

Определение состава атрибутов учетных записей пользователей для централизованного администрирования гетерогенных систем

А.Ю. Ефимов ¹✉¹ НИИ «Центрпрограммсистем», г. Тверь, 170024, Россия

Ссылка для цитирования

Ефимов А.Ю. Определение состава атрибутов учетных записей пользователей для централизованного администрирования гетерогенных систем // Программные продукты и системы. 2025. Т. 38. № 4. С. 637–643. doi: 10.15827/0236-235X.152.637-643

Информация о статье

Группа специальностей ВАК: 2.3.6

Поступила в редакцию: 09.06.2025

После доработки: 19.06.2025

Принята к публикации: 20.06.2025

Аннотация. Для повышения эффективности защиты информации и сокращения необходимых для этого ресурсов в сложных информационных системах применяется централизованное управление комплексом средств защиты информации. Данная статья посвящена решению задачи организации учетных записей пользователей касательно состава их атрибутов в условиях гетерогенных информационных систем. Ее актуальность подтверждается наличием проблем, возникающих из-за различий реализации механизмов защиты (в частности, учетных записей пользователей) в компонентах таких систем. В работе рассмотрены существующие методы решения проблемы, выявлена важная роль наборов атрибутов учетных записей в вопросе применимости в условиях гетерогенных информационных систем. Предложен новый эффективный подход к организации учетных записей, основанный на оценке схожести и различий атрибутов в разных операционных системах и последующем разделении атрибутов на группы общих и специфичных. Описаны модель состава атрибутов учетных записей в гетерогенной информационной системе, разработанная на ее основе методика определения состава атрибутов, ее достоинства и недостатки, а также условия и способ применения результатов. Показано направление дальнейшего развития. Применение представленного подхода позволит упростить централизацию управления комплексом средств защиты информации и сократить объем ресурсов, необходимых для управления, без потери при этом эффективности защиты информации.

Ключевые слова: защита информации, информационная безопасность, централизованное администрирование, гетерогенная информационная система, операционная система, учетная запись, атрибут

Введение. Различного рода *информационные системы (ИС)* получили в настоящее время широкое распространение. При этом в большей их части необходимо (и зачастую требуется на законодательном уровне) обеспечение защиты информации, например, в связи с обработкой в них информации ограниченного доступа (персональные данные, коммерческая или государственная тайна и т.п.) либо из-за высоких требований по доступности и/или непрерывности их функционирования (при управлении технологическими процессами, в критической информационной инфраструктуре и т.п.) [1].

Не новой, но до сих пор сохраняющей свою актуальность тенденцией при построении современных ИС является повышение интеграции информационных потоков и процессов, приводящей к росту структурной сложности ИС. В качестве их компонентов выступают не отдельные компьютеры, объединенные в локальную вычислительную сеть, а целые ИС, уже существующие или создаваемые [2–4]. Примерами таких комплексных ИС являются распределенные корпоративные системы (объединяющие ИС филиалов), ИС предприятия (в которых взаимодействуют, например, автоматизирован-

ные системы управления технологическими процессами или управления закупками, складами, поставками и кадрами), комплексные тренажерные системы различной направленности (обеспечивающие взаимодействие отдельных тренажеров) и т.п.

Поскольку компоненты таких комплексных ИС могут создаваться в разное время либо заведомо предназначены для выполнения сильно различающихся задач, зачастую это приводит к гетерогенности этих компонентов – в используемых версиях или даже типах ОС, в системном и функциональном ПО, а также в *средствах защиты информации (СрЗИ)*.

Следует отметить, что такого рода гетерогенность встречается и в более простых ИС, когда отдельные компьютеры системы (предназначенные, например, для выполнения задач реального времени или для работы унаследованного ПО) функционируют под управлением ОС, отличающихся от используемых на остальных компьютерах.

Защита информации является одним из неотъемлемых и зачастую критически важных аспектов ИС, однако ее обеспечение требует как технических, так и человеческих ресурсов,

причем с повышением уровня защищенности растет и ресурсоемкость задачи [3, 5]. С учетом того, что требования по уровню защищенности информации обычно задаются для создаваемой ИС (в виде государственных нормативных требований, корпоративных стандартов и т.п.), в процессе создания ИС возникает задача минимизации расхода ресурсов на обеспечение защиты информации.

