ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71753— 2024

Защита информации

СИСТЕМЫ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ И ПРАВАМИ ДОСТУПА

Общие требования

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Обществом с ограниченной ответственностью «СОЛАР СЕКЬЮРИТИ» (ООО «СОЛАР СЕКЬЮРИТИ»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 октября 2024 г. № 1558-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2024

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 4
5 Общие положения 4
6 Уровень 1: управление объектами информационных ресурсов 6
7 Уровень 2: управление правами доступа пользователей 10
8 Общие требования к управлению учетными записями и правами доступа в контролируемых информационных системах 18
9 Уровни контроля за учетными записями и правами доступа в информационных системах 19
10 Меры защиты информации в системе управления учетными записями и правами доступа 20
Приложение А (справочное) Основные процессы управления учетными записями и правами доступа пользователей 24
Библиография 34

Введение

Одной из главных задач защиты информации при ее автоматизированной (автоматической) обработке является управление правами доступа. Какими бы совершенными ни были средства, разграничивающие права доступа к информации и пресекающие несанкционированный доступ к ней, они не позволяют защититься от действий пользователей, имеющих легальный доступ к защищаемой информации. При этом нельзя исключать возможность предоставления ошибочного, избыточного доступа пользователям, а также гарантировать своевременное прекращение доступа пользователей по истечении сроков предоставления доступа или изменения статуса пользователя, например при увольнении.

Системы, автоматизирующие управление учетными записями и правами доступа пользователей, позволяют своевременно предоставлять доступ пользователям и прекращать доступ пользователей к информационным ресурсам в сложных гетерогенных системах, состоящих из большого количества подсистем с собственными механизмами идентификации и аутентификации.

Подобные системы позволяют автоматизировать процесс согласования доступа пользователей на основе ролевой модели организации и электронных заявок на управление правами доступа пользователей. Наличие матрицы легальных прав доступа пользователей позволяет осуществлять контроль соответствия легальных и фактических прав доступа пользователей в информационных системах. В случае обнаружения нелегальных прав доступа пользователей об этом информируются ответственные лица и принимаются необходимые меры.

Для контроля соответствия легальных прав доступа пользователей в информационных системах политике информационной безопасности организации в системах автоматизации управления учетными записями и доступом пользователей могут применяться дополнительные средства контроля на основе правил проверки соответствия прав доступа пользователей политике ИБ.

Системы, автоматизирующие управление учетными записями и правами доступа пользователей, могут использоваться как средства защиты информации при построении подсистем информационной безопасности в сложных гетерогенных информационных системах. Они позволяют реализовать часть мер защиты информации, связанных с управлением учетными записями и правами доступа пользователей.

Для понимания положений настоящего стандарта необходимы знания основ информационных технологий, а также способов защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

СИСТЕМЫ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ И ПРАВАМИ ДОСТУПА

Общие требования

Information protection.
Automatic accounts and access management systems.
General requirements

Дата введения — 2024—12—20

1 Область применения

Настоящий стандарт устанавливает общие требования к системам управления учетными записями и правами доступа пользователей и автоматизации процессов, связанных с управлением учетными записями и правами доступа.

Для процессов, связанных с управлением учетными записями и правами доступа, определяются состав участников и содержание процессов, подлежащих автоматизации, и даются общие рекомендации по разработке и внедрению систем управления учетными записями и правами доступа пользователей.

Положения данного стандарта не описывают детальные требования к управлению учетными записями и правами непосредственно в контролируемых информационных системах, так как подход к реализации управления учетными записями и правами доступа определяется архитектурой конкретных систем. Устанавливаются общие требования по реализации процессов управления в ИС.

Стандарт предназначен для организаций, занимающихся разработкой и внедрением подобных систем, а также организаций, использующих или планирующих использовать подобные системы.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 33707 (ISO/IEC 2382:2015) Информационные технологии. Словарь

ГОСТ Р ИСО/МЭК 15504-2 Информационная технология. Оценка процесса. Часть 2. Проведение оценки

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 59383 Информационная технология. Методы и средства обеспечения безопасности. Основы управления доступом

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом ут-

Издание официальное

верждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 50922, ГОСТ 33707, а также следующие термины с соответствующими определениями:

3.1 **атрибут объекта:** Элемент данных объекта, который задает наименование, формат, диапазон возможных значений и представление значений при обращении.

Примечание — В качестве объектов могут выступать элементы кадровых данных, объекты каталога пользователей, контролируемые объекты информационной системы.

3.2 **бизнес-роль:** Роль, не привязанная к конкретной контролируемой информационной системе и используемая для формирования стандартного набора прав доступа, необходимого для выполнения определенной задачи, выполняемой в рамках какого-либо бизнес-процесса организации.

3.3 **групповые права доступа пользователя:** Права доступа пользователя к информационным ресурсам, предоставленные автоматически на основании правил, настроенных в системе управления учетными записями и правами доступа.

Примечание — Правила могут предоставлять права доступа пользователю на основании его положения в организационно-штатной структуре организации или иных атрибутов пользователя.

3.4 **единый каталог пользователей:** Каталог системы управления учетными записями и правами доступа, использующийся для хранения перечня пользователей, их данных, ролей, учетных записей и их прав, а также организационно-штатной структуры организации, с указанием позиций, занимаемых в ней пользователями.

3.5 **инвентаризация контролируемых объектов информационной системы:** Процедура определения перечня контролируемых объектов информационной системы, их владельцев, уровней критичности, подтверждения соответствия состояния контролируемых объектов правилам информационной безопасности, установленным в организации.

3.6 **индивидуальные права доступа пользователя:** Права доступа пользователя к информационным ресурсам, предоставленные пользователю персонально на основании запроса в системе управления учетными записями и правами доступа либо в результате легализации уже имеющихся прав доступа к информационным ресурсам.

3.7

информационная система; ИС: Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

[[1], статья 2, пункт 3]

3.8 **информационный ресурс;** ИР: Именованный элемент контролируемой информационной системы, использующийся в модели разграничения доступа информационной системы как объект доступа.

3.9 **источник кадровых данных:** Информационная система, подключенная к системе управления учетными записями и правами доступа, являющаяся источником данных о сотрудниках и об организационно-штатной структуре организации.

3.10 **ИТ-роль:** Роль, относящаяся к конкретной контролируемой информационной системе и используемая для формирования стандартного набора прав доступа в данной информационной системе.

Примечание — Как правило, ИТ-роль соответствует какой-либо функции, выполняемой пользователем в данной информационной системе.

3.11 **коннектор:** Отчуждаемый программный модуль, используемый для интеграции системы управления учетными записями и правами доступа и контролируемой информационной системы или чтения источника кадровых данных, имеющий стандартизованный для данной системы управления учетными записями и правами доступа программный интерфейс.

Примечание — В коннекторе реализуются процедуры чтения, создания, изменения, удаления контролируемых объектов информационной системы.

3.12 **контролируемая информационная система:** Система, подключенная к системе управления учетными записями и правами доступа, в которой осуществляется управление и/или контроль учетных записей и прав доступа пользователей.

3.13 **контролируемый объект информационной системы:** Объект информационной системы, используемый для разграничения доступа пользователей в информационной системе.

Примечания

1 Контролируемыми объектами в информационной системе обычно являются учетные записи, организационные единицы, роли либо группы, информационные ресурсы, права доступа.

2 Номенклатура таких объектов зависит от архитектуры конкретной информационной системы.

3.14 **критический информационный ресурс:** Информационный ресурс, получение доступа к которому нарушителем информационной безопасности организации может нанести значительный ущерб.

3.15 **легальные права доступа:** Права доступа пользователя к информационным ресурсам, предоставленные в установленном в организации порядке.

3.16

нарушитель информационной безопасности организации: Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

[ГОСТ Р 53114—2008, статья 3.3.5]

3.17

несанкционированный доступ: Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

[ГОСТ Р 53114—2008, статья 3.3.6]

3.18 **обратная синхронизация:** Процесс передачи данных контролируемой информационной системы или источника кадровых данных в систему управления учетными записями и правами доступа, связанный с созданием, изменением или удалением объектов единого каталога пользователей.

3.19 **организационная единица:** Элемент организационно-штатной структуры организации, подразделение с перечнем находящихся в нем сотрудников.

3.20 **организационно-штатная структура организации:** Схематическое представление структуры организационных единиц организации в порядке существующей иерархии, а также перечень должностей в организационных единицах и перечень сотрудников.

Примечание — Организационно-штатная структура организации может храниться в кадровой системе организации, едином каталоге пользователей системы управления учетными записями и правами доступа и частично в контролируемых информационных системах (структура организационных единиц).

3.21 **парольная политика:** Набор правил, определяющих требования к паролям и способам их создания и изменения, а также правила использования паролей в информационной системе.

3.22

политика информационной безопасности (организации): Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

[ГОСТ Р 53114—2008, статья 3.2.18]

3.23 **пользователь:** Лицо, имеющее учетную запись в контролируемых ИС и доступ к ИР организации.

Примечание — Пользователями могут быть сотрудники организации и лица, имеющие договорные отношения с организацией и выполняющие работы с использованием ИР организации.

3.24 **право доступа:** Право, предоставленное пользователю на санкционированное использование информационных ресурсов.

3.25 **прямая синхронизация:** Процесс передачи данных из системы управления учетными записями и правами доступа в контролируемую информационную систему, связанный с созданием, изменением или удалением контролируемых объектов информационной системы.

3.26 **ролевая модель организации:** Набор стандартных шаблонов прав доступа (ролей) к информационным ресурсам организации, а также правила автоматического назначения ролей пользователям организации.

3.27 **система управления учетными записями и правами доступа;** СУУЗиПД: Система, осуществляющая централизованное, автоматизированное управление учетными записями пользователей и правами доступа в информационных системах на основании настроенных правил и запросов пользователей.

3.28 **учетная запись;** УЗ: Логический объект, существующий в пределах одной или нескольких информационных систем и представляющий субъект доступа в ее (их) пределах.

3.29 **фактические права доступа:** Права доступа пользователя к информационным ресурсам, фактически предоставленные пользователю в контролируемой информационной системе.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ИБ — информационная безопасность;
ИТ — информационные технологии;
РД — руководящий документ;
СУБД — система управления базами данных;
ФИО — фамилия, имя, отчество;
API — прикладной программный интерфейс (application programming interface);
HTTPS — безопасный протокол передачи гипертекста (hypertext transfer protocol secure);
LDAP — легковесный протокол доступа к каталогам (lightweight directory access protocol);
OpenID — открытый стандарт децентрализованной системы аутентификации (open identifier);
URL — унифицированный указатель ресурса (uniform resource locator).

5 Общие положения

5.1 Целью процесса управления УЗ и правами доступа является обеспечение своевременного предоставления пользователям доступа к ИР организации и гарантий того, что всем УЗ пользователей в ИС доступ к ИР предоставлен в соответствии с правилами политики ИБ организации.

5.2 Для достижения данной цели должно обеспечиваться выполнение следующих требований:

- все УЗ пользователей в ИС должны быть инвентаризованы и привязаны к конкретным пользователям;
- должны быть инвентаризованы все ИР в ИС, доступ к которым в соответствии с установленными в организации правилами должен разграничиваться. Права доступа УЗ к ИР также должны быть инвентаризованы;
- все УЗ пользователей в ИС должны создаваться, изменяться, блокироваться/разблокироваться и удаляться в соответствии с установленными правилами;
- права доступа учетных записей к ИР в ИС должны быть предоставлены в соответствии с установленными правилами. Любые изменения прав доступа УЗ к ИР должны осуществляться в соответствии с установленными правилами;
- любые несанкционированные изменения УЗ и их прав доступа к ИР должны выявляться. По фактам несанкционированных изменений должны оповещаться ответственные лица и проводиться расследование в установленном порядке.

5.3 Управление УЗ и правами доступа с применением СУУЗиПД в общем случае охватывает:

- процессы ведения единого каталога пользователей;
- процессы создания, изменения, блокирования/разблокирования и удаления УЗ пользователей в ИС;
- контроль соблюдения парольной политики для паролей УЗ пользователей в ИС;
- процессы назначения прав доступа УЗ к ИР на основании ролевой модели;

- ведение ролевой модели организации;
- контроль за соблюдением политики ИБ в части прав доступа УЗ к ИР.

5.4 Применение СУУЗиПД позволяет установить единые правила управления правами доступа в различных ИС организации и контролировать их соблюдение при помощи автоматизированных средств. Тем самым решается как задача обеспечения непрерывности контроля за соблюдением политики ИБ организации, так и задача минимизации затрат на предоставление пользователям доступа и обеспечение контроля за соблюдением политики ИБ.

5.5 С целью систематизации функций и процессов СУУЗиПД выделяют следующие функциональные уровни, как показано на рисунке 1:

- уровень 1 — уровень управления объектами ИС, связанными с УЗ и правами доступа. На данном уровне сосредоточены функции и процессы, обеспечивающие управление единым каталогом пользователей и связанными с пользователями контролируемыми объектами ИС;
- уровень 2 — уровень процессов управления правами доступа пользователей. На данном уровне сосредоточены функции и процессы согласования и управления правами доступа пользователей, контролем соответствия легальных и фактически предоставленных прав доступа в ИС;
- уровень 3 — уровень контроля за соответствием прав доступа пользователей требованиям РД: регламентов и политики ИБ организации, стандартов, рекомендаций, законов и подзаконных актов. Также к этому уровню относятся средства контроля численных показателей защищенности и рисков.



Рисунок 1 — Функциональные уровни СУУЗиПД

5.6 Такое разделение позволяет оценить потребность организаций в системах соответствующего класса с точки зрения зрелости процессов самой организации. Данные уровни соответствуют уровням 2, 3 и 4 возможностей процесса (в данном случае — процесса управления правами доступа пользователей в организации), описанным в ГОСТ Р ИСО/МЭК 15504-2. Указанное разделение позволяет классифицировать существующие СУУЗиПД с точки зрения реализации в них функциональных уровней:

- СУУЗиПД, управляющие контролируемыми объектами ИС, — системы, осуществляющие синхронизацию контролируемых объектов в разных ИС с использованием информации из источников кадровых данных на основании настроенных правил;
- СУУЗиПД, управляющие правами доступа пользователей, — системы, осуществляющие синхронизацию контролируемых объектов ИС, а также реализующие процессы управления правами доступа пользователей в организации и контролирующие легальность прав доступа пользователей;
- СУУЗиПД, контролирующие соответствие РД, — системы, осуществляющие управление правами доступа пользователей, а также контролирующие соответствие прав доступа пользователей РД и численные показатели защищенности и рисков.

5.7 Предметом рассмотрения данного стандарта являются первые два уровня СУУЗиПД, относящиеся непосредственно к процессам управления УЗ и правами доступа. Требования на уровне 3 будут изложены в нормативном документе, содержащем описание методов контроля соответствия требованиям и оценки уровня защищенности, реализуемых в СУУЗиПД.

