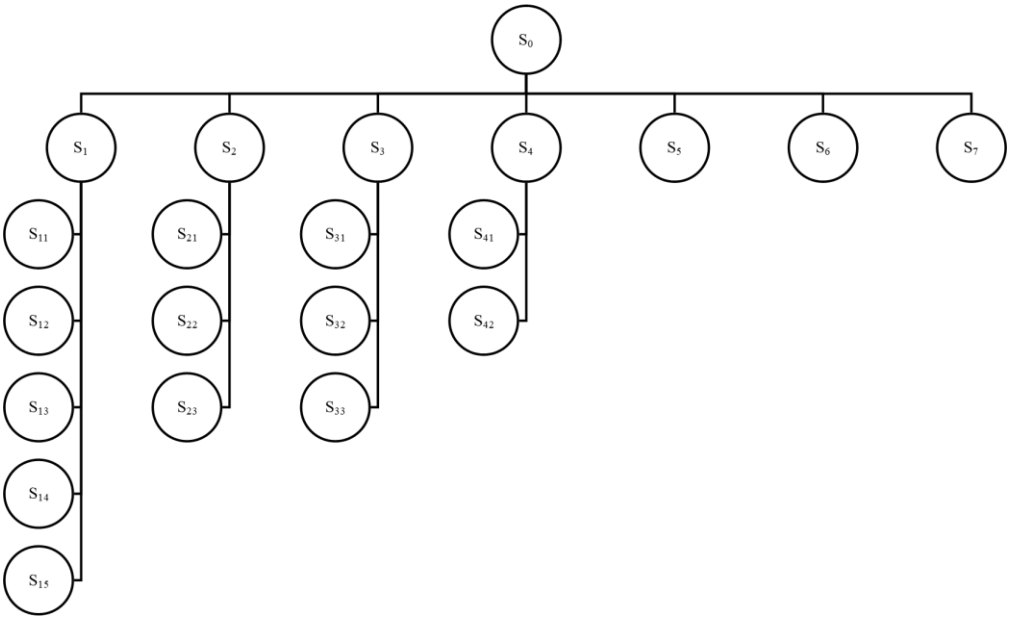

Рис. 4. Графовая модель структуры информационного ресурса института
Fig. 4. Graph model of the structure of the information resource of the Institute

В табл. 1 представлено описание элементов s_i.

Таблица 1. Перечень вершин графа
Table 1. List of graph vertices

S_0	Начальник подразделения (начальник института); Head of the department (head of the institute);
S_1	Заместитель начальника по учебной работе; Deputy Head for Academic Affairs
S_2	заместитель начальника института по научной работе; Deputy Head of the Institute for Research
S_3	Заместитель начальника по работе с личным составом; Deputy Chief of Human Resources
S_4	Заместитель начальника по организации службы; Deputy Head of Service Organization
S_5	Тыл; rear
S_6	Финансово-экономический отдел; Financial and economic department
S_7	Отдел делопроизводства и режима; Office work and regime department
S_{11}	Учебный отдел; Training Division
S_{12}	Кафедры; Departments
S_{13}	Факультеты; Faculties
S_{14}	Библиотека (общая); Library (shared)
S_{15}	Специальная библиотека; Special library
S_{21}	Научно-исследовательский отдел; Research department
S_{22}	Редакционно-издательский отдел; Editorial and publishing department
S_{23}	Адъюнктура; Postgraduate education
S_{31}	Отдел морально-психологической подготовки; Department of moral and psychological preparation
S_{32}	Отдел кадров; Human Resources Department
S_{33}	Инспекция по личному составу; Personnel inspection
S_{41}	Комендантское отделение; Commandant's office

Ресурсы Воронежского института МВД России проклассифицированы по видам деятельности сотрудником. Особое внимание уделяется тому, что в информационной системе органов внутренних дел циркулирует не только информация, отличающаяся по сфере деятельности, но и по уровням конфиденциальности.

Заменим позицию S, выступающую как субъект информационной системы, на значение t – рубрика. Таким образом, корневой граф, представленный на рис. 5, (табл. 2) можно озаглавить как иерархический тематический классификатор информационных объектов воронежского института МВД России.