Одним из эффективных подходов по сокращению необходимых ресурсов является централизация управления комплексом СрЗИ, используемым в ИС (в том числе в компонентах ИС). Данный подход позволяет обеспечивать единый центр управления информационной безопасностью ИС, согласованность политик безопасности как между компонентами ИС, так и между используемыми СрЗИ, оперативный мониторинг ИС в целом и т.п. [6].

Однако при применении централизованного управления в гетерогенных ИС возникают проблемы, определяемые именно этой гетерогенностью, а точнее, различиями реализаций в используемых ОС и СрЗИ таких ключевых с точки зрения информационной безопасности элементов, как учетные записи пользователей, модели управления доступом, права доступа, события безопасности и т.п. [7].

Данная статья посвящена проблеме централизованного управления учетными записями пользователей в гетерогенных ИС в отношении состава атрибутов этих учетных записей. Решение этой проблемы является одним из необходимых условий для обеспечения эффективного централизованного управления комплексом СрЗИ гетерогенной ИС, что подчеркивает актуальность рассматриваемого вопроса.

Обзор существующих подходов

Необходимо отметить, что в отечественных и зарубежных научных публикациях вопрос централизованного управления учетными записями пользователей применительно к гетерогенным ИС недостаточно исследован.

В работе [8] на примере гетерогенных ИС университета сравниваются два распространенных подхода к автоматизации процессов управления учетными записями пользователей и их привилегиями – создание единой точки аутентификации и авторизации пользователей (внешней по отношению к ИС) и создание единого хранилища данных об учетных записях пользователей и их атрибутах с двусторонней синхронизацией этих данных между хранили-

щем и ИС. Авторы акцентируют внимание в основном на вопросах возможности изменения учетных записей (только в центральной точке либо в самих ИС), а также надежности и безопасности реализации обоих подходов. При этом проблема организации специфичных для используемых ИС данных (атрибутов) учетных записей авторами только обозначается, но не прорабатывается.

В [9] рассматривается процесс интеграции системы управления учетными данными (*Identity Management, IdM*) с управляемой ИС. В рассматриваемой IdM-системе предусматривается ведение учетных записей пользователей в связке с правами их доступа к интегрируемому информационному ресурсу, при использовании типовых или специфичных интеграционных сервисов для обновления пользователей из IdM-системы в информационные ресурсы. Недостатком предлагаемого подхода является использование для учетной записи пользователя фиксированного и весьма базового набора атрибутов, а именно: идентификатор (логин), Ф.И.О. пользователя, контактный телефон, пароль и признак руководителя отдела технической поддержки. Такой базовый набор позволяет управлять доступом к однотипным ресурсам, но не обеспечивает возможности тонкой настройки учетной записи для гетерогенного окружения, в том числе с поддержкой механизмов мандатного контроля доступа и целостности.

Аналогичный недостаток отмечается и в работе [10], где автор останавливается на вопросе ролевого управления доступом с иерархической схемой ресурсов и детализацией до конкретных прав доступа, но применительно к самой учетной записи пользователя еще опирается на схожий фиксированный базовый набор атрибутов.

Анализ публикаций также показывает, что для однородных ИС механизмы централизованного управления учетными записями пользователей хорошо проработаны и реализуются с помощью разного рода IdM-систем, систем управления идентификацией и доступом (*Identity and Access Management, IAM*), а также служб каталогов [6, 11].

Вполне очевидно, что для отдельных ОС вопросы способов централизованного хранения данных учетных записей, а также их тиражирования или применения с централизованных ресурсов имеют готовые решения или подходы к решению. Однако применительно к гетерогенным ИС, использующим одновременно раз-

личные ОС, вопрос управления учетными записями пользователей научно практически не проработан, несмотря на существующую потребность в его решении. При этом явно наблюдается важная роль наборов атрибутов, используемых в учетных записях, в вопросе применимости в условиях гетерогенных ИС.