6 Уровень 1: управление объектами информационных ресурсов

6.1 Единый каталог пользователей

6.1.1 Основной задачей СУУЗиПД на данном уровне является формирование единого каталога пользователей (как внутренних, так и внешних) для организации.

6.1.2 Единый каталог пользователей должен являться частью СУУЗиПД и использоваться для хранения следующей информации об организации:

- организационно-штатной структуры организации с иерархией организационных единиц, их атрибутами, перечнем должностей в организационных единицах, информацией о руководителях организационных единиц;
- перечня пользователей организации с указанием позиций, занимаемых ими в организационно-штатной структуре, их атрибутов, ролей и УЗ.

6.1.3 Источниками данных для формирования единого каталога пользователей могут являться:

- источники кадровых данных;
- реестры пользователей (например, реестры контрагентов или клиентов);
- данные, введенные пользователями СУУЗиПД, имеющими права доступа для управления единым каталогом пользователей.

6.1.4 В едином каталоге пользователей должна храниться только информация, необходимая для управления УЗ и правами доступа пользователя. Для СУУЗиПД должны быть определены типы персональной информации пользователей, необходимой для функционирования СУУЗиПД (например, ФИО, контакты, место работы и т. п.). Хранение в едином каталоге пользователей иной персональной информации пользователей не допускается.

6.1.5 В связи с тем, что в разных организациях правила управления УЗ и правами пользователей отличаются, СУУЗиПД должна поддерживать настройку перечня хранимых и обрабатываемых данных пользователей в едином каталоге пользователей.

6.1.6 Для каждого пользователя в едином каталоге пользователей должна храниться информация о его правах доступа в контролируемых ИС. Эта информация используется при предоставлении прав доступа УЗ пользователей.

6.1.7 В едином каталоге пользователей должна храниться информация об УЗ пользователей в контролируемых ИС. Все пользовательские УЗ в контролируемых ИС должны быть привязаны к соответствующему пользователю в едином каталоге пользователей.

6.1.8 Для упрощения работы с перечнем пользователей в едином каталоге пользователей и для группового управления доступом в СУУЗиПД должна использоваться одна или более иерархий организационных единиц. Организационные единицы образуют древовидную структуру, в которой размещаются пользователи.

6.1.9 Для указания позиции пользователя в каждой организационной единице должен использоваться соответствующий признак — должность.

6.1.10 Иерархия организационных единиц и должностей в них должна формироваться вне зависимости от наличия в данной структуре сотрудников. В СУУЗиПД должна иметься возможность создания пустых организационных единиц и незамещенных должностей.

6.1.11 Единый каталог пользователей должен обеспечивать возможность помещения одного пользователя в различные организационные единицы и на различные должности внутри одной организационной единицы. Для каждой позиции пользователя внутри организационно-штатной структуры в СУУЗиПД должна иметься возможность раздельного управления перечнем прав доступа пользователя (более подробно требования к управлению правами доступа пользователей описаны в 7.3 и 7.4).

6.1.12 Поскольку информация об организационной единице и должности пользователя может использоваться для группового управления правами доступа, СУУЗиПД должна поддерживать обновление данной информации вручную или на основании кадровых данных, поступающих из источников кадровых данных.

6.1.13 Операция перевода пользователя в другую организационную единицу или на другую должность должна осуществляться вручную или при поступлении информации о переводе сотрудника в источнике кадровых данных в момент наступления даты соответствующего кадрового события перевода сотрудника.

6.1.14 В процессе обработки операции перевода пользователя СУУЗиПД должна переместить пользователя на новую позицию в организационно-штатной структуре в едином каталоге пользователей.

6.1.15 После перемещения пользователя в едином каталоге пользователей должна быть обновлена информация в УЗ пользователя в контролируемых ИС согласно настроенным правилам.

6.1.16 При наличии у пользователя групповых прав доступа, основанных на информации об организационной единице и должности пользователя, перемещение пользователя должно сопровождаться пересмотром его прав доступа, описанным в 7.5.

6.1.17 В едином каталоге пользователей для каждого пользователя должен присутствовать специальный атрибут — статус пользователя. Данный атрибут используется для управления статусом УЗ пользователя в контролируемых ИС.

6.1.18 Как минимум должны поддерживаться следующие статусы пользователя:

- работает — пользователь в настоящее время работает;
- не работает — пользователь временно не работает по причине отпуска, больничного и т. д.;
- уволен — пользователь в настоящее время уволен.

6.1.19 В СУУЗиПД для каждой контролируемой ИС должна обеспечиваться возможность настройки выполняемых действий в отношении УЗ пользователя в случае изменения текущего статуса пользователя.

6.1.20 При изменении статуса пользователя должно поддерживаться (как минимум) выполнение следующих действий:

- блокирование/разблокирование УЗ пользователя;
- перемещение УЗ пользователя в отдельную организационную единицу (при наличии технической возможности для контролируемой ИС);
- изменение атрибутов УЗ пользователя;
- предоставление/прекращение прав доступа УЗ пользователя к каким-либо ИР;
- удаление УЗ пользователя (при наличии технической возможности для контролируемой ИС).

6.1.21 В СУУЗиПД могут быть добавлены дополнительные статусы для более гибкого управления пользовательскими УЗ. Например, могут использоваться дополнительные статусы: на больничном, в отпуске, в декретном отпуске и т. д. Для дополнительных статусов пользователя могут быть настроены соответствующие действия СУУЗиПД, осуществляемые в отношении его УЗ.

6.2 Синхронизация единого каталога пользователей

6.2.1 Организационно-штатная структура и перечень пользователей организации СУУЗиПД должны поддерживать процесс автоматической синхронизации единого каталога пользователей с источниками кадровых данных и дополнительных реестров пользователей. Синхронизация с единым каталогом пользователей показана на рисунке 2.

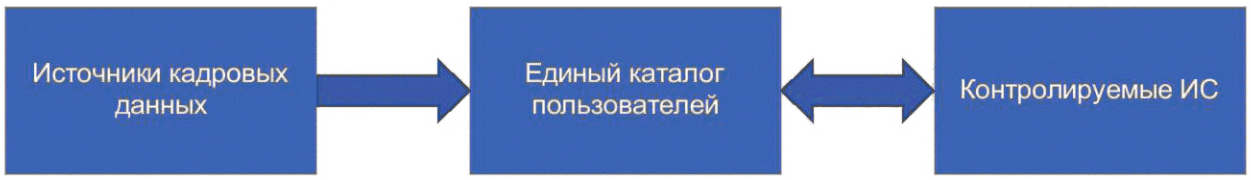

Рисунок 2 — Синхронизация с единым каталогом пользователей

6.2.2 При формировании единого каталога пользователей могут использоваться несколько источников данных. В этом случае в СУУЗиПД должны использоваться настраиваемые правила загрузки данных из источников для разрешения конфликтов в данных.

6.2.3 СУУЗиПД должна корректно обрабатывать ситуацию, когда данные одного и того же пользователя имеются в разных источниках данных. В этом случае СУУЗиПД по заранее настроенным прави-

лам должна идентифицировать данные этого пользователя в различных источниках и корректно осуществлять объединение данных пользователя при помощи соответствующих правил.

6.2.4 Правила должны позволять назначать приоритеты источников кадровых данных для каждого из атрибутов пользователя в едином каталоге пользователей. Должна поддерживаться возможность определения приоритетов на основании анализа информации из других атрибутов пользователя, полученных из кадровых данных, например даты изменения информации, типа пользователя, его положения в организационно-штатной структуре и т. д.

6.2.5 Единый каталог пользователей должен поддерживать ведение перечня пользователей, не являющихся сотрудниками организации, но имеющих УЗ в контролируемых ИС и имеющих доступ к ИР организации. Это должны быть пользователи, имеющие договорные отношения с организацией и выполняющие работы с использованием ИР организации.

6.2.6 Лица, ответственные за своевременное предоставление и прекращение доступа таких пользователей, определяются регламентом управления доступом организации. Данные ответственные лица на регулярной основе должны осуществлять контроль за актуальностью перечня внешних пользователей и вручную прекращать их доступ к ИР организации. Рекомендуется предоставлять данным пользователям временный доступ к ИР организации. В этом случае по истечении срока действия доступа СУУЗиПД автоматически должна лишить их доступа к ИР. Подробнее процесс предоставления временного доступа к ИР описан в 7.3.

6.2.7 Для пользователей, созданных в едином каталоге пользователей вручную, должна корректно обрабатываться ситуация с появлением их в источниках кадровых данных. В случае, если СУУЗиПД на основании правил сопоставления определяет, что данные пользователя, полученные из кадрового источника, соответствуют уже имеющемуся пользователю, должны осуществляться корректное связывание и заполнение недостающих данных пользователя в едином каталоге пользователей.

6.2.8 Для поддержания организационно-штатной структуры в актуальном состоянии СУУЗиПД должна синхронизировать ее с источниками кадровых данных. С кадровыми данными должна синхронизироваться следующая информация в едином каталоге пользователей:

- перечень, атрибуты и структура организационных единиц организации;
- перечень должностей организации и штатное расписание для каждой организационной единицы.

6.2.9 СУУЗиПД должна иметь настраиваемые механизмы контроля корректности получаемых кадровых данных перед использованием их для проведения синхронизации единого каталога пользователей. Должны отслеживаться (как минимум) следующие ситуации, возникающие при загрузке кадровых данных:

- отсутствие в загружаемых данных части организационно-штатной структуры или массовые операции по удалению или перемещению организационных единиц и должностей;
- отсутствие в загружаемых данных значительного количества пользователей организации или массовые операции по удалению или перемещению пользователей;
- массовые изменения атрибутов пользователей или организационных единиц.

6.2.10 Для указанных выше ситуаций в СУУЗиПД должна поддерживаться настройка порогов срабатывания блокировки подобных массовых изменений.

6.2.11 В случае срабатывания блокировки массовых изменений должно осуществляться оповещение администраторов СУУЗиПД. Администратор СУУЗиПД должен иметь возможность проанализировать кадровые данные, приведшие к срабатыванию механизмов блокировки, и разрешить соответствующие изменения, если они не связаны со сбоем механизмов выгрузки данных из кадровой системы и синхронизации единого каталога пользователей.

6.3 Управление учетными записями в контролируемых информационных системах

6.3.1 СУУЗиПД должна поддерживать создание УЗ в контролируемых ИС по настроенным правилам. Как минимум должны поддерживаться следующие правила создания УЗ:

- создание УЗ для любого пользователя, имеющегося в едином каталоге пользователей;
- создание УЗ при предоставлении пользователю первого права доступа к какому-либо ИР в соответствующей ИС;
- создание УЗ при предоставлении первого права доступа в ИС, использующей в качестве субъектов доступа УЗ другой ИС. В этом случае при предоставлении прав доступа к ИР УЗ создается в другой ИС. Такой сценарий реализуется для ИС, использующих внешние средства идентификации и аутентификации, например, для внешнего LDAP-каталога.

6.3.2 СУУЗиПД должна позволять определять правила соответствия атрибутов пользователя в едином каталоге пользователей и атрибутов УЗ пользователя в контролируемых ИС.

6.3.3 Данные правила должны действовать как при прямой синхронизации из единого каталога пользователей в контролируемую ИС, так и при обратной синхронизации из контролируемой ИС (или кадрового источника) в единый каталог пользователей.

6.3.4 Правила прямой и обратной синхронизации должны определяться раздельно для каждого атрибута.

6.3.5 В случаях, когда изменяемый атрибут еще не заполнен или когда он уже имеет некоторое значение, правила синхронизации должны определяться раздельно. Таким образом реализуется сценарий с приоритетом информации о пользователе, заполненной вручную.

6.3.6 Правила прямой и обратной синхронизации должны использоваться в следующих случаях:

- при создании/изменении УЗ пользователя в управляемой ИС правила используются для формирования новых значений атрибутов УЗ пользователя на основании данных единого каталога;
- при проверке соответствия атрибутов УЗ в ИС атрибутам пользователя правила используются для формирования эталонного значения атрибутов УЗ, сравниваемого с фактическим;
- при обратной синхронизации единого каталога с контролируемыми ИС или с данными кадрового источника правила используются для формирования значений атрибутов пользователя в едином каталоге на основании атрибутов УЗ в контролируемых ИС или кадровых данных.

6.4 Парольные политики в системе управления учетными записями и правами доступа

6.4.1 В СУУЗиПД должна поддерживаться настройка парольной политики для пользователей СУУЗиПД (при использовании в СУУЗиПД собственной идентификации и аутентификации) и УЗ в контролируемых ИС. Данные политики применяются при создании УЗ и смене пароля.

6.4.2 Генерация пароля может осуществляться по запросу пользователя (в случае утраты или компрометации пароля) и автоматически (в случае создания новой УЗ или истечения максимального срока действия пароля).

6.4.3 Ответственные лица, перечень которых определяется регламентом организации, должны иметь возможность запросить в СУУЗиПД сброс пароля для выбранной УЗ в ИС. Новый пароль должен вводиться пользователем, запросившим сброс пароля, или генерироваться СУУЗиПД автоматически. Новый пароль должен соответствовать настроенной парольной политике.

6.4.4 В случае генерации пароля новый пароль должен доставляться пользователю безопасным образом. Должны использоваться защищенные каналы связи либо специализированные средства безопасной передачи пароля (например, принтеры ПИН-конвертов).

6.4.5 Не допускается передача пароля по открытым каналам связи. Открытые каналы связи могут быть использованы только для оповещения об изменении пароля с передачей пользователю (или ответственному лицу) ссылки, по которой он может перейти в СУУЗиПД и после прохождения процедуры аутентификации получить пароль. После просмотра и подтверждения получения пароля в СУУЗиПД сохраненный пароль должен уничтожаться без возможности восстановления.

6.4.6 Ссылка должна направляться ответственному лицу только в случае, если до получения пароля пользователь не сможет самостоятельно пройти процедуру аутентификации в СУУЗиПД и получить пароль. Например, в случае создания УЗ пользователя в LDAP-каталоге, который используется как внешняя система аутентификации для СУУЗиПД. В противном случае ссылка должна направляться самому пользователю, пароль которого был изменен.

6.4.7 Парольная политика должна (как минимум) устанавливать следующие характеристики для пароля:

- задание минимальной сложности пароля с определяемыми при настройке требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов, минимальной и максимальной длине пароля;
- запрет на использование указанного количества ранее использованных паролей;
- задание минимального числа символов, различающихся в новом и старом пароле;
- ограничение максимального срока действия пароля;
- ограничение количества ошибочных попыток ввода пароля с указанием времени блокирования после достижения максимального числа попыток.