При организации доступа к информационным ресурсам (библиотекам, документам, архивам) применяется тематический классификатор, который представляет собой совокупность тематических рубрик и отражает логическую архитектуру всех информационных ресурсов.

При наделении правами доступа пользователей системы устанавливается частичный порядок на сформированном классификаторе, представленным в виде корневого дерева [10]. Тематическая классификация на основе отображения множества рубрик ($T=t_1, t_2,\ldots t_m$) на множестве объектов и субъектов определяется на корневом дереве иерархического рубрикатора.

Функция тематического окрашивания f_m, работа которой заключается в том, чтобы в каждый момент времени для любого субъекта и объекта определить соответствующую рубрику:

$$f_M[x] = t^M \text{ , где } x \in S \cup O, t_i^M \in T^M .$$

Реализация тематико-иерархического разграничения доступа заключается в переходе из состояния в момент времени t_k в момент времени t_{k+1}.

В свою очередь, такие переходы приводят к новым отношениям доступа между уже существующими сущностями (создают новые или удаляют субъекты и объекты).

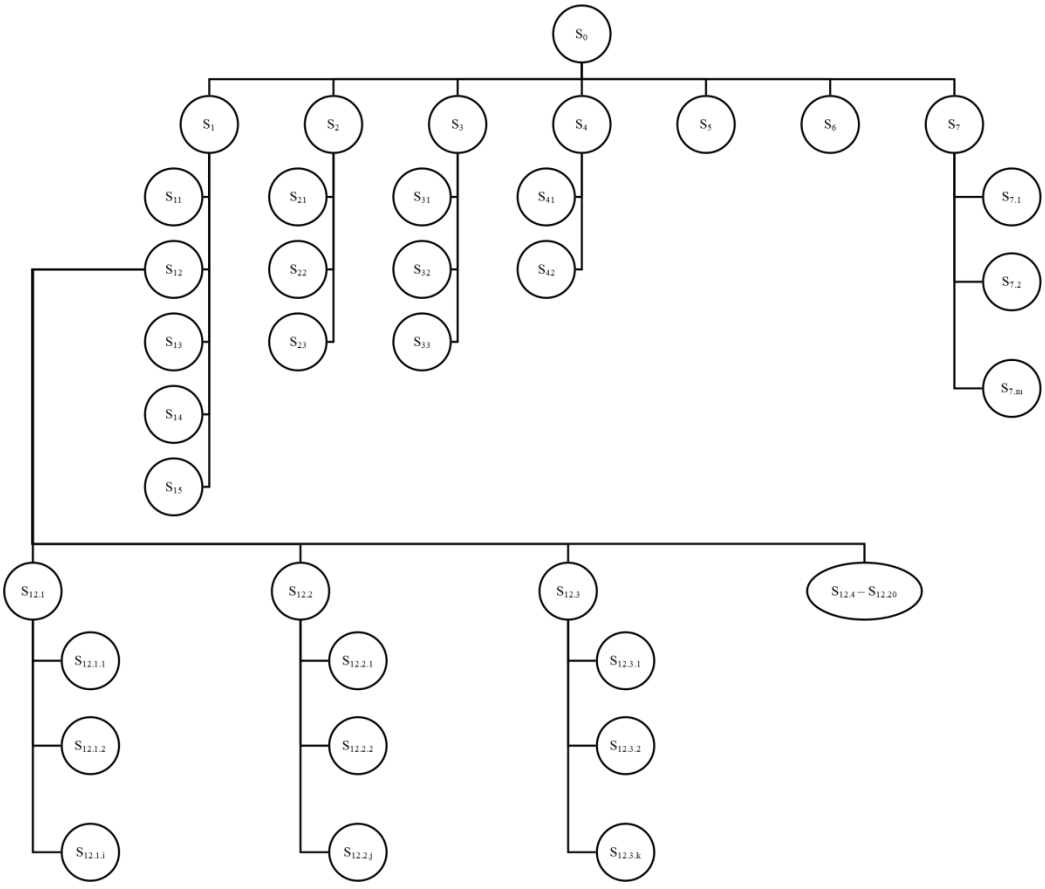

Рис. 5. Иерархический тематический классификатор
Fig. 5. Hierarchical Topic Classifier