Предлагаемый подход

Существующие подходы к организации учетных записей пользователей предполагают использование некоторого фиксированного набора атрибутов, где каждому присвоено единственное значение. Подобная линейная схема хорошо работает в однородной ИС. Однако в условиях гетерогенной ИС, когда реализация учетных записей пользователей в разных ОС различается, ее применение уже становится затруднительным.

Для решения этой проблемы в данном исследовании предлагается подход, общий смысл которого заключается в разделении всех используемых в ИС атрибутов учетных записей пользователей на отдельные группы – группу атрибутов, общих для всей ИС, и несколько (по количеству ОС, используемых в ИС) групп атрибутов, так или иначе различающихся в конкретных ОС. При этом общие атрибуты будут иметь по одному значению, как и в подходе для однородной ИС, а различающиеся – одно или более значений, в зависимости от количества ОС, в которых они применимы. Фактически, различающиеся атрибуты представляются в нескольких экземплярах, каждый со своим значением. Соответственно, в каждой конкретной ОС будет использоваться группа общих атрибутов и соответствующая данной ОС группа различающихся атрибутов.

Реализация данного подхода в рамках исследования требует разработки

- модели состава атрибутов учетных записей пользователей в гетерогенной ИС;
- методики определения состава атрибутов учетных записей пользователей в гетерогенной ИС.

Для разработки модели рассмотрим, из чего состоит учетная запись пользователя. Она представляет собой определенный набор атрибутов пользователя (таких, как идентификатор (логин), пароль, полное имя пользователя и т.п.) и их значений, на которые могут накладываться различного рода ограничения в ОС.

Используемый в учетной записи пользователя набор атрибутов может существенно влиять на такие итоговые показатели ИС, как:

- удобство администрирования: чем меньше атрибутов используется, тем проще администратору безопасности настраивать учетные записи. Хорошей практикой в этом случае является использование только явно необходимых атрибутов для функционирования системы и выполнения задач администрирования, и отказ от использования чисто информационных (день рождения, домашний адрес пользователя);

- степень использования механизмов защиты: чем больше используется специфичных для конкретной ОС атрибутов, тем более полно могут применяться имеющиеся механизмы защиты, что приведет к повышению уровня защищенности ИС. Например, использование атрибутов механизма мандатного контроля целостности позволит применять его в ИС;

- соответствие требованиям безопасности информации: применение определенных атрибутов может являться обязательным для выполнения отдельных требований безопасности. Например, без использования атрибутов, относящихся к мандатному контролю доступа (минимальный и/или максимальный уровень конфиденциальности, доступные мандатные категории и т.п.), выполнение нормативного требования по реализации данного механизма окажется невозможным.

В условиях, когда в ИС используются две или более различные ОС, поддерживаемые ими атрибуты учетных записей можно разделить на общие для всех применяемых ОС и различающиеся, а различия атрибутов – на форматные, содержательные и структурные.

К форматным различиям отнесем случаи, когда однотипные атрибуты учетных записей в разных ОС имеют ограничения по формату – длине, допустимым наборам символов и т.п. Подобные различия можно наблюдать в любых ОС на примере атрибута идентификатора (имени, логина) пользователя.

К содержательным различиям отнесем случаи, когда сами атрибуты в разных ОС совпадают, но различаются их значения. Характерный пример – привилегии пользователя, набор которых может отличаться не только у разных ОС, но и у различных версий одной и той же ОС.

К структурным различиям отнесем случаи, когда в разных ОС присутствуют специфичные для данных ОС (или групп ОС) атрибуты. Например, в ОС на базе UNIX/Linux одним из базовых атрибутов является основная (или первичная) группа пользователя, в то время как в ОС семейства Windows такой атрибут отсутствует в принципе. Другим показательным

примером являются атрибуты мандатного контроля целостности, в том или ином виде присутствующие в ОС семейства Windows и ОС Astra Linux, но отсутствующие в защищенной ОС реального времени «Нейтрино», поскольку в ней такой механизм не реализован.