6.4.8 СУУЗиПД должна поддерживать возможность задания парольной политики отдельно для самой СУУЗиПД и для каждой из контролируемых ИС, а также отдельных политик для различных типов УЗ, классифицируемых по настраиваемым в СУУЗиПД правилам.

6.4.9 СУУЗиПД должна отслеживать срок действия как паролей пользователей, использующихся для аутентификации в самой СУУЗиПД, так и паролей в контролируемых ИС. В случае приближения истечения максимального срока действия пароля СУУЗиПД должна предоставлять возможность оповещения пользователя о необходимости смены пароля, а в случае отсутствия действий пользователя — по достижении максимального срока действия пароля предоставлять возможность автоматической смены пароля и передачи пользователю нового пароля с использованием механизмов, описанных выше.

6.4.10 Пароли пользователей в СУУЗиПД не должны храниться в открытом виде, доступном для просмотра эксплуатирующим персоналом или нарушителями, получившими несанкционированный доступ к СУУЗиПД. В случае хранения паролей пользователей в СУБД или конфигурационных файлах СУУЗиПД к паролям должно применяться необратимое преобразование (для постоянного хранения пароля, например для аутентификации пользователя или проверки соответствия политике) либо обратимое преобразование для паролей, временно хранящихся в СУУЗиПД до момента передачи их пользователю.

7 Уровень 2: управление правами доступа пользователей

7.1.1 Общие принципы управления правами доступа

7.1.1 Основной задачей СУУЗиПД на данном уровне является формирование матрицы легальных прав доступа пользователей организации. Данная матрица содержит права доступа пользователей к ИР контролируемых ИС, которые были предоставлены в установленном порядке.

7.1.2 Матрица легальных прав доступа пользователей должна использоваться СУУЗиПД для предоставления прав доступа пользователям к ИР и обнаружения несанкционированных действий по изменению прав доступа пользователей в контролируемых ИС.

7.1.3 СУУЗиПД должна работать в сложной гетерогенной среде и контролировать ИС с различными моделями разграничения доступа (используемые модели разграничения доступа описываются в ГОСТ Р 59383). При этом СУУЗиПД должна предоставлять для пользователей, не являющихся администраторами ИС, единообразные способы управления правами доступа, вне зависимости от конкретного способа разграничения доступа в ИС.

7.1.4 Рекомендуется приводить все имеющееся многообразие моделей разграничения доступа контролируемых ИС к ролевой модели, как наиболее распространенной и удобной для пользователей СУУЗиПД.

7.1.5 Рекомендуется придерживаться следующих подходов для управления правами доступа в контролируемых ИС:

- для ИС с дискреционной моделью разграничения доступа — объединять устойчивые комбинации прав доступа к ИР в виде ролей СУУЗиПД. Пользователи СУУЗиПД должны использовать роли для формирования запросов на предоставление и прекращение доступа. СУУЗиПД должна формировать матрицу легальных прав доступа как сумму прав доступа к каждому ИР, полученную из ролей пользователя, и устанавливать в ИС списки управления правами доступа пользователей к ИР в соответствии с матрицей легальных прав доступа. В качестве непосредственного владельца ИР в контролируемой ИС выступает СУУЗиПД, в которой, в свою очередь, назначаются владельцы ИР и реализуются процессы управления правами доступа к данным ИР;
- для ИС с мандатной моделью разграничения доступа — создавать один ИР, соответствующий контролируемой ИС, с перечнем прав доступа, соответствующим перечню уровней безопасности для данной ИС (например, уровни безопасности «для служебного пользования», «конфиденциально», «строго конфиденциально»). Для каждой пары «ИР — право доступа» (и соответственно уровня безопасности) должна быть создана роль с наименованием, содержащим в себе наименование ИС и уровень безопасности. Пользователи в этом случае должны использовать соответствующие роли для формирования запросов на предоставление или прекращение доступа. СУУЗиПД должна формировать матрицу легальных прав доступа как сумму прав доступа пользователей к ИР (и соответствующих уровней безопасности для ИС) и формировать перечень уровней безопасности пользователя в соответствующей ИС;

- для ИС с разграничением доступа на основе идентификационных данных — использовать подход, аналогичный подходу для ИС с дискреционной моделью разграничения доступа;

- для ИС с ролевой моделью разграничения доступа — создавать в СУУЗиПД структуру ролей, аналогичную имеющейся в контролируемой ИС, и использовать для управления правами доступа пользователей данные роли;

- для ИС с атрибутной моделью разграничения доступа — формировать в контролируемой ИС политики доступа с правилами следующей структуры «(пользователь обладает ролью «Роль…») ЛОГИЧЕСКОЕ_И (уточняющее правило, устанавливающее соответствие атрибутов пользователя и ИР)». Для каждой политики управления правами доступа и соответствующей роли ИС должна быть создана роль СУУЗиПД, которая используется пользователями для предоставления и прекращения доступа. СУУЗиПД должна формировать матрицу легальных прав доступа пользователя как перечень ролей в СУУЗиПД и соответствующих ролей в ИС и назначать в ИС пользователям соответствующие роли. Тем самым атрибутная модель разграничения доступа для пользователей СУУЗиПД сводится к ролевой, а уточняющие правила настраиваются администраторами контролируемой ИС;

- для ИС с разграничением доступа на основе псевдонимов — использовать подход, аналогичный подходу для ИС с дискреционной моделью разграничения доступа. Поскольку в СУУЗиПД имеется единый каталог пользователей организации с информацией об УЗ пользователей в каждой контролируемой ИС, СУУЗиПД должна осуществлять трансляцию идентификатора пользователя в соответствующий псевдоним в контролируемой ИС.

7.1.6 В контролируемых ИС могут использоваться комбинированные модули разграничения доступа пользователей. Например, в контролируемой ИС могут использоваться одновременно ролевая и мандатная модели разграничения доступа. В этом случае СУУЗиПД должна поддерживать формирование множества ролей, соответствующих ролевой модели контролируемой ИС, и одновременно поддерживать множество ролей, соответствующих уровням безопасности данной ИС. При назначении пользователям ролей СУУЗиПД должна автоматически определять, объектам какой модели разграничения доступа в контролируемой ИС соответствует данная роль, и предоставлять УЗ пользователя необходимую роль либо устанавливать уровень безопасности для УЗ пользователя.

7.2 Управление ролевой моделью организации

7.2.1 Для упорядочивания процесса управления правами доступа пользователей в СУУЗиПД должно поддерживаться создание ролевой модели организации. Ролевая модель позволяет определить набор стандартных шаблонов прав доступа пользователей (ролей) и тем самым упростить пользователям предоставление необходимых прав доступа и принятие решений ответственными лицами при согласовании и пересмотре прав доступа. Правильно построенная ролевая модель позволяет скрыть от пользователей нюансы реализации модели разграничения доступа в каждой конкретной ИС и единообразно управлять правами доступа, несмотря на различия моделей разграничения доступа в разных ИС. Пример ролевой модели показан на рисунке 3.

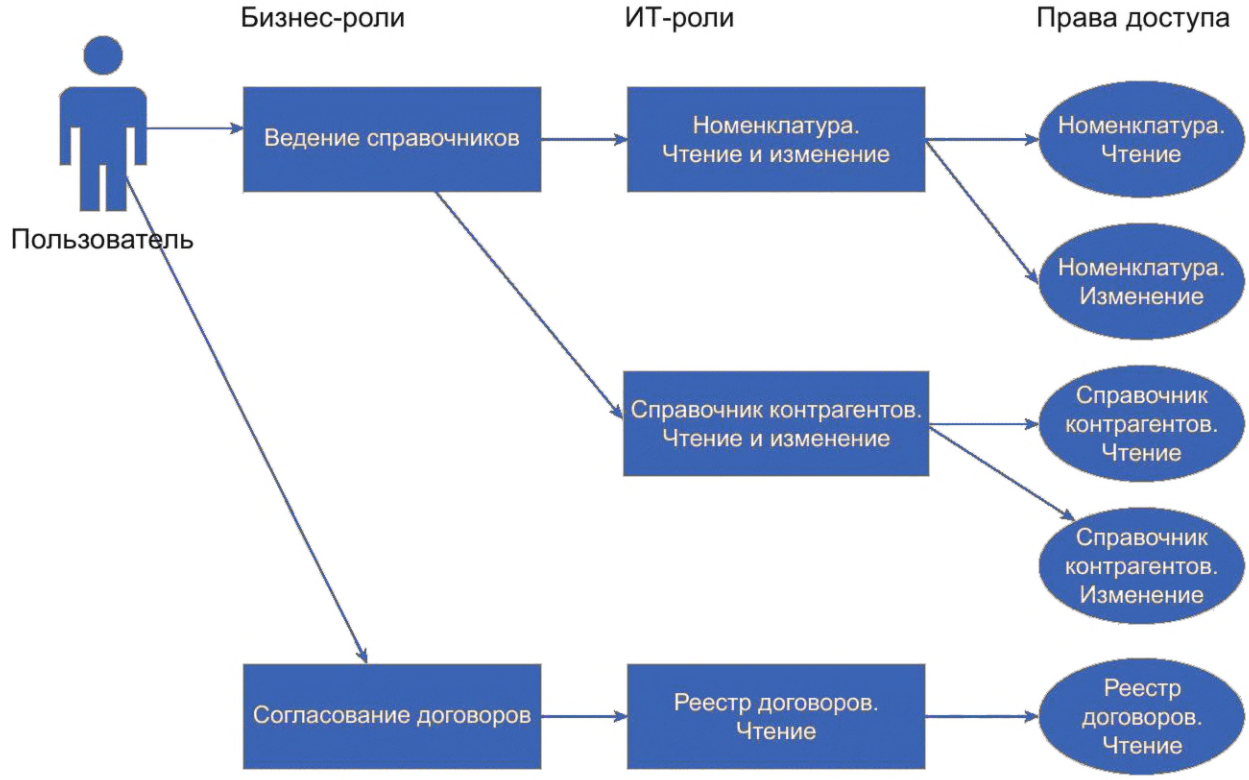

Рисунок 3 — Пример ролевой модели организации

7.2.2 При построении ролевой модели рекомендуется разделять все роли на два вида: ИТ-роли и бизнес-роли.

7.2.3 Роли, непосредственно предоставляющие пользователям права доступа к ИР (ИТ-роли), пользователям не предоставляются. Вместо этого ИТ-роли включаются в другие роли, не содержащие прав доступа непосредственно (бизнес-роли). Для формирования перечня ИТ-ролей рекомендуется использовать подходы, описанные в 7.5.

7.2.4 При формировании перечня бизнес-ролей рекомендуется создавать бизнес-роли для каждой задачи в рамках имеющихся в организации бизнес-процессов, а данные бизнес-роли объединять в высокоуровневые бизнес-роли, соответствующие участникам бизнес-процессов организации. Данный подход позволит создать ролевую модель, понятную для пользователей организации, упростит выбор необходимых ролей при запросах на предоставление и прекращение доступа пользователей, а также при определении правил назначения групповых прав доступа.

7.2.5 При формировании ролевой модели рекомендуется стремиться к тому, чтобы ИТ-роли представляли собой иерархию небольшой глубины, в идеале являясь плоским списком. Бизнес-роли могут образовывать иерархию любой глубины, в зависимости от сложности бизнес-процессов организации и глубины декомпозиции бизнес-процессов.

7.2.6 Отображение назначенных прав доступа на модель разграничения доступа конкретной ИС должно осуществляться в модуле интеграции, так называемом коннекторе. Подробнее коннекторы описаны в разделе 8.

7.2.7 Поскольку пользователи могут занимать несколько разных должностей в организационно-штатной структуре организации, СУУЗиПД должна поддерживать раздельное управление ролями для разных должностей пользователя. Для каждой из должностей, занимаемых пользователем, должна быть возможность назначить как индивидуальные, так и групповые права доступа.

7.2.8 Матрица легальных прав доступа пользователей должна строиться СУУЗиПД автоматически, как сумма всех прав доступа к ИР, предоставленных пользователям посредством назначенных им ролей для всех должностей, занимаемых пользователем. При определении прав доступа, предоставляемых ролью, должны учитываться права доступа ролей, включенных в назначенную роль на всю глубину вложенности.

7.2.9 Столбцам матрицы легальных прав доступа соответствуют пользователи, а строкам — права доступа к ИР. Ячейка, находящаяся на пересечении столбца, соответствующего пользователю, и строки, соответствующей праву доступа к ИР, показывает, имеется ли у пользователя соответствующее право доступа к ИР.

7.2.10 Матрица легальных прав доступа должна автоматически пересчитываться СУУЗиПД после любых изменений легальных прав доступа пользователей. Легальные права доступа пользователей могут изменяться в результате следующих действий в СУУЗиПД:

- предоставления или прекращения индивидуальных прав доступа пользователя;
- предоставления или прекращения групповых прав доступа пользователя;
- пересмотра прав доступа пользователей;
- изменения ролевой модели организации;
- процесса контроля соответствия легальных и фактических прав доступа.

7.2.11 Кроме матрицы легальных прав доступа СУУЗиПД должна построить матрицу фактических прав доступа. Данная матрица имеет такое же множество столбцов и строк, как и матрица легальных прав доступа, однако наполняется исходя не из прав доступа пользователя, назначенных в СУУЗиПД, а исходя из фактически предоставленных прав доступа в ИС для УЗ, привязанных к пользователю. Матрица фактических прав доступа должна обновляться СУУЗиПД автоматически за счет проведения периодической процедуры считывания прав доступа к ИР в контролируемых ИС либо по событиям изменения прав доступа в ИС, если API контролируемой ИС поддерживает функцию оповещения о таких изменениях.

7.2.12 СУУЗиПД должна использовать результаты сравнения матриц легальных и фактических прав доступа для определения прав доступа, которые должны быть предоставлены УЗ пользователя вследствие согласованных изменений доступа, и прав доступа, которые были предоставлены пользователю в контролируемой ИС в обход установленного процесса управления правами доступа с использованием СУУЗиПД. Порядок действий СУУЗиПД в случае обнаружения прав доступа, предоставленных в обход установленного процесса управления правами доступа, описан в 7.5.

7.3 Управление индивидуальными правами доступа пользователей

7.3.1 Процесс управления индивидуальными правами доступа пользователей в СУУЗиПД должен инициироваться в случае, если пользователю организации для исполнения им служебных обязанностей требуется предоставить новые права доступа либо потребность в соответствующих правах доступа отпадает.

7.3.2 Ответственное лицо (администратор СУУЗиПД, сам пользователь, руководитель или ответственный за ИБ организационной единицы) при помощи СУУЗиПД должно указать конкретного пользователя (с указанием занимаемой должности, если пользователь занимает несколько должностей) и необходимые роли либо запросить отзыв каких-либо имеющихся у пользователя ролей.