Таблица 2. Перечень вершин графа
Table 2. List of graph vertices

S_{71}-S_{7m}	Сотрудники отдела делопроизводства и режима; Office work and regime department employees
$S_{12.1}$	Кафедра информационной безопасности; Department of Information Security
$S_{12.1.1}$- $S_{12.1.i}$	Сотрудники кафедры информационной безопасности; Employees of the Department of Information Security
$S_{12.2}$	Кафедра компьютерной безопасности; Department of Computer Security
$S_{12.2.1}$- $S_{12.2.j}$	Сотрудники кафедры компьютерной безопасности; Employees of the Department of Computer Security
$S_{12.3}$	Кафедра оперативно-разыскной деятельности; Department of operational-search activity
$S_{12.3.1}$- $S_{12.3.k}$	Сотрудники кафедры оперативно-разыскной деятельности; Employees of the department of operational-investigative activities
$S_{12.4.}$- $S_{12.20}$	Кафедры института; Departments of the institute

При таком управлении доступом реализуется принятие решения о правомочности доступа субъекта S к объекту O, обеспечивающее транзитивность потоков при реализации требуемого подмножества безопасных по определенному критерию информационных потоков. Применение такого метода значительно сокращает обработку большого количества информации, соответственно, повышается производительность АС.

Вывод. Таким образом, в статье проведен анализ открытых литературных источников и специальной литературы ФСТЭК России, посвященных вопросам защиты информации в АС ОВД. Анализ показал, что в существующих СЗИ используемых в системах критического применения к которым, несомненно, относятся и ОВД, в соответствии с приказами и директивами ФСТЭК используются дискреционный и мандатный методы доступа.

В то же время, эти методы были разработаны в 70-х годах прошлого столетия и требуют, в соответствии с существующими реалиями, к которым можно отнести случаи, когда в качестве штатного пользователя может выступать человек с экстремистскими убеждениями, действия которого могут привести к нежелательным последствиям жизни российского общества.

Существующие методы, в соответствии с их достоинствами и недостатками, на таких типов пользователей не реагируют. Поэтому, предлагаемый новый метод, основанный на семантической близости [9], поможет устранить такие недостатки. Сущность такого метода, применимая к объектам информатизации ОВД, будет рассмотрена в дальнейших исследованиях.

Библиографический список:

1. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]. — URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения 20.06.2022).
2. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [Электронный ресурс]. — URL:http://fstec.ru/component/attachment s/ 299 (дата обращения: 26.06.2022).
3. Гостехкомиссия РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Воениздат, 1992. – 29 с.
4. Анализ угроз безопасности информации при обработке персональных данных в мобильной медицине / В.П. Гулов, В.А. Хвостов, А.В. Скрыпников, В.П. Косолапов, Г.В. Сыч // Системный анализ и управление в биомедицинских системах. 2020. – Т.19, №2. – С. 129-138.
5. Зегжда Петр Дмитриевич. Основы информационной безопасности: учебное пособие / П. Д. Зегжда, Е. А. Рудина; Санкт-Петербургский государственный политехнический университет. — Санкт-Петербург: Изд-во Политехн. ун-та. 2008. - 224 с.
6. Кристофидес Н. Теория графов. Алгоритмический подход. - М.: Мир, 1978. - 432 с.
7. Лепешкин, О. М. Мандатная модель разграничения доступа на основе среды радикалов / О. М. Лепешкин, Р. С. Гаппоев // Известия ЮФУ. Технические науки. – 2011. – № 12(125). – С. 70-77.
8. Медведев, Н. В. Модели управления доступом в распределенных информационных системах / Н. В. Медведев, Г. А. Гришин // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. – 2011. – № 1. – С. 1.

9. Модели управления доступом пользователя информационной системы с использованием иерархических метрик семантической близости / Е. А. Рогозин, А. А. Хвостов, А. В. Калач [и др.] // Вестник Воронежского института ФСИН России. – 2021. – № 4. – С. 110-120.
10. Модель индивидуально группового назначения доступа к иерархически организованным объектам медицинских информационных систем с использованием мобильных технологий / В. П. Гулов, В. А. Хвостов, В. П. Косолапов, Г. В. Сыч // Системный анализ и управление в биомедицинских системах. – 2021. – Т. 20. – № 1. – С. 135-146..