Необходимо отметить, что при использовании в ИС различных ОС вполне возможна ситуация, когда совпадающие атрибуты в принципе отсутствуют, а даже самые базовые атрибуты (логин, пароль, Ф.И.О. пользователя) попадают в группу с как минимум форматными различиями. В то же время при использовании нескольких версий одной ОС, напротив, большая часть атрибутов может оказаться в группе совпадающих, а количество различающихся тем или иным образом будет минимальным, вплоть до их полного отсутствия (что не относится к гетерогенной ИС).

С учетом вышесказанного, сформируем модель состава атрибутов учетных записей в гетерогенной ИС.

Обозначим множество ОС, используемых в ИС, как $OS = \{os_1, os_2, \dots, os_n\}$, где os_i – конкретная ОС (или даже конкретная версия ОС в случаях, когда в разных версиях ОС атрибуты учетных записей различаются; далее для упрощения изложения будем говорить только об ОС в целом); n – количество ОС, используемых в ИС. Здесь ограничение множества по фактору использования ОС в ИС является крайне важным, так как именно данное ограничение определяет, какие атрибуты в данной ИС будут общими (совпадающими), а какие различными.

Обозначим как AC_i множество атрибутов, планируемых к применению в os_i (состав атрибутов учетной записи для os_i). Изначально закладываем в модель возможно неполный состав атрибутов, доступных для os_i , отфильтровывая непланируемые к использованию.

Из данного множества выделим следующие подмножества: G – множество атрибутов, общих для используемых ОС; F и C – множества атрибутов, присутствующих во всех используемых ОС, но имеющих форматные и содержательные различия соответственно; S_i – множество атрибутов, специфичных для os_i :

$$AC_i = G \cup F \cup C \cup S_i.$$

Введем также обозначение X^* – множество значений атрибутов (или, как вариант, кортежей атрибут–значение) из множества X .

Исходя из сущности атрибутов множества G следует отметить, что множество G^* будет единым для общей учетной записи. Напротив, для каждой используемой ОС (os_i) потребуется свое множество S_i^* . Что же касается множеств

F и C , то здесь ситуация уже не такая однозначная.

Рассмотрим несколько подходов по использованию атрибутов с форматными различиями.

Первый подход предусматривает унификацию атрибутов, то есть введение таких ограничений на значения атрибутов, которые удовлетворяют требованиям всех используемых ОС и при этом не создают существенных с точки зрения эффективности защиты информации ограничений. При таких ограничениях фактически F оказывается подмножеством G , поэтому, как следствие, получаем $AC_i = G \cup C \cup S_i$. Такой подход, очевидно, упрощает модель и ее реализацию, однако не всегда возможен, так как ограничения в различных ОС могут быть несовместимыми между собой.

Второй подход, напротив, предполагает полное дифференцирование (независимость) атрибутов с форматными различиями для каждой из используемых ОС. В этом случае множества F и G будут непересекающимися, а для каждой из используемых ОС будет задано свое множество значений F_i^* . К достоинствам такого подхода можно отнести гарантированную возможность соблюдения действующих в ОС ограничений на значения атрибутов, недостатком же является увеличение объема информации в учетной записи, зачастую с ее дублированием.

Третий подход является гибридом первого и второго и предусматривает разделение атрибутов с форматными различиями на два непересекающихся подмножества – унифицированные (Fu – атрибуты, для которых возможна безопасная унификация) и дифференцированные (Fd – не подвергнутые унификации атрибуты). Он позволит найти компромиссное для конкретных ситуаций решение и соблюсти разумный баланс между простотой структуры учетной записи (и, как следствие, удобством администрирования) и эффективностью применения механизмов защиты отдельных ОС.

Поскольку при последнем подходе атрибуты из множества Fu фактически становятся общими во всех ОС, можно объединить их с множеством G : $GFu = G \cup Fu$. Аналогично атрибуты из множества Fd фактически становятся специфичными для используемых ОС, что позволяет совместить их с множеством S_i : $SFdi = S_i \cup Fd$. Таким образом, атрибуты из множества F распределяются между множествами GFu и $SFdi$, получая в результате $AC_i = GFu \cup C \cup SFdi$.