7.3.3 СУУЗиПД должна поддерживать предоставление временного доступа пользователям. В этом случае инициатор запроса доступа должен указать временной промежуток, в течение которого пользователю требуется доступ.

7.3.4 СУУЗиПД должна поддерживать продление временного доступа пользователей. Для запроса на продление временного доступа должен поддерживаться процесс согласования, аналогичный процессу запроса временного доступа.

7.3.5 Для согласования индивидуальных прав доступа рекомендуется в СУУЗиПД автоматически включать в список согласующих следующих ответственных лиц:

- руководитель/куратор пользователя — подтверждает наличие производственной необходимости при назначении прав доступа к ИР или отсутствие такой необходимости при прекращении доступа;
- ответственный за ИБ организационной единицы — подтверждает соответствие запрошенных прав доступа политике ИБ, регламентам и другим руководящим документам организации или данной конкретной организационной единицы;
- ответственный за ИБ контролируемой ИС, доступ к ИР которой был запрошен, — подтверждает соответствие запрошенных прав доступа политике ИБ, регламентам и другим руководящим документам, относящимся к данной ИС;
- ответственный за ИТ для контролируемой ИС, доступ к ИР которой был запрошен, — подтверждает техническую возможность предоставления прав доступа данному пользователю к указанным ИР;
- руководитель ИБ организации — согласует доступ к ИР, которые являются критическими.

7.3.6 В зависимости от типа запроса, критичности данного ИР и политики ИБ организации определенные шаги в процессе согласования могут быть пропущены или добавлены. В частности, рекомендуется использовать следующие правила пропуска шагов согласования:

- шаг согласования может быть пропущен, если согласующее данный шаг лицо является одновременно инициатором запроса либо уже согласовало данный запрос в рамках предыдущего шага согласования;

- шаг согласования ответственного за ИБ организационной единицы и контролируемой ИС может быть пропущен в случае запроса на отзыв прав доступа, а также при запросе предоставления прав доступа к ИР, не являющимся критическими;

- шаг согласования ответственным за ИТ для контролируемой ИС может быть пропущен в случае запроса отзыва прав доступа, а также при запросе предоставления прав доступа к ИР, в отношении которых заведомо не существует технических ограничений (например, на включение УЗ в группу в LDAP-каталоге).

7.3.7 После завершения процесса согласования СУУЗиПД должна проверить наличие у пользователя УЗ, необходимой для доступа к запрошенному ИР, и создать ее в случае необходимости.

7.3.8 Если для пользователя был запрошен временный доступ, дальнейшая обработка запроса СУУЗиПД должна быть отложена до начала временного промежутка, на который должен быть предоставлен доступ.

7.3.9 После проверки на наличие УЗ пользователя и создания ее в случае необходимости СУУЗиПД должна предоставить УЗ запрошенные права доступа. В зависимости от модели разграничения доступа контролируемой ИС УЗ должны быть предоставлены соответствующий мандат, права доступа к ИР, УЗ должна быть включена в группу либо ей должна быть предоставлена роль и т. д.

7.3.10 В случае, если для пользователя запрошен временный доступ, СУУЗиПД должна автоматически прекращать доступ пользователя в момент, указанный как окончание временного промежутка, на который должен быть предоставлен доступ.

7.3.11 В СУУЗиПД для запросов на временный доступ пользователя перед прекращением доступа пользователя к ИР рекомендуется оповещать инициатора и получателя временного доступа о приближении даты завершения временного доступа.

7.4 Управление групповыми правами доступа пользователей

7.4.1 Для удобства управления правами доступа в СУУЗиПД должна поддерживаться возможность определения перечня правил автоматического назначения прав доступа для группы пользователей, объединенных по какому-либо признаку. СУУЗиПД, как минимум, должна поддерживать в качестве такого признака нахождение пользователей внутри указанных организационных единиц или на какой-либо должности; могут использоваться и другие атрибуты или комбинации атрибутов пользователей, их должностей или организационных единиц, в которых они находятся.

7.4.2 Использование групповых прав доступа позволяет автоматизировать процесс назначения и прекращения прав доступа, которые являются типовыми для организационных единиц либо должностей.

7.4.3 Групповые права доступа рекомендуется согласовывать один раз при создании правила назначения. После согласования данные права доступа должны назначаться СУУЗиПД автоматически для любого пользователя, который оказывается в составе организационной единицы или на соответствующей должности либо по другим настраиваемым критериям.

7.4.4 В связи с отсутствием дополнительного согласования в процессе назначения групповых прав доступа рекомендуется не использовать данный механизм для предоставления доступа к критическим ИР.

7.4.5 В случае необходимости изменения групповых прав доступа ответственное лицо (администратор СУУЗиПД, руководитель или ответственный за ИБ организационной единицы) должно иметь возможность при помощи СУУЗиПД запросить предоставление или отзыв определенных ролей для организационной единицы или должности либо указать иные критерии назначения или отзыва группового доступа пользователей.

7.4.6 Для согласования групповых прав доступа рекомендуется в СУУЗиПД автоматически включать в список согласующих следующих ответственных лиц:

- руководителя организационной единицы, для которой запрашивается или прекращается доступ, подтверждающего наличие производственной необходимости для предоставления доступа к ИР или отсутствие такой необходимости при прекращении доступа;

- ответственного за ИБ организационной единицы, подтверждающего при предоставлении доступа соответствие запрошенных прав доступа политике ИБ, регламентам и другим руководящим документам организации или данной конкретной организационной единицы;

- ответственного за ИБ контролируемой ИС, доступ к ИР которой был запрошен, подтверждающего соответствие запрошенных прав доступа политике ИБ, регламентам и другим руководящим документам, относящимся к данной ИС;

- ответственного за ИТ для контролируемой ИС, доступ к ИР которой был запрошен, подтверждающего техническую возможность предоставления доступа пользователям из данной организационной единицы к указанным ИР.

7.4.7 Вследствие того, что настоящим стандартом не рекомендуется использовать групповые права доступа для назначения доступа к критическим ИР, участие руководителя ИБ в этом случае не требуется.

7.4.8 После завершения процесса согласования СУУЗиПД должна автоматически инициировать процесс назначения или прекращения соответствующего доступа для всех пользователей, подпадающих под действие данного правила. Данный процесс выполняется аналогично описанному выше процессу «Управление индивидуальными правами доступа пользователей», но этап согласования пропускается.

7.5 Пересмотр прав доступа пользователей

7.5.1 Права доступа пользователей к ИР регулярно меняются, в результате чего у пользователей постепенно накапливаются избыточные права доступа, что приводит к снижению уровня ИБ организации. С целью своевременного прекращения доступа пользователей к ИР, доступ к которым более не требуется для выполнения пользователями своих должностных обязанностей, в организации должны быть реализованы процессы регулярного пересмотра прав доступа пользователей к ИР.

7.5.2 Пересмотр прав доступа пользователей в СУУЗиПД должен инициироваться в следующих случаях:

- автоматически при переводе пользователя с одной должности на другую или из одной организационной единицы в другую;

- автоматически по настроенному расписанию должен инициироваться процесс пересмотра прав доступа для организации в целом или для отдельных организационных единиц;

- вручную ответственными лицами должен инициироваться пересмотр прав доступа в случае существенных изменений ИТ-инфраструктуры или организационно-штатной структуры.

7.5.3 Перевод пользователя с одной должности на другую

7.5.3.1 Процесс перевода пользователя с одной должности на другую должен инициироваться СУУЗиПД автоматически как часть процесса автоматического перевода пользователя по итогам изменений его места работы в источнике кадровой информации либо перемещения пользователя внутри организационно-штатной структуры вручную.

7.5.3.2 Роли переводимого пользователя должны подвергаться пересмотру. Для этого СУУЗиПД должна направлять ответственным лицам запрос о подтверждении имеющихся у пользователя ролей. Рекомендуется включать в процесс подтверждения следующих ответственных лиц:

- новый руководитель пользователя — подтверждает наличие или отсутствие производственной необходимости для существующих у пользователя прав доступа;

- ответственный за ИБ контролируемой ИС — подтверждает соответствие имеющихся у пользователя прав доступа политике ИБ, регламентам и другим руководящим документам;

- руководитель ИБ организации — подтверждает права доступа к критическим ИР.

7.5.3.3 Рекомендуется подвергать пересмотру групповые права доступа, полученные пользователем на текущей должности и отсутствующие на новой. Пересмотру могут подвергаться все права доступа, в том числе индивидуальные, или только права доступа к критическим ИР. Перечень прав доступа, подвергаемых пересмотру, должен настраиваться в СУУЗиПД исходя из политики ИБ и регламента управления доступом в организации.

7.5.3.4 Все права доступа пользователя, подтвержденные ответственными лицами, должны оставаться у пользователя, а для неподтвержденных прав доступа пользователя в СУУЗиПД должно инициироваться прекращение соответствующих прав.

7.5.4 Регулярный процесс пересмотра прав доступа

7.5.4.1 Целью данного процесса является регулярная ревизия прав доступа с целью устранения избыточных прав доступа, более не требующихся для выполнения должностных обязанностей пользователями.

7.5.4.2 Данный процесс должен инициироваться СУУЗиПД автоматически в соответствии с настроенным расписанием для организации или отдельных организационных единиц.

7.5.4.3 Для каждой организационной единицы, для которой инициируется процесс пересмотра прав доступа, должны создаваться задачи на пересмотр прав доступа всех пользователей, находящихся в данной организационной единице.

7.5.4.4 При пересмотре прав доступа в согласовании участвуют следующие ответственные лица:

- руководитель организационной единицы — подтверждает наличие или отсутствие производственной необходимости для существующих у пользователей прав доступа;
- ответственный за ИБ организационной единицы — подтверждает соответствие имеющихся у пользователя прав доступа политике ИБ, регламентам и другим руководящим документам;
- руководитель ИБ организации — подтверждает права доступа к критическим ИР.

7.5.4.5 В зависимости от настроек в СУУЗиПД пересмотру должны подвергаться либо все права доступа пользователей, либо только права доступа к критическим ИР, либо права доступа по каким-либо иным критериям.

7.5.4.6 Все права доступа пользователей, подтвержденные ответственными лицами, должны оставаться у пользователей, а для неподтвержденных прав доступа пользователя в СУУЗиПД должно инициироваться прекращение соответствующих прав доступа.

7.5.4.7 Результаты пересмотра прав доступа должны фиксироваться СУУЗиПД в специальном журнале с возможностью проведения анализа результатов пересмотра в дальнейшем.

7.5.4.8 В данном журнале должна фиксироваться следующая информация:

- перечень пользователей, для которых был инициирован процесс пересмотра прав доступа;
- перечень ИР с правами доступа, в отношении которых был проведен пересмотр прав доступа для каждого пользователя;
- сроки проведения пересмотра прав доступа для каждого пользователя и ИР;
- ответственные лица, включенные в список подтверждающих права доступа для каждого пользователя и ИР, а также принятые ими решения (подтверждено/не подтверждено).

7.5.5 Процесс пересмотра прав доступа при изменении контролируемой информационной системы и организационно-штатной структуры

7.5.5.1 В случае массовых изменений организационно-штатной структуры организации или существенных изменений контролируемой ИС ответственное лицо (администратор СУУЗиПД, ответственный за ИБ организационной единицы или контролируемой ИС) должно иметь возможность вручную запустить процесс пересмотра прав доступа.

7.5.5.2 Ответственность за определение случаев, в которых должен осуществляться пересмотр прав доступа, возлагается на соответствующее ответственное лицо, которое при принятии решения руководствуется положениями регламента управления доступом организации и политикой ИБ организации.

7.5.5.3 СУУЗиПД должна предоставлять возможность выбрать пересмотр прав доступа для выбранного перечня организационных единиц либо для всех пользователей, имеющих доступ к выбранным контролируемым ИС или конкретным ИР.

7.5.5.4 После ручной инициации процесс пересмотра доступа аналогичен описанному в 7.5.2.

7.6 Процесс изменения ролевой модели организации

7.6.1 Процесс изменения ролевой модели организации инициируется лицом (или группой лиц), отвечающим за ИБ определенной организационной единицы или организации в целом, либо лицом, отвечающим за ИБ определенной контролируемой ИС.

7.6.2 Инициатор изменения ролевой модели исходя из появившихся потребностей должен иметь возможность произвести изменения существующей ролевой модели в СУУЗиПД. Данные изменения должны формироваться в рамках отдельной транзакции и до завершения процесса изменения и со-

гласования ролевой модели не должны оказывать влияние на текущие процессы управления доступом в СУУЗиПД.

7.6.3 После внесения в систему всех изменений ролевой модели данный пакет изменений в СУУЗиПД должен направляться на согласование другим ответственным лицам. Рекомендуется включать в перечень согласующих следующих ответственных лиц:

- руководителей организационных единиц, пользователей в которых затронет изменение ролевой модели, проверяющих отсутствие изменений прав доступа, препятствующих выполнению их подчиненными должностных обязанностей;
- ответственных за ИБ организационных единиц, пользователей в которых затронет изменение ролевой модели, проверяющих соответствие новой ролевой модели политике ИБ и регламентам;
- ответственных за ИБ контролируемых ИС, доступ к ИР которых затронет изменение ролевой модели, проверяющих соответствие новой ролевой модели политике ИБ и регламентам;
- ответственных за ИТ контролируемой ИС, доступ к ИР которых затронет изменение ролевой модели, проверяющих техническую возможность предоставления доступа к ИР в рамках новой ролевой модели.

7.6.4 При согласовании изменений ролевой модели СУУЗиПД должна показывать для каждого согласующего, какие именно изменения ролевой модели он должен согласовать и каким образом изменения повлияют на доступ пользователей.

7.6.5 После завершения процесса согласования СУУЗиПД должна произвести изменения существующей ролевой модели, произвести корректировку прав доступа пользователей в соответствии с процессами, описанными в 7.3 и 7.4. В этом случае этап согласования изменений прав доступа пропускается.

7.7 Контроль соответствия легальных и фактических прав доступа

7.7.1 Для решения задачи своевременного выявления и устранения несанкционированных прав доступа в СУУЗиПД на регулярной основе должна осуществляться сверка фактических и легальных прав доступа пользователей к ИР в контролируемых ИС.

7.7.2 При сверке СУУЗиПД должна проверять соответствие фактических и легальных прав доступа, при этом фактические права доступа определяются в процессе регулярного чтения прав доступа к ИР в контролируемых ИС (подробное описание процесса контроля прав доступа представлено в разделе 9), а легальные права доступа определяются текущим состоянием матрицы легальных прав доступа.

7.7.3 Также при сверке должно проверяться отсутствие лишних УЗ, созданных в обход СУУЗиПД.

7.7.4 Любое вновь обнаруженное расхождение фактических и легальных прав доступа и лишние УЗ должны автоматически фиксироваться СУУЗиПД в журнале несанкционированных прав доступа, после чего должен запускаться автоматизированный процесс реагирования на расхождение.