References:

1. FSTEC RF. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for the protection of information [Electronic resource].URL:https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (accessed 20.06.2022). (In Russ)
2. FSTEC RF. Guidance document. The concept of protection of computer equipment and automated systems from unauthorized access to information [Electronic resource]. URL: http://fstec.ru/component/attachment s/ 299 (date of access: 06/26/2022). (In Russ)
3. State Technical Commission of the Russian Federation. Guidance document. Computer facilities. Protection against unauthorized access to information. Indicators of security from unauthorized access to information. M.: [Voyenizdat] *Military Publishing House*, 1992: 29. (In Russ)
4. Analysis of threats to information security in the processing of personal data in mobile medicine. V.P. Gulov, V.A. Khvostov, A.V. Skrypnikov, V.P. Kosolapov, G.V. Sych. [Sistemnyy analiz i uprav-leniye v biomeditsinskikh sistemakh.]*System analysis and management in biomedical systems.* 2020; 19(2): 129-138. (In Russ)
5. Zegzhda Petr Dmitrievich. Fundamentals of information security: textbook. P. D. Zegzh-da, E. A. Rudina; St. Petersburg State Polytechnic University. St. Petersburg: [Sankt-Peterburg: Izd-vo Politekhn. un-ta.] *Publishing house of Politekhn. University.* 2008: 224. (In Russ)
6. Christofides N. Graph Theory. [Algoritmicheskiy podkhod] *Algorithmic approach*. M.: Mir, 1978: 432. (In Russ)
7. Lepeshkin, O. M., Gappoev R. S. Mandatory model of access control based on the environment of radicals [Izvestiya YUFU. Tekhnicheskiye nauki] *Izvestiya SFedU. Technical Science*. 2011; 125 (12): 70-77. (In Russ)
8. Medvedev, N. V. Models of access control in distributed information system. N. V. Medvedev, G. A. Grishin. [Nauka i obrazovaniye: nauchnoye izdaniye MGTU im. N.E. Baumana] *Science and education: scientific edition of MSTU im. N.E. Bauman*. 2011; 1: 1. (In Russ)
9. Rogozin E. A., Khvostov A. A., Kalach A. V. [et al.] Models of information system user access control using hierarchical semantic proximity metrics. [Vestnik Vo-ronezhskogo instituta FSIN Rossii] *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2021; 4:110-120. (In Russ)
10. Gulov V. P., Khvostov V. A., Kosolapov V. P., Sych G. V. Model of individually group assignment of access to hierarchically organized objects of medical information systems using mobile technologies. [Sistemnyy analiz i upravleniye v biomeditsinskikh sistemakh] *System Analysis and Management in biomedical systems*. 2021; 20(1):135-146. (In Russ)

Сведения об авторах:

Вольф Владимир Андреевич, адъюнкт; volf.vladimir2010@yandex.ru

Наседкина Валерия Сергеевна, адъюнкт; valeriya.sn@mail.ru

Попов Антон Дмитриевич, кандидат технических наук, преподаватель кафедры автоматизированных информационных систем органов внутренних дел; anton.holmes@mail.ru

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; evgenirogozin@yandex.ru

Хвостов Виктор Анатольевич, кандидат технических наук, доцент кафедры информационной безопасности; hvahva1@mail.ru

Information about authors:

Vladimir A.Volf, adjunct; volf.vladimir2010@yandex.ru

Valeria S. Nasedkina, adjunct; valeriya.sn@mail.ru

Anton D. Popov, Cand.Sci. (Eng.), Lecturer, Department of Automated Information Systems of Internal Affairs Bodies; anton.holmes@mail.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Victor A. Khvostov, Cand.Sci. (Eng.), Assoc. Prof., Department of Information Security; hvahva1@mail.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/Received 29.05.2022.

Одобрена после рецензирования/ Reviced 18.06.2022.

Принята в печать/Accepted for publication 18.06.2022.