Аналогично возможно дополнить множество $SFdi$ множеством C атрибутов с содержа-

тельными различиями ($SFdC_i = SFd_i \cup C$), так как для каждой из используемых ОС будет задано свое множество значений C_i^* ; в итоге получим $AC_i = GFu \cup SFdC_i$.

По результатам описанных трансформаций состав учетной записи можно представить как две группы атрибутов, к первой относятся общие и унифицированные, имеющие по единому значению для всех ОС, ко второй – дифференцированные и специфичные, имеющие отдельные значения для используемых ОС. Как видно, такой результат полностью соответствует предлагаемому в данной статье подходу.

Типичной для гетерогенной ИС является ситуация, когда у одного и того же пользователя может возникнуть потребность работать в нескольких (а возможно, и во всех) ОС, используемых в ИС. В соответствии с этим состав общей учетной записи пользователя (для всех используемых ОС) можно представить в виде множества

$$AC = GFu \cup \bigcup_{i=1}^n SFdC_i.$$

Описанная выше модель позволяет полноценно настроить учетную запись пользователя в любой из используемых ОС.

В качестве оптимизации модели на этапе реализации (с точки зрения исключения ненужной информации) можно удалить из объединения в правой части выражения множества атрибутов, не требуемых в реальности (когда пользователю не нужно работать с одной или несколькими ОС). При такой оптимизации состав атрибутов общей учетной записи k -го пользователя примет следующий вид:

$$AC_k = GFu \cup \bigcup_{i \in I_k} SFdC_i,$$

где I_k – множество индексов ОС, с которыми требуется работать k -му пользователю.

На основе описанной выше модели сформулируем методику определения состава атрибутов учетных записей пользователей в гетерогенной ИС.

– Выявление перечня ОС, используемых в рассматриваемой ИС (множество OS). Если предполагается использование нескольких версий одной и той же ОС и при этом в разных версиях ОС атрибуты учетных записей различаются, то каждая конкретная версия ОС учитывается отдельно.

– Выявление множества AC_i атрибутов, планируемых к применению, для каждой из используемых ОС. Отбор из полного перечня

имеющихся для данной ОС атрибутов осуществляется экспертным методом с учетом планируемых к использованию механизмов защиты и функциональных задач ИС. Кроме того, такой отбор уменьшит объем действий по следующим шагам методики.

– Выявление множества G общих для всех используемых ОС атрибутов учетных записей.

– Выявление множества F атрибутов, имеющих форматные отличия.

– Выявление множества Fu атрибутов, которые могут быть унифицированы без нарушения требований по безопасности, а также прочих требований, предъявляемых в ИС. Оценка возможности унификации производится экспертным методом.

– Формирование множества GFu общих и унифицированных атрибутов.

– Формирование множества Fd дифференцированных атрибутов.

– Выявление множества C атрибутов с содержательными различиями.

– Выявление множеств S_i специфичных атрибутов для каждой из используемых ОС.

– Формирование множества $SFdC_i$ дифференцированных и специфичных атрибутов.

– Определение итогового состава атрибутов общей учетной записи AC .

Выходными данными методики являются множества GFu , $SFdC_i$ и AC .

Описанная методика может применяться разработчиками системы защиты информации гетерогенной ИС при ее проектировании или модернизации. Результаты применения методики могут использоваться в качестве исходных данных для проектирования и реализации системы управления учетными записями пользователей ИС в части состава их атрибутов. Эти исходные данные должны использоваться для настройки существующих средств хранения и тиражирования данных учетных записей (таких, как *IdM*- или *IAM*-системы, службы каталогов) либо для проектирования вновь разрабатываемых программных средств.

При условии создания и поддержания в актуальном состоянии БД атрибутов учетных записей и ограничений на них для различных типов и версий ОС возможна практически полная автоматизация описанной методики (за исключением шагов отбора планируемых к применению атрибутов и оценки возможности унификации атрибутов). Также необходимо отметить, что количество ОС, используемых при создании ИС в защищенном исполнении, весьма невелико, и обычно используются ОС, сертифицированные на соответствие требованиям

по безопасности (<https://reestr.fstec.ru/reg3>). Кроме того, учитывая высокую степень регламентированности вопросов информационной безопасности в Российской Федерации (для информационных систем персональных данных, государственных информационных систем, значимых объектов критической инфраструктуры и т.п.), при создании таких ИС широко принята практика предъявления типовых требований по безопасности [1]. Как следствие, результаты выполнения методики для одной ИС могут затем повторно использоваться для похожих.