7.7.5 В записи о расхождении должна фиксироваться следующая информация:

- ИР и права доступа, в отношении которых имеется расхождение, а также ИС, в составе которой находится этот ИР;
- УЗ, в отношении которой имеется расхождение прав доступа, а также информация о пользователе в едином каталоге пользователей, к которому привязана данная УЗ, если УЗ привязана к пользователю;
- дата обнаружения расхождения, а также дата изменений в контролируемой ИС;
- дата возникновения и субъект доступа (учетная запись), внесший изменения в ИС, приведшие к возникновению расхождения (если в контролируемой ИС имеется техническая возможность мониторинга изменений с определением их инициатора).

7.7.6 В зависимости от настроек СУУЗиПД может сразу после обнаружения расхождения автоматически внести изменения в права доступа пользователя в контролируемой ИС с целью устранения несанкционированных прав доступа к ИР, а также заблокировать УЗ.

7.7.7 Для каждого расхождения СУУЗиПД должна автоматически назначать ответственного за расследование расхождения согласно настроенным правилам. Рекомендуется назначать ответственным за расследование одного из следующих ответственных лиц:

- администратора ИБ, ответственного за соответствующую контролируемую ИС или за конкретный ИР;

- администратора ИБ, ответственного за организационную единицу пользователя, которому были предоставлены права доступа;

- конкретного сотрудника службы ИБ, ответственного за проведение расследований расхождений прав доступа;

- иное ответственное лицо.

7.7.8 После назначения ответственного лица СУУЗиПД должна оповестить его о появлении расхождения.

7.7.9 Ответственное лицо должно иметь возможность при помощи СУУЗиПД проанализировать информацию о расхождении.

7.7.10 По результатам анализа ответственное лицо при помощи СУУЗиПД должно иметь возможность произвести одно из следующих действий:

- устранить расхождение прав доступа в контролируемой ИС, приведя фактические права доступа пользователя в соответствие с легальными правами доступа, или удалить новую УЗ;

- легализовать расхождение прав доступа, предоставив пользователю недостающие права доступа, или связать новую УЗ с пользователем;

- оставить расхождение в активном состоянии на время (если политика ИБ и регламенты разрешают для контролируемой ИС или данного ИР наличие активных расхождений);

- делегировать принятие решения по расхождению другому ответственному лицу.

7.7.11 В любом случае ответственное лицо должно указать для расхождения результаты расследования с обоснованием принятого решения, которые должны быть сохранены в журнале с возможностью анализа результатов расследования позднее.

8 Общие требования к управлению учетными записями и правами доступа в контролируемых информационных системах

8.1 В каждой организации имеется свой уникальный набор контролируемых ИС. Чтобы избежать необходимости модифицировать СУУЗиПД для каждой новой организации, СУУЗиПД должна поддерживать возможность выделения функционала интеграции с контролируемой ИС в отдельные отчуждаемые программные модули (коннекторы), взаимодействующие с СУУЗиПД через стандартизованный программный интерфейс.

8.2 Программный интерфейс коннекторов должен обеспечивать (как минимум) следующие функции:

- инициализацию параметров подключения к конкретной контролируемой ИС. В организации может иметься несколько однотипных ИС, интеграция с которыми осуществляется при помощи одного и того же коннектора. Соответственно, в СУУЗиПД будет создано несколько экземпляров однотипных коннекторов с различными параметрами подключения к разным контролируемым ИС;

- загрузку перечня контролируемых объектов ИС, таких как УЗ, ИР, и прав доступа УЗ к ИР. Может выполняться загрузка дополнительных контролируемых объектов, необходимых для управления в рамках модели разграничения доступа данной контролируемой ИС;

- создание новой УЗ. Перечень атрибутов УЗ формируется СУУЗиПД на основании правил прямой синхронизации, описанных выше;

- изменение УЗ и прочих контролируемых объектов. Перечень атрибутов УЗ и прочих контролируемых объектов формируется СУУЗиПД на основании правил прямой синхронизации;

- изменение пароля УЗ. Перед выполнением операции изменения пароля УЗ в СУУЗиПД должна осуществляться проверка пароля на соответствие парольной политике;

- удаление контролируемого объекта ИС. В зависимости от конкретной модели разграничения доступа в контролируемой ИС данная операция может приводить как к физическому удалению объекта, так и к пометке его как удаленного.

8.3 Описание данного программного интерфейса должно быть приведено в технической документации на СУУЗиПД.

8.4 При разработке коннектора должна учитываться возможность разрыва соединения с контролируемой ИС. В этом случае коннектор должен самостоятельно восстанавливать соединение при следующем обращении к контролируемой ИС.

8.5 Необходимо учитывать возможность возникновения ошибки при обращении к контролируемой ИС. Такая ошибка должна корректно обнаруживаться, обрабатываться, после чего в СУУЗиПД должна передаваться вся информация, необходимая для диагностики ошибки.

8.6 Поскольку не все контролируемые ИС поддерживают программные интерфейсы, допускающие модификацию объектов модели разграничения прав доступа, и не всегда целесообразна реализация коннектора, реализующего полную автоматизацию управления контролируемой ИС, допускаются различные способы интеграции СУУЗиПД, реализуемые коннектором и контролируемой ИС.

8.7 Чтение данных об учетных записях и правах доступа должно осуществляться одним из следующих способов:

- с подключением к контролируемой ИС непосредственно через стандартный API, базу данных контролируемой ИС, файловую систему, на которой развернута контролируемая ИС, с автоматическим считыванием необходимой информации на регулярной основе или по событиям;
- без непосредственного подключения к контролируемой ИС. В этом случае выгрузка данных из контролируемой ИС осуществляется вручную при помощи функций экспорта данных и конфигурации либо при помощи отчетов. Выгрузка данных должна осуществляться на периодической основе администратором контролируемой ИС, после чего эти данные должны вручную загружаться в СУУЗиПД. Частота выгрузки определяется для каждой ИС отдельно, с учетом требований политики ИБ, наличия в данной контролируемой ИС критических ИР и частоты изменений контролируемых объектов ИС.

8.8 Создание, изменение или удаление объектов управления в ИС должно осуществляться одним из следующих способов:

- с подключением коннектора к контролируемой ИС при помощи API, прямого изменения контролируемых объектов ИС в базе данных, изменения файлов конфигурации контролируемой ИС либо иными способами с целью автоматической модификации объектов контролируемой ИС;
- без автоматического изменения контролируемых объектов ИС коннектором. В этом случае СУУЗиПД должна формировать набор поручений на изменение управляемых объектов для администраторов контролируемых ИС.

9 Уровни контроля за учетными записями и правами доступа в информационных системах

9.1 В зависимости от используемого метода интеграции СУУЗиПД и контролируемой ИС выделяют три возможных уровня контроля контролируемой ИС:

- без автоматизированной сверки. При данном уровне контроля СУУЗиПД не подключается к управляемой ИС и возможность периодической сверки контролируемых объектов ИС и их модификации отсутствует. Сверка контролируемых объектов ИС осуществляется при выгрузке данных из контролируемой ИС и загрузке их в СУУЗиПД вручную администратором ИС, а модификация объектов управления осуществляется вручную при помощи поручений администратору ИС;
- с автоматической сверкой. При данном уровне контроля СУУЗиПД должна подключаться к управляемой ИС для выполнения периодической сверки контролируемых объектов ИС, но при этом не осуществляет автоматическую модификацию контролируемых объектов ИС. Модификацию контролируемых объектов ИС должны осуществлять администраторы контролируемой ИС вручную, однако СУУЗиПД в процессе автоматической сверки должна отслеживать изменения контролируемых объектов ИС и контролировать корректность действий администраторов ИС;
- с автоматизированным управлением и сверкой. При данном уровне контроля СУУЗиПД должна подключаться к контролируемой ИС для выполнения периодической сверки контролируемых объектов ИС, а также автоматически осуществлять их модификацию. В этом случае достигается максимальный уровень контроля за корректностью предоставленных прав доступа к ИР и за действиями администраторов ИС.

9.2 Конкретный способ подключения должен определяться в зависимости от критичности ИР контролируемой ИС, количества контролируемых объектов ИС и частоты их изменения, наличия технической возможности для выгрузки данных и модификации контролируемых объектов ИС.

10 Меры защиты информации в системе управления учетными записями и правами доступа

10.1 Общие положения

10.1.1 Поскольку СУУЗиПД предназначена для хранения и обработки данных пользователей, полученных из кадровых и иных источников, и учитывая, что в СУУЗиПД хранятся ФИО пользователей и их контакты, СУУЗиПД является ИС, осуществляющей обработку персональных данных, и требует применения соответствующих мер защиты.

10.1.2 При использовании СУУЗиПД в качестве подсистемы управления УЗ и правами доступа пользователей для организации она выступает как средство защиты информации для ИС организации. Это означает, что СУУЗиПД должна обеспечивать необходимые меры защиты, связанные с управлением УЗ и правами доступа пользователей.

10.1.3 Перечень реализуемых в СУУЗиПД мер защиты зависит от требуемого уровня защищенности СУУЗиПД и ИС, в составе которых эксплуатируется СУУЗиПД. Требуемый уровень защищенности зависит от численности пользователей и состава данных, хранящихся в СУУЗиПД и защищаемой ИС. Соответствующая классификация должна осуществляться на этапе проектирования конкретного решения.

10.1.4 В СУУЗиПД не обязательно реализовывать все меры защиты, указанные ниже, часть мер защиты рекомендуется реализовывать на уровне операционной системы, других ИС или дополнительных средств защиты информации. Ниже приводится перечень мер защиты, которые должны быть обязательно реализованы в самой СУУЗиПД, а также перечень мер защиты, реализация которых в СУУЗиПД рекомендуется.

10.2 Идентификация и аутентификация субъектов доступа и объектов доступа

10.2.1 При доступе в СУУЗиПД должны осуществляться идентификация и аутентификация пользователей. СУУЗиПД должна использовать собственные механизмы аутентификации либо внешние средства аутентификации, такие как LDAP-аутентификация, OpenID-аутентификация, либо иные.

10.2.2 Рекомендуется поддерживать для аутентификации в СУУЗиПД многофакторную (двухфакторную) аутентификацию, как минимум для пользователей, имеющих следующие права в СУУЗиПД:

- права администратора СУУЗиПД;
- права конфигурирования СУУЗиПД;
- права на выполнение операций по работе с расхождениями легальных и фактических прав доступа в контролируемых ИС.

10.2.3 Управление идентификаторами пользователей в СУУЗиПД описано в 6.3.

10.2.4 Управление средствами аутентификации в части управления паролями пользователей описано в 6.4.

10.2.5 В случае использования в СУУЗиПД аутентификации пользователей на основе паролей вводимые пользователем символы пароля должны заменяться условными знаками.

10.3 Управление правами доступа субъектов доступа к объектам доступа

10.3.1 Управление УЗ пользователей описано в разделе 6.

10.3.2 В СУУЗиПД должно быть реализовано разграничение доступа пользователей как к выполняемым операциям, так и к данным, к которым применяются соответствующие операции. При этом доступ должен разграничиваться к любым операциям, выполняемым пользователями в СУУЗиПД.

10.3.3 В качестве модели разграничения доступа к операциям рекомендуется использовать ролевую модель, аналогичную используемой для управления правами доступа к контролируемой ИС.

10.3.4 В качестве модели разграничения доступа к данным рекомендуется использовать ролевую либо комбинированную (ролевую и атрибутную) модель.

10.3.5 В СУУЗиПД должен быть сформирован перечень ролей, соответствующий задачам, выполняемым пользователями с использованием СУУЗиПД. В зависимости от модели разграничения доступа в СУУЗиПД в роли должны быть добавлены следующие права доступа:

- в случае использования только ролевой модели в роли должны добавляться права на выполнение операций и права доступа к конкретным объектам в СУУЗиПД;

- в случае использования комбинированной (ролевой и атрибутной) модели в роли должны добавляться права на выполнение операций и политики, определяющие правила доступа к объектам в СУУЗиПД на основании их атрибутов.

10.3.6 Поскольку в СУУЗиПД в едином каталоге пользователей хранятся персональные данные пользователей, должна иметься возможность ограничивать доступ к данным не только на уровне объектов, но и на уровне атрибутов объектов. Данное требование является обязательным в отношении разграничения доступа к атрибутам объектов единого каталога и атрибутам УЗ контролируемых ИС, загруженным в СУУЗиПД. Для прочих объектов, используемых в СУУЗиПД, разграничение доступа к атрибутам является рекомендуемым.

10.3.7 При настройке ролевой модели и назначении ролей в СУУЗиПД пользователям должны предоставляться минимально необходимые права доступа к операциям и данным, необходимые для выполнения пользователями задач в соответствии с регламентом управления доступом.

10.3.8 СУУЗиПД должна поддерживать ограничение количества неуспешных попыток входа пользователей с блокировкой (временной или постоянной) пользователя, превысившего количество неуспешных попыток. Количество неуспешных попыток ввода и срок блокировки должны настраиваться.

10.3.9 Должно поддерживаться блокирование сеанса доступа к СУУЗиПД после установленного времени бездействия пользователя или по его запросу. Повторный доступ к СУУЗиПД должен осуществляться только после прохождения процедуры идентификации и аутентификации.

10.3.10 СУУЗиПД не должна разрешать пользователям выполнять какие-либо действия до завершения выполнения процедуры идентификации и аутентификации. В случае использования для доступа в СУУЗиПД протокола HTTPS должно блокироваться обращение неавторизованного пользователя к любым URL, которые могут быть использованы для доступа пользователя к СУУЗиПД.

10.4 Регистрация событий безопасности

10.4.1 СУУЗиПД должна поддерживать регистрацию событий безопасности во внутренних журналах или передачу событий во внешние хранилища по защищенному протоколу передачи данных.

10.4.2 Как минимум, должна иметься возможность регистрации следующих событий безопасности:

- успешной и неуспешной попыток входа пользователя в СУУЗиПД;
- выхода пользователя из СУУЗиПД;
- любых изменений конфигурации СУУЗиПД;
- создания, изменения, удаления объектов единого каталога пользователей;
- изменения паролей пользователей в СУУЗиПД;
- создания, изменения, удаления подключения СУУЗиПД к контролируемой ИС;
- создания, изменения, удаления контролируемого объекта ИС в СУУЗиПД;
- изменения пароля УЗ в контролируемой ИС;
- привязки УЗ к пользователю в едином каталоге пользователей в СУУЗиПД;
- предоставления или прекращения прав доступа УЗ к ИР;
- создания, изменения, удаления ролей в СУУЗиПД;
- предоставления или прекращения прав доступа роли к ИР;
- создания запроса на изменение индивидуальных и групповых прав доступа в СУУЗиПД;
- назначения согласующих для запроса на изменение индивидуальных и групповых прав доступа в СУУЗиПД;
- успешного или неуспешного согласования запроса на управление индивидуальными и групповыми правами доступа в СУУЗиПД.