Недостатком предлагаемой методики является отсутствие формализации шагов отбора планируемых к применению атрибутов и оценки возможности унификации атрибутов и, как следствие, необходимость использования для оценки экспертного метода. Однако данный недостаток не является существенным, так как результаты экспертной оценки зачастую также могут использоваться повторно.

Заключение


В настоящем исследовании представлен новый подход к организации учетных записей пользователей в гетерогенных ИС, основанный на разделении атрибутов учетных записей на

группы общих и специфичных. В рамках данного подхода разработана модель состава атрибутов учетных записей пользователей, а на ее основе создана методика определения состава атрибутов учетных записей для набора ОС, используемых в гетерогенной ИС. Применение представленного подхода в ходе проектирования или модернизации системы защиты информации гетерогенной ИС позволит упростить (в части управления учетными записями) централизацию управления комплексом СРЗИ, используемым в ИС, и сократить объем технических и человеческих ресурсов, необходимых для управления, без потери при этом эффективности защиты информации.

В качестве направления дальнейшего развития рассматривается проработка формализации процессов отбора планируемых к применению атрибутов и оценки возможности и безопасности унификации атрибутов учетных записей в соответствии с заданными требованиями по безопасности информации. Решение этой задачи позволит повысить степень обоснованности разделения атрибутов на группы, а также даст возможность полноценной автоматизации процесса определения состава атрибутов учетных записей для гетерогенных ИС.

Список литературы

1. Алексеев В.В., Емельянов Е.В., Кастерин Д.А., Стрельцов А.А. Правовой подход к построению системы защиты информации в организации // Правовая информатика. 2020. № 2. С. 54–61.
2. Липаев В.В. Экономика производства сложных программных продуктов. М.: СИНТЕГ, 2008. 432 с.
3. Богаченко Н.Ф. Анализ проблем управления разграничением доступа в крупномасштабных информационных системах // Математические структуры и моделирование. 2018. № 2. С. 135–152.
4. Nielsen C.B., Larsen P.G., Fitzgerald J. et al. Systems of systems engineering: Basic concepts, model-based techniques, and research directions. ACM Computing Surveys, 2015, vol. 48, no. 2, art. 18. doi: 10.1145/2794381.
5. Богаченко Н.Ф. О сложности подсистем разграничения доступа крупномасштабных информационных систем // Математические структуры и моделирование. 2018. № 4. С. 92–98. doi: 10.24147/2222-8772.2018.4.92-98.
6. Мажорова А.О. Преимущества и варианты внедрения identity management system // Вопросы науки и образования. 2018. № 8. С. 43–44.
7. Максудов М.О., Дорошенко И.Е., Селифанов В.В. Проблемы формирования структуры функций системы управления информационной безопасностью значимого объекта критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2022. № 6. С. 143–148. doi: 10.33764/2618-981X-2022-6-143-148.
8. Boranbayev A., Mazhitov M., Yamalutdinov R. Managing user accounts across heterogeneous information systems in the university. Proc. Int. Conf. SERP, 2013, pp. 83–87.
9. Петров М.А. Моделирование процесса интеграции IdM системы с управляемой информационной системой // Вестн. науки. 2024. Т. 1. № 8. С. 146–153.
10. Плетнев А.В., Поляков С.В. Организация разграничения доступа пользователей к функционалу информационной системы // EESJ. 2022. Т. 1. № 1. С. 28–35. doi: 10.31618/EESA.2782-1994.2022.1.77.232.
11. Петров М.А. Основные компоненты автоматизированной системы управления доступом к информационным ресурсам // Вестн. науки. 2024. № 8. С. 154–159.

Defining the set of user account attributes for centralized administration of heterogeneous systemsAleksey Yu. Efimov ¹ Research Institute Centerprogramsistem,
Tver, 170024, Russian Federation**For citation**Efimov, A.Yu. (2025) 'Defining the set of user account attributes for centralized administration of heterogeneous systems', *Software & Systems*, 38(4), pp. 637–643 (in Russ.). doi: 10.15827/0236-235X.152.637-643**Article info**

Received: 09.06.2025

After revision: 19.06.2025

Accepted: 20.06.2025

Abstract. To improve information security efficiency and minimize resource requirements, centralized management of protection mechanisms is used in complex information systems. The paper focuses on addressing user account management challenges, specifically organization of account attributes within heterogeneous information systems. The relevance of the issue is confirmed by problems due to differences in the implementation of security mechanisms, particularly user account management systems, across information system components. The author examines existing problem-solving methods and highlights the role of user account attribute sets in ensuring interoperability within heterogeneous information systems. A new effective methodology for account management introduces attribute similarity assessment across different operating system platforms and subsequent categorization into universal and platform-specific groups. The paper describes four key components: a user account attribute set model for user accounts in heterogeneous systems; a corresponding methodology for attribute specification; evaluation of the approach's advantages and limitations; and practical application requirements and methods. The author also identifies directions for future research. Implementing this approach will simplify centralized administration of information security systems and reduce required administrative resources without compromising protection effectiveness.

Keywords: information protection, information security, centralized administration, heterogeneous information system, operating system, user account, attribute

References

1. Alekseev, V.V., Emelyanov, E.V., Kasterin, D.A., Streltsov, A.A. (2020) 'A legal approach to building an information protection system in an organization', *Legal Informatics*, (2), pp. 54–61 (in Russ.).
2. Lipaev, V.V. (2008) *Economics of Complex Software Production*. Moscow, 432 p. (in Russ.).
3. Bogachenko, N.F. (2018) 'The analysis of problems of access control administration in large-scale information systems', *Math. Structures and Modeling*, (2), pp. 135–152 (in Russ.).
4. Nielsen, C.B., Larsen, P.G., Fitzgerald, J. et al. (2015) 'Systems of systems engineering: basic concepts, model-based techniques, and research directions', *ACM Computing Surveys*, 48(2), art. 18. doi: 10.1145/2794381.
5. Bogachenko, N.F. (2018) 'On the complexity of access control subsystems of large-scale complex IT systems', *Math. Structures and Modeling*, (4), pp. 92–98 (in Russ.). doi: 10.24147/2222-8772.2018.4.92-98.
6. Mazhorova, A.O. (2018) 'Advantages and implementation options of identity management system', *Problems Sci. and Education*, (8), pp. 43–44 (in Russ.).
7. Maksudov, M.O., Doroshenko, I.E., Selifanov, V.V. (2022) 'Problems of forming the structure of functions of the information security management system of a significant object of critical information infrastructure', *Interexpo Geo-Siberia*, (6), pp. 143–148 (in Russ.). doi: 10.33764/2618-981X-2022-6-143-148.
8. Boranbayev, A., Mazhitov, M., Yamalutdinov, R. (2013) 'Managing user accounts across heterogeneous information systems in the university', *Proc. Conf. SERP*, pp. 83–87.
9. Petrov, M.A. (2024) 'Modeling process of integrating IdM system with managed information system', *Bull. of Sci.*, 1(8), pp. 146–153 (in Russ.).
10. Pletnev, A.V., Polyakov, S.V. (2022) 'Organization of user access differentiation to information system functionality', *EESJ*, 1(1), pp. 28–35. doi: 10.31618/EESA.2782-1994.2022.1.77.232.
11. Petrov, M.A. (2024) 'Main components of automated access control system for information resources', *Bull. of Sci.*, (8), pp. 154–159 (in Russ.).

АвторыЕфимов Алексей Юрьевич ¹,
зам. директора, efimovay@cps.tver.ru**Authors**Aleksey Yu. Efimov ¹,
Deputy Director, efimovay@cps.tver.ru¹ НИИ «Центрпрограммсистем»,
г. Тверь, 170024, Россия¹ Research Institute Centerprogramsistem,
Tver, 170024, Russian Federation