10.4.3 СУУЗиПД должна предоставлять возможность определения перечня событий безопасности, подлежащих регистрации, и сроков их хранения.

10.4.4 СУУЗиПД должна предоставлять возможность определять состав и содержание информации о событиях безопасности, подлежащих регистрации. Для каждого типа событий должна иметься возможность указать перечень данных событий безопасности, которые должны сохраняться.

10.4.5 СУУЗиПД должна реагировать на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора и передачи информации, и достижение предела или переполнения объема (емкости) памяти. В случае возникновения сбоя СУУЗиПД должна оповещать администратора по настроенным каналам связи.

10.4.6 СУУЗиПД или внешняя система хранения журнала событий безопасности должна поддерживать мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

10.4.7 В СУУЗиПД должно обеспечиваться корректное генерирование временных меток для событий безопасности. Синхронизация системного времени должна обеспечиваться СУУЗиПД или внешними средствами.

10.4.8 СУУЗиПД или внешняя система хранения журнала событий безопасности должна обеспечивать защиту информации о событиях безопасности. Модификация или очистка журнала событий безопасности до истечения настроенного времени хранения должны быть исключена.

10.5 Контроль (анализ) защищенности информации

10.5.1 СУУЗиПД должна обеспечивать контроль правил генерации и смены паролей пользователей в СУУЗиПД и контролируемых ИС (описаны в 6.4), создания и удаления УЗ пользователей в контролируемых ИС (описаны в 6.3), реализации правил разграничения доступа, полномочий пользователей в СУУЗиПД (описаны в 10.3).

10.6 Обеспечение доступности информации

10.6.1 В СУУЗиПД должны использоваться отказоустойчивые технические средства, должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования.

10.6.2 В СУУЗиПД должны быть реализованы функции для осуществления контроля безотказного функционирования технических средств, возможности обнаружения и локализации отказов функционирования, средства оповещения администратора СУУЗиПД о сбоях.

10.6.3 В СУУЗиПД должны быть реализованы собственные средства для осуществления периодического резервного копирования информации на резервные машинные носители информации либо должна быть описана процедура выполнения резервного копирования с использованием внешних средств. Должны быть описаны места хранения данных СУУЗиПД (БД, конфигурационные файлы и т. д.) и порядок их резервного копирования, обеспечивающий сохранение целостности копируемой информации.

10.6.4 В СУУЗиПД должны иметься собственные средства для осуществления восстановления информации с резервных машинных носителей информации либо должна быть описана процедура восстановления информации с использованием внешних средств.

10.6.5 СУУЗиПД должна поддерживать информирование администраторов и пользователей СУУЗиПД о наличии поручений в СУУЗиПД и возникновении событий, требующих их внимания, по различным каналам доставки информации пользователям.

10.6.6 Администратор СУУЗиПД должен иметь возможность настроить способы доставки информации до пользователей.

10.6.7 Рекомендуется поддерживать в СУУЗиПД хотя бы один из следующих способов доставки информации:

- по электронной почте;
- по SMS;
- через мессенджеры;
- при помощи формирования запроса в системе управления ИТ-услугами.

10.6.8 В качестве адресов пользователей должны использоваться контакты пользователей, хранящиеся в едином каталоге пользователей СУУЗиПД.

10.6.9 Рекомендуется поддерживать в СУУЗиПД доставку информации пользователям по различным каналам связи с указанием приоритетов. В этом случае, если попытка доставить информацию по одному каналу завершается с ошибкой, СУУЗиПД должна последовательно пытаться доставить информацию другими способами в порядке указанных приоритетов.

10.7 Защита информационной системы, ее средств, систем связи и передачи данных

10.7.1 В СУУЗиПД должно обеспечиваться разделение функций по администрированию СУУЗиПД и функций по управлению учетными записями и правами доступа пользователей. Методы разграничения доступа пользователей описаны в 10.3.

10.7.2 В СУУЗиПД должна обеспечиваться защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи. Для всех каналов связи между компонентами СУУЗиПД, выходящих за пределы контролируемой зоны, должны использоваться протоколы, защищенные от прослушивания и подмены передаваемой информации (например, протокол HTTPS).

10.7.3 СУУЗиПД должна обеспечивать, как минимум, защиту следующих каналов связи:

- с коннекторами в случае, если канал связи с ними проходит за пределами контролируемой зоны;
- с контролируемыми ИС и источниками кадровых данных;
- пользовательского интерфейса СУУЗиПД с пользователями;
- каналов связи, используемых для передачи сообщений администраторам и пользователям СУУЗиПД при помощи электронной почты, SMS, мессенджеров;
- каналов связи с внешними системами, такими как системы управления ИТ-услугами, системы управления информацией и событиями безопасности и т. п.

10.7.4 В СУУЗиПД должно обеспечиваться подтверждение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов СУУЗиПД, контролируемых и внешних ИС. Подтверждение подлинности должно обеспечиваться для всех соединений, описанных в 10.7.3.

10.7.5 В СУУЗиПД должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании. СУУЗиПД должна обеспечивать эту защиту собственными средствами либо поддерживать интеграцию с внешними средствами, обеспечивающими защиту от атак, направленных на отказ в обслуживании.

10.8 Выявление инцидентов и реагирование на них

10.8.1 СУУЗиПД должна обеспечивать следующие возможности по выявлению инцидентов (расхождений легальных и фактических прав доступа) и реагирования на них (требования к данным функциям СУУЗиПД описаны в 7.7):

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение, идентификацию и регистрацию инцидентов;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;
- предоставление необходимой информации для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий;
- принятие мер по устранению последствий инцидентов.

Приложение А
(справочное)

Основные процессы управления учетными записями и правами доступа пользователей

В данном приложении приведены основные процессы в СУУЗиПД, связанные с управлением УЗ и правами пользователей. Описанные схемы процессов являются типовыми и могут быть изменены в соответствии с руководящими документами конкретной организации.

А.1 Процесс создания нового пользователя

Процесс создания нового пользователя инициируется автоматически при обнаружении в кадровом источнике информации о новом сотруднике или вручную руководителем нового сотрудника либо куратором для внештатного пользователя.

В случае инициации процесса вручную для штатного пользователя информация позднее подтверждается появлением в кадровом источнике информации о новом сотруднике. Сопоставление пользователя, созданного вручную, и данных, полученных из кадровой системы, осуществляется по настроенным в СУУЗиПД правилам сопоставления (подробнее см. 6.2.7).

Ведение перечня внештатных пользователей возлагается на ответственное лицо — куратора.

Результатом процесса являются запись в едином каталоге пользователей и предоставление новому пользователю УЗ и прав доступа согласно регламенту организации.

Схема процесса приема на работу показана на рисунке А.1.

А.2 Процесс перевода на другую должность

Процесс перевода на другую должность инициируется автоматически при обнаружении в кадровом источнике информации о переводе сотруднике на другую должность либо вручную для внештатного пользователя.

Результатом процесса являются изменение информации об организационной единице и должности пользователя в едином каталоге пользователей, предоставление пользователю прав доступа для новой должности и пересмотр существующих прав доступа согласно регламенту организации.

Схема процесса перевода на новую должность показана на рисунке А.2.

А.3 Процесс изменения статуса пользователя

Процесс изменения статуса пользователя инициируется автоматически при обнаружении в кадровом источнике информации об изменении статуса пользователя либо вручную руководителем (временная разблокировка) или сотрудником ИБ (временная блокировка).

В зависимости от нового статуса пользователя результатом процесса являются:

- блокирование или разблокирование пользователя согласно регламенту организации;
- увольнение пользователя с последующим прекращением доступа и блокированием или удалением всех его УЗ в контролируемых ИС.

Схема процесса изменения статуса пользователя показана на рисунке А.3.

А.4 Процесс изменения индивидуального доступа пользователя

Процесс изменения индивидуального доступа пользователя инициируется заинтересованным лицом (самим пользователем или его руководителем) в случае возникновения необходимости в изменении доступа пользователя в соответствии с его должностными обязанностями.

Как правило, изменение доступа пользователя требует согласования ответственными лицами. Порядок согласования зависит от регламента организации и настраивается на этапе развертывания СУУЗиПД.

Результатом процесса, в случае положительного решения при согласовании, является изменение прав доступа пользователя в контролируемых ИС. Изменение прав доступа может потребовать создания новых УЗ пользователя.

Схема процесса изменения прав доступа пользователя показана на рисунке А.4.

А.5 Процесс изменения групповых прав доступа пользователей

Процесс изменения групповых прав доступа инициируется заинтересованным лицом (руководителем организационной единицы или иным ответственным лицом) в случае возникновения необходимости в изменении прав доступа пользователей, работающих в соответствующей организационной единице или на соответствующей должности либо сгруппированных по иным критериям в соответствии с их должностными обязанностями.

Как правило, изменение групповых прав доступа требует согласования ответственными лицами. Порядок согласования зависит от регламента организации и настраивается на этапе развертывания СУУЗиПД.

Результатом процесса в случае положительного решения при согласовании является изменение прав доступа для всех пользователей в соответствующей организационной единице или на должности либо сгруппированных по иному критерию в контролируемых ИС. Также данные изменения коснутся и новых пользователей, которые будут приняты в соответствующую организационную единицу или на соответствующую должность либо подпадут

под указанные критерии. Такие изменения прав доступа пользователей, как правило, не требуют дополнительного согласования.

Схема процесса изменения групповых прав доступа пользователей показана на рисунке А.5.

А.6 Процесс пересмотра прав доступа пользователей

Процесс пересмотра прав доступа пользователей инициируется в следующих случаях:

- автоматически при переводе пользователя с одной должности на другую или из одной организационной единицы в другую;
- автоматически по настроенному расписанию должен инициироваться процесс пересмотра прав доступа для организации в целом или для отдельных организационных единиц;
- вручную ответственными лицами должен инициироваться пересмотр прав доступа в случае существенных изменений ИТ инфраструктуры или организационно-штатной структуры.

В процессе пересмотра прав доступа пользователей для ответственных сотрудников формируются задачи по проверке назначенных прав доступа пользователей. Перечень ответственных сотрудников, привлекаемых для проверки назначенных прав доступа пользователей, зависит от регламента организации и настраивается на этапе развертывания СУУЗиПД.

Результатом процесса, в случае положительного решения при проверке, является сохранение прав доступа для пользователей либо, в случае отрицательного решения, отзыв соответствующих прав доступа пользователей. В любом случае принятое решение фиксируется в журнале и должно быть позднее проанализировано ответственными сотрудниками.

Схема процесса пересмотра прав доступа пользователей показана на рисунке А.6.

А.7 Процесс изменения ролевой модели организации

Процесс изменения ролевой модели организации инициируется ответственным лицом (или группой лиц) в случае появления потребности в создании новой роли, изменении или удалении существующей роли. Ответственным лицом (или группой лиц) может выступать один или более сотрудников, отвечающих за ИБ определенной организационной единицы или организации в целом либо отвечающих за ИБ определенной контролируемой ИС.

В процессе изменения ролевой модели организации ответственное лицо создает новые роли, изменяет или удаляет существующие роли. Ответственное лицо может изменить наименование, описание либо иные атрибуты роли, а также изменить перечень прав доступа, предоставляемых данной ролью.

Результатом процесса является изменение ролевой модели организации. При этом в зависимости от внесенных изменений может произойти изменение прав доступа пользователей, которым назначены измененные или удаленные роли.

Схема процесса изменения ролевой модели организации показана на рисунке А.7.

А.8 Процесс контроля соответствия легальных и фактических прав доступа

Процесс контроля соответствия легальных и фактических прав доступа осуществляется СУУЗиПД непрерывно. В зависимости от архитектуры СУУЗиПД и возможностей, предоставляемых каждой контролируемой ИС, контроль может осуществляться по расписанию или по событиям изменения объектов контролируемой ИС.

В процессе контроля соответствия права доступа, предоставленные каждой учетной записи пользователя в контролируемой ИС, сравниваются с легальными правами доступа пользователя, предоставленными ему в СУУЗиПД. Все выявленные расхождения фиксируются в журнале несанкционированных прав доступа. В зависимости от настроек СУУЗиПД расхождение может быть автоматически устранено либо передано для расследования ответственному сотруднику, который принимает по нему решение.

Результатом процесса контроля соответствия фактических и легальных прав доступа являются фиксация всех несанкционированных изменений прав доступа в журнале несанкционированного доступа, расследование и устранение инцидентов. Решения по инцидентам, принятые ответственным сотрудником, фиксируются в журнале и могут быть позднее проанализированы.

Схема процесса контроля соответствия фактических и легальных прав доступа показана на рисунке А.8.

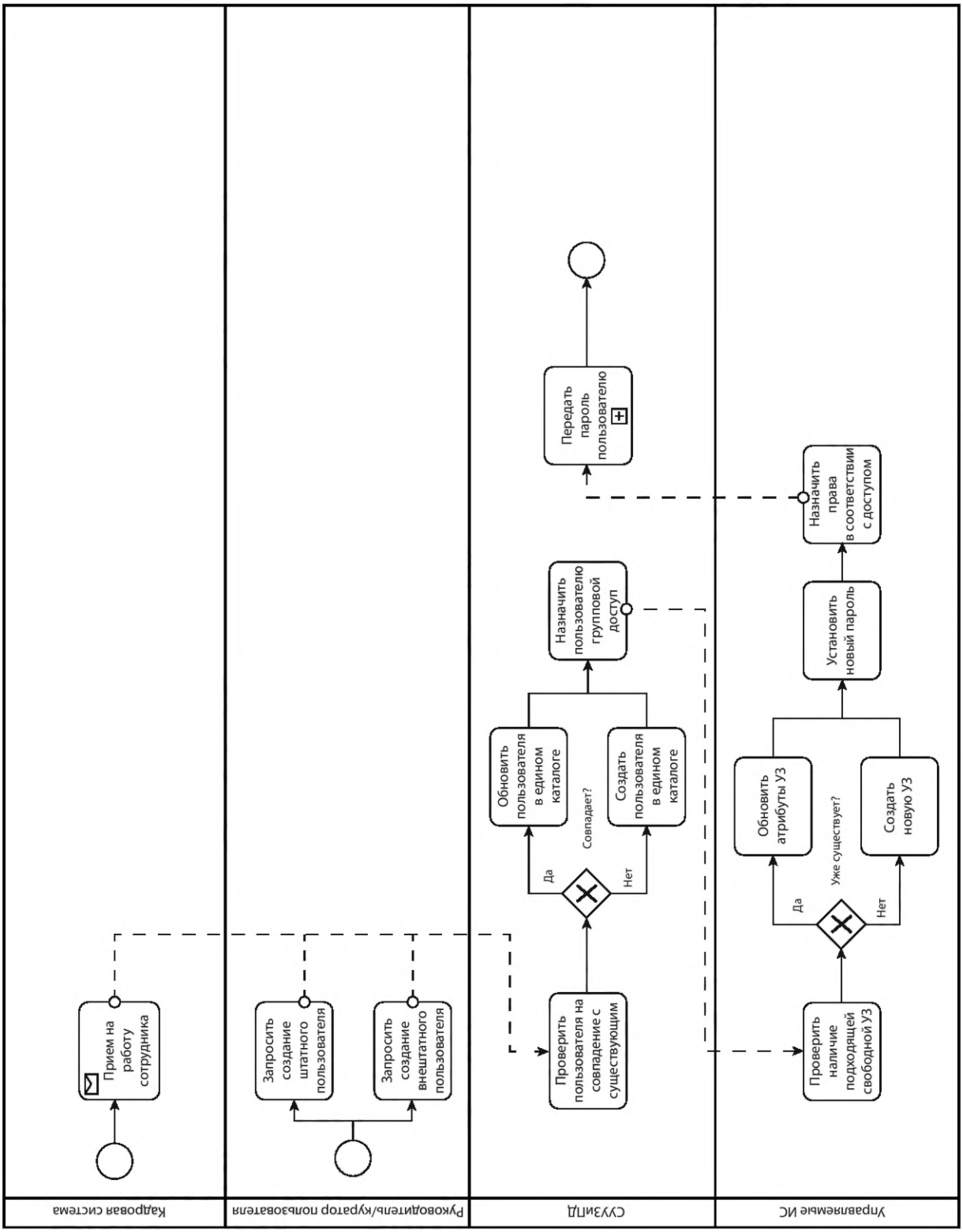

Рисунок А.1 — Создание нового пользователя

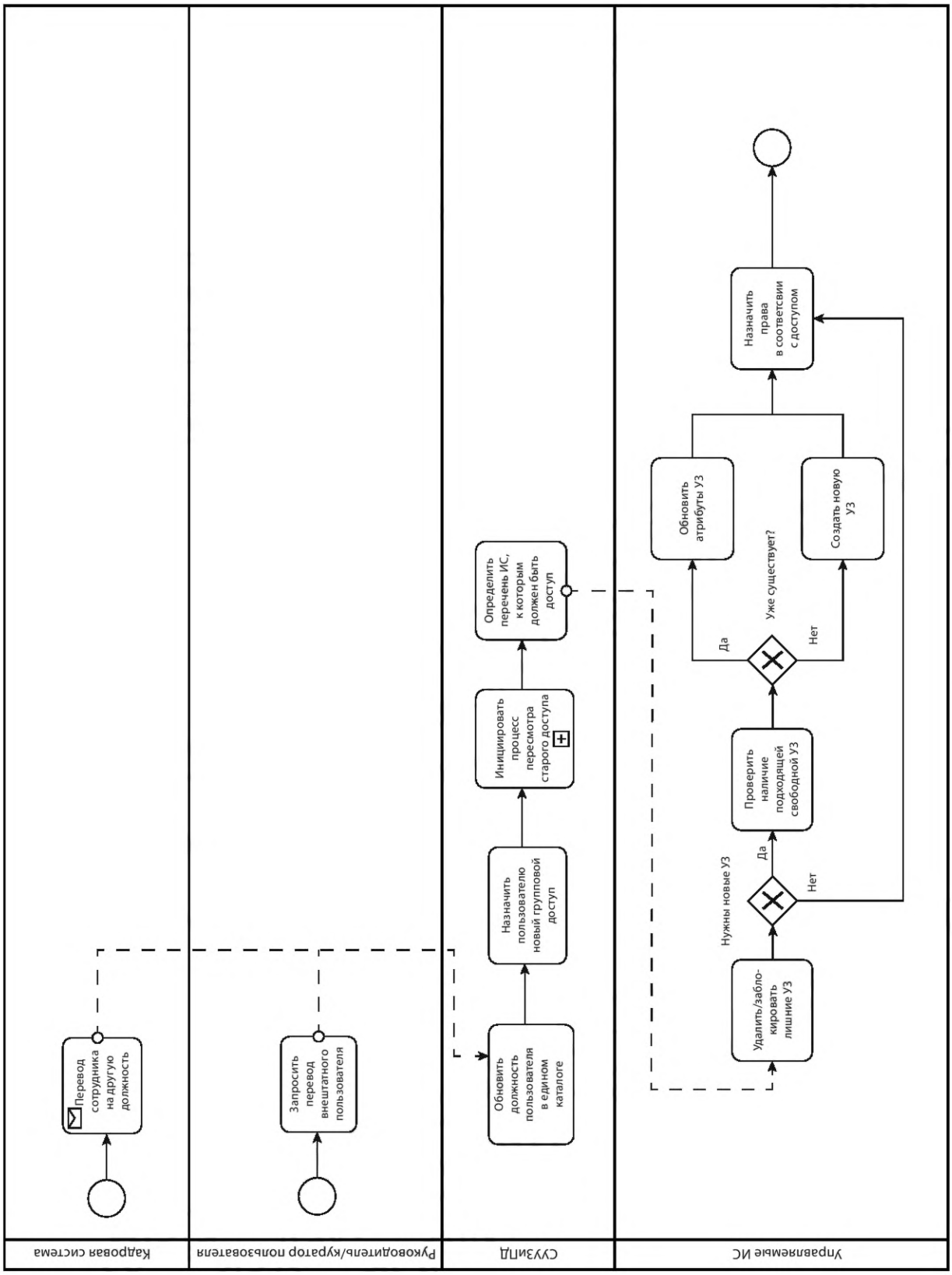

Рисунок А.2 — Перевод на новую должность

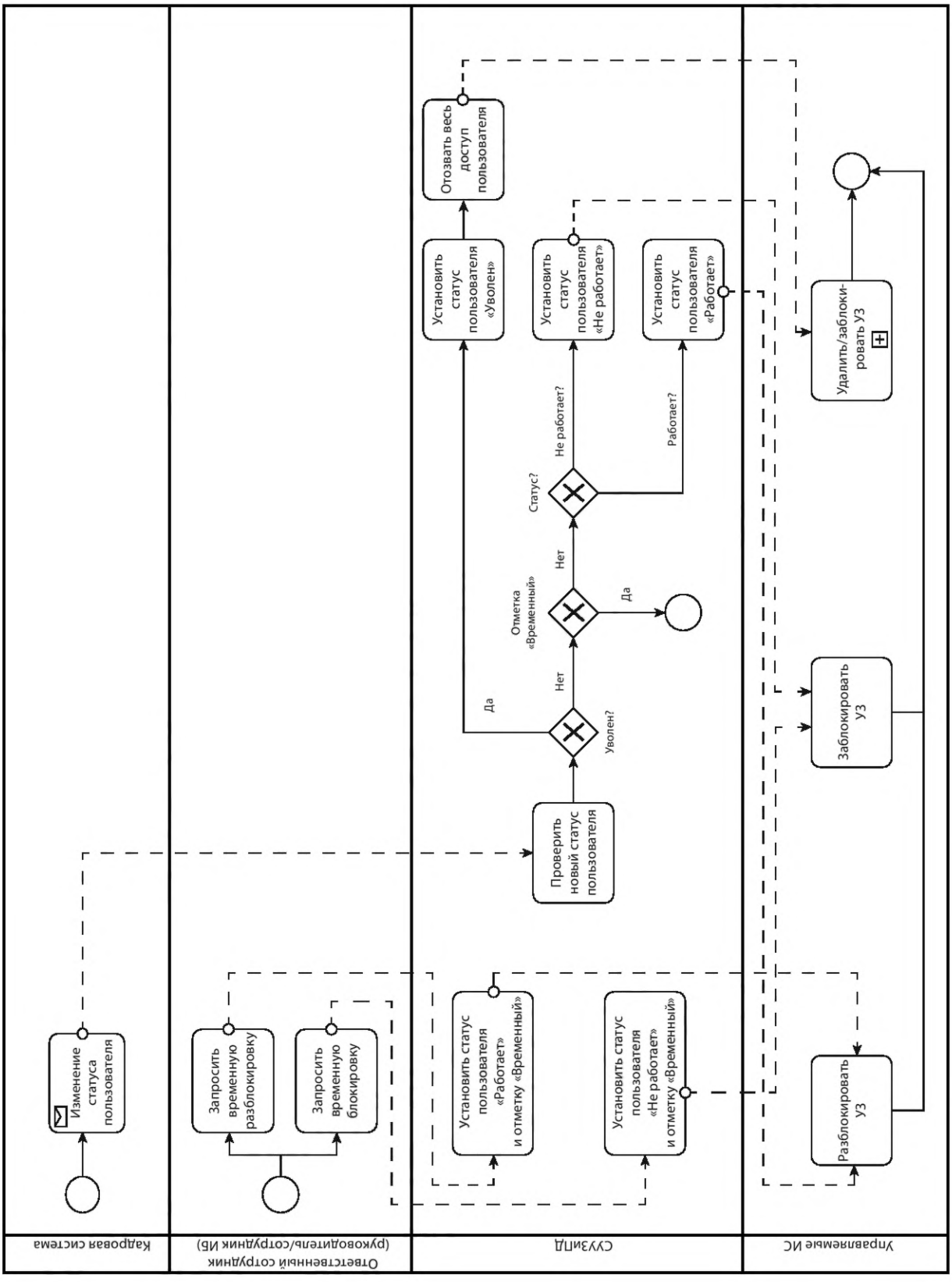

Рисунок А.3 — Изменение статуса пользователя

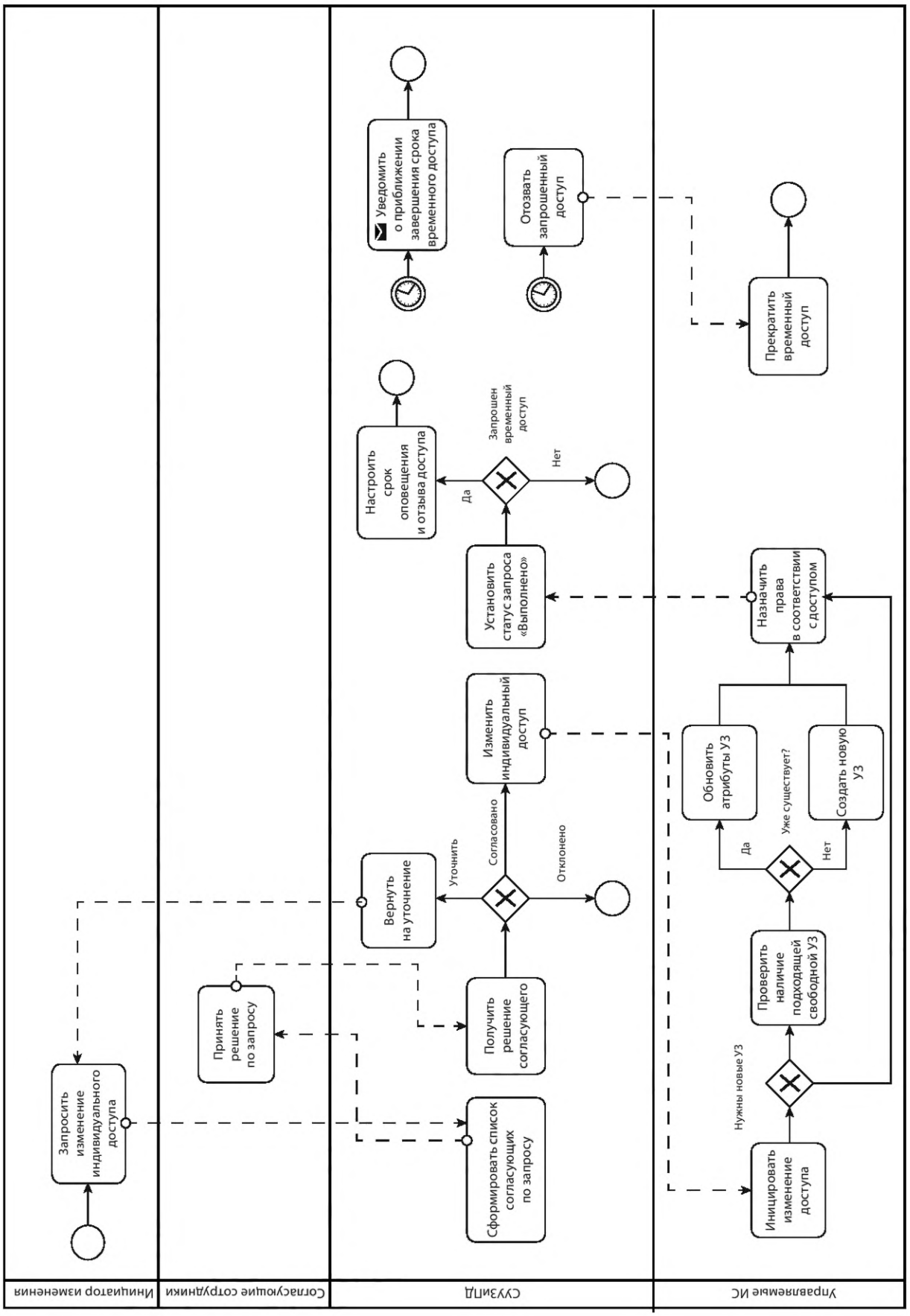

Рисунок А.4 — Изменение прав доступа пользователя

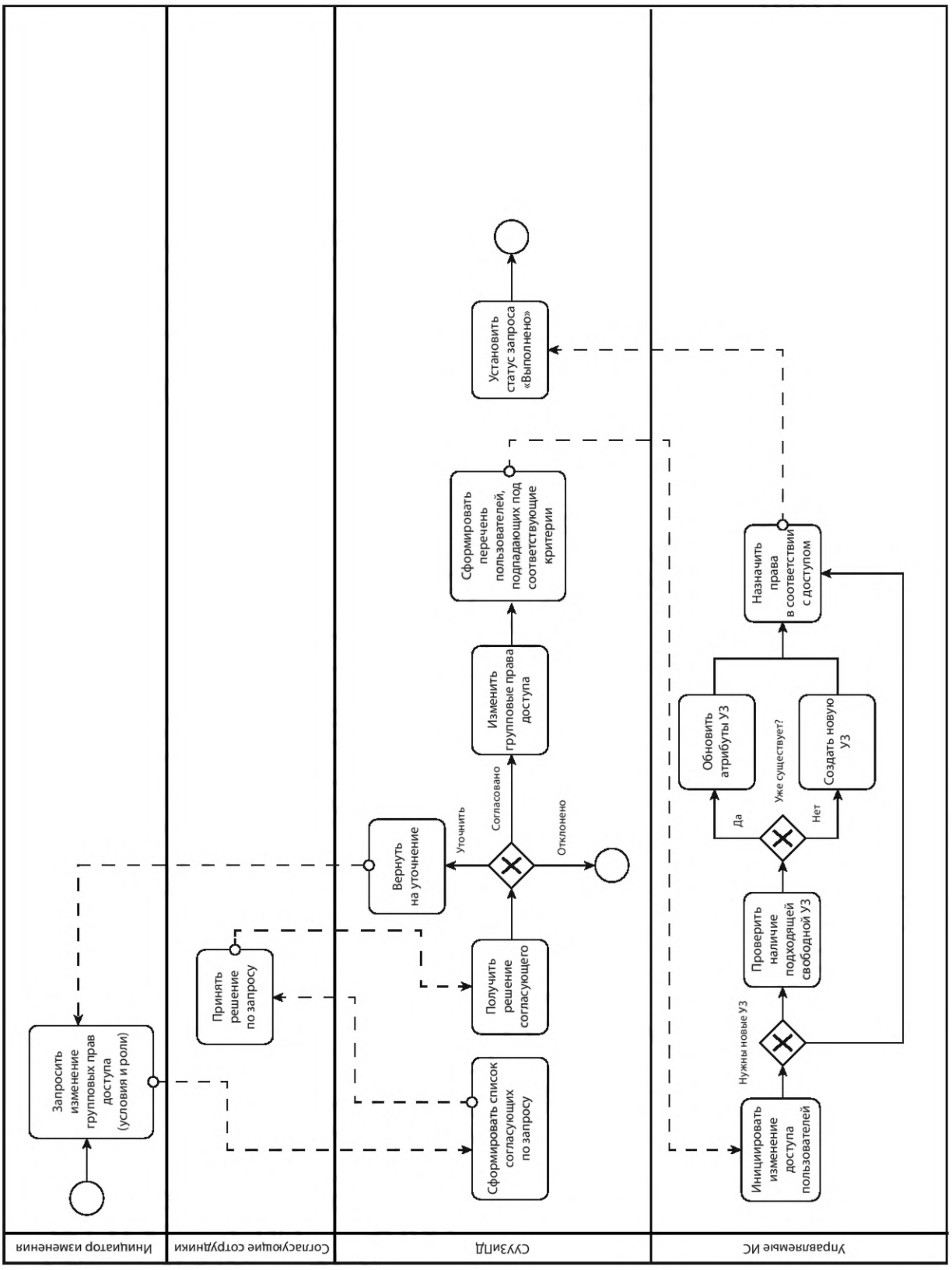

Рисунок А.5 — Изменение групповых прав доступа пользователей

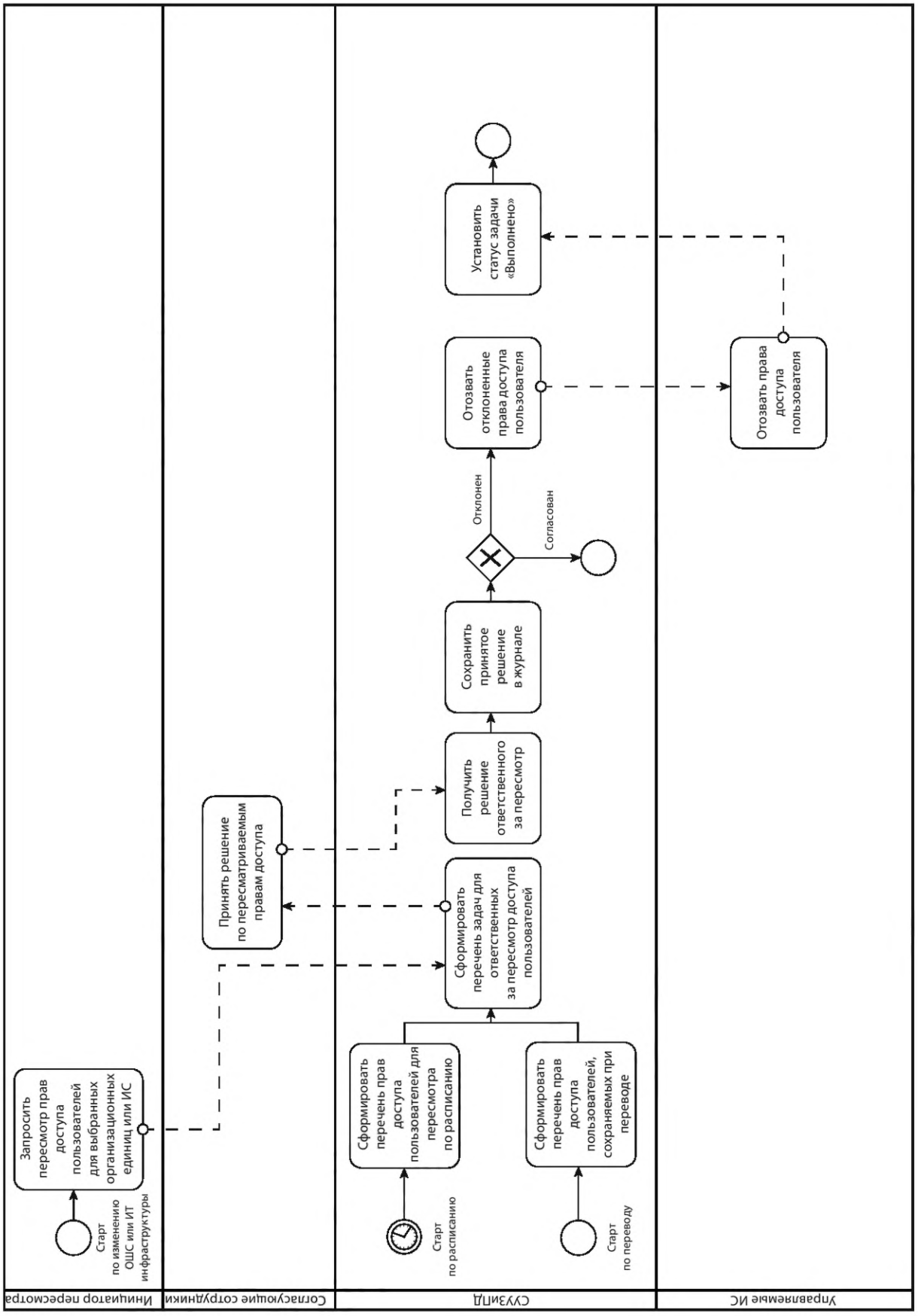

Рисунок А.6 — Пересмотр прав доступа пользователей

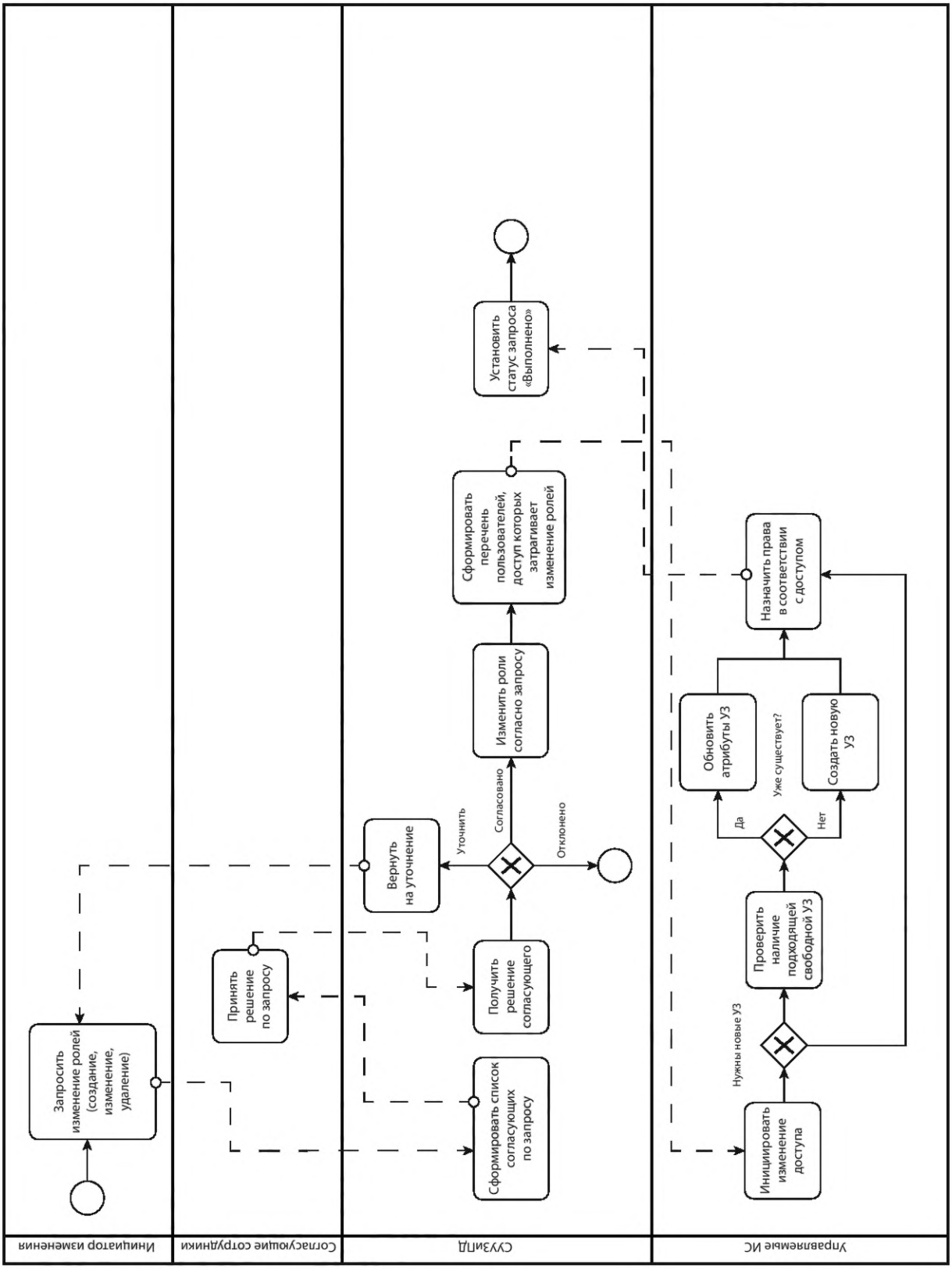

Рисунок А.7 — Изменение ролевой модели организации

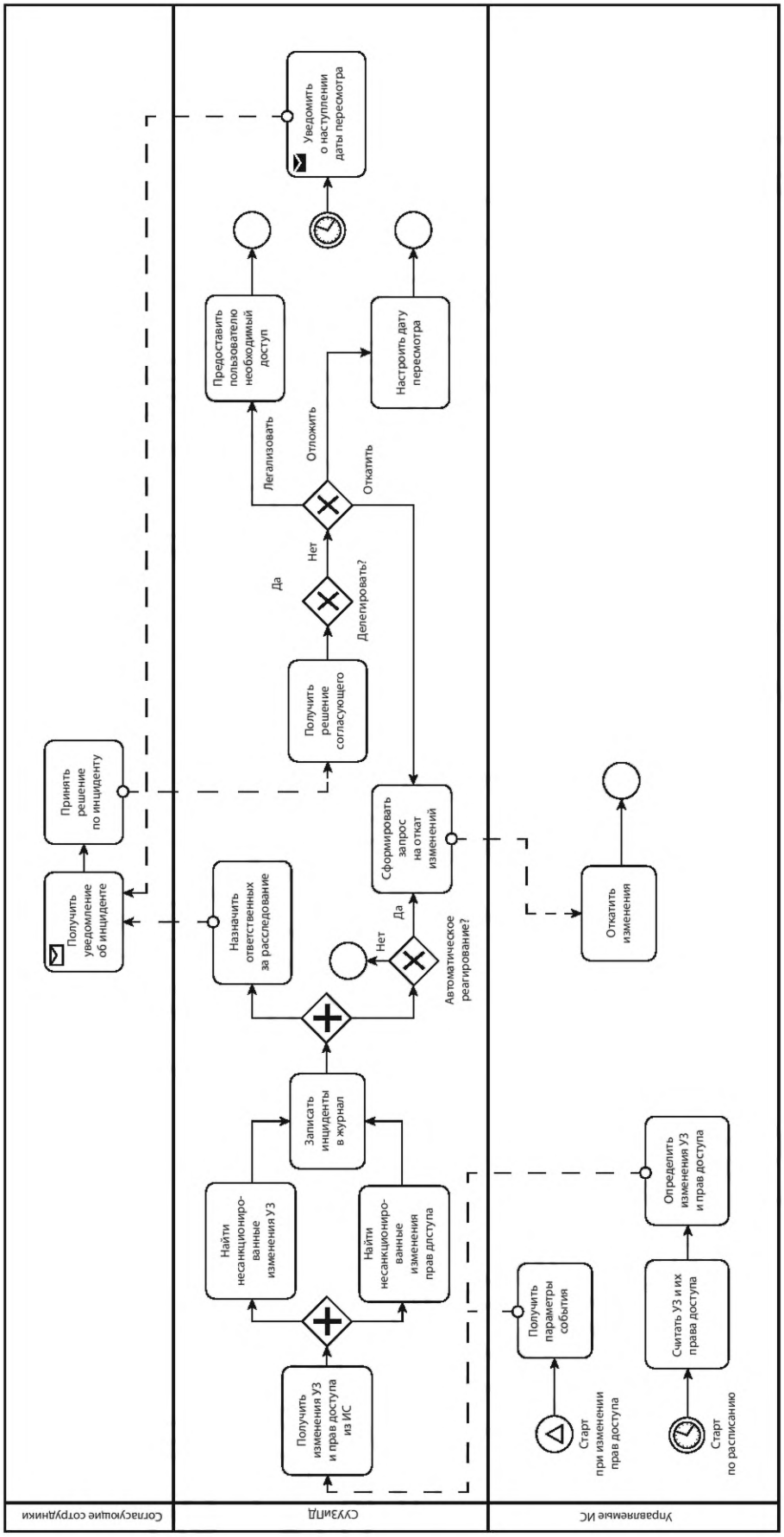

Рисунок А.8 — Контроль соответствия фактических и легальных прав доступа

Библиография

[1] Федеральный закон от 27 июля 2006 г. № 149-ФЗ
«Об информации, информационных технологиях и защите информации»

УДК 004:006.354 ОКС 35.030

Ключевые слова: защита информации, управление учетными записями, управление доступом, автоматизация процессов управления доступом, ролевая модель, парольная политика

Редактор *З.А. Лиманская*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 31.10.2024. Подписано в печать 22.11.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 3,95.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru