УДК 004.05
DOI 10.17513/snt.39703

СТАНДАРТИЗАЦИЯ УПРАВЛЕНИЯ ДОСТУПОМ К КОРПОРАТИВНЫМ ИНФОРМАЦИОННЫМ РЕСУРСАМ НА ОСНОВЕ ПРОЦЕССНОГО ПОДХОДА

Сысоева Л.А.

ФГБОУ ВО «Российский государственный гуманитарный университет», Москва, e-mail: Leda@rggu.ru

Одним из трендов в развитии архитектурных решений корпоративных информационных систем является переход на цифровые платформы и экосистемы, требующие решения большого количества задач по интеграции информационных ресурсов, что обуславливает необходимость разработки и внедрения систем управления доступом к информационным ресурсам организации на основе единых подходов, методов, технологий. Целью исследования является формирование наборов данных, необходимых для реализации процессов управления доступом к информационным ресурсам в автоматизированных системах, в соответствии с рекомендациями стандартов и выделение групп рисков при управлении доступом. В статье представлена концептуальная модель управления доступом к информационным ресурсам автоматизированных систем, разработанная на основе процессного подхода и положений ГОСТ Р 59383-2021. Стандартизация процессов управления доступом включает: подготовку и утверждение политики управления доступом к корпоративным информационным ресурсам; определение систем, обеспечивающих выполнение политики; унификацию процессов управления доступом; унификацию наборов данных для процессов. В соответствии с рекомендациями стандарта были сформированы наборы данных, необходимые для реализации унифицированных процессов системы управления идентификационными данными и системы управления доступом к информационным ресурсам корпоративной информационной системы. Представлено описание наборов данных для процессов аутентификации субъекта, назначения и поддержки атрибутов участников информационного взаимодействия, формирования привилегий субъектов, предоставления доступа. Для процессов управления доступом выделены группы рисков: аутентификационные риски, риски целостности запроса доступа, риски авторизации, риски при предоставлении доступа в соответствии с данными токена доступа. В качестве практического примера формирования набора данных для реализации процессов управления доступом представлено описание прав пользователей в корпоративной информационной системе образовательной организации.

Ключевые слова: корпоративная информационная система, доступ к информационным ресурсам, стандартизация, процесс управления, политика управления

STANDARDIZATION OF ACCESS MANAGEMENT TO CORPORATE INFORMATION RESOURCES BASED ON A PROCESS APPROACH

Sysoeva L.A.

Russian State University for the Humanities, Moscow, e-mail: Leda@rggu.ru

One of the trends in the development of architectural solutions of corporate information systems is the transition to digital platforms and ecosystems that require solving a large number of tasks for integrating information resources, which necessitates the development and implementation of access control systems for information resources of the organization based on unified approaches, methods, technologies. The purpose of the study is to form the datasets necessary to implement access control processes for information resources in automated systems, in accordance with the recommendations of standards and to identify risk groups in access control. The article presents a conceptual model for controlling access to information resources of automated systems, developed on the basis of the process approach and the provisions of GOST R 59383-2021. Standardization of access control processes includes: formation and approval of an access control policy for corporate information resources; identify systems that enforce the policy; unifying access control processes; unifying data sets for processes. In accordance with the recommendations of the standard, the data sets necessary for the implementation of unified processes of the identity management system and the system for controlling access to information resources of the corporate information system were formed. A description of data sets for processes is presented: authentication of a subject, assignment and support of attributes of participants in information interaction, formation of privileges of subjects, granting access. For access control processes, risk groups are identified: authentication risks, access request integrity risks, authorization risks, access grant risks in accordance with access token data. As a practical example of the creation of a set of data for the implementation of access control processes, a description of user rights in the corporate information system of an educational organization is presented.

Keywords: enterprise information system, access to information resources, standardization, management process, management policy

Корпоративные информационные системы (КИС) – это совокупность информационных систем, объединенных сквозными бизнес-процессами и общим документооборотом, где каждая из систем выполняет соответствующие задачи по управлению принятием решений, а все системы в целом обеспечивают устойчивое функционирование организации [1, с. 8; 2].

Архитектура КИС включает множество распределенных информационных ресурсов (ИР), которые формируются, сопрово-

ждаются и предоставляются посредством различных автоматизированных информационных систем [3, с. 9]. В настоящее время одним из трендов в развитии архитектурных решений КИС является переход на цифровые платформы и экосистемы, требующие решения большого количества задач по интеграции информационных ресурсов. Реализация бизнес-процессов (основных, обеспечивающих, управления) также требует совместного использования корпоративных информационных ресурсов различными категориями пользователей [4]. Все вышеперечисленные аспекты обосновывают необходимость разработки и внедрения систем управления доступом к ИР организации на основе единых подходов, методологий.

Для унификации политики, процессов, технологий, моделей разграничения доступа к корпоративным информационным ресурсам Федеральным агентством по техническому регулированию и метрологии в 2021 г. были введены в действие национальные стандарты в сфере обеспечения безопасности информации при использовании автоматизированных систем. В их состав входит стандарт ГОСТ Р 59383-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом» [5], регламентирующий формирование единой политики управления доступом к информационным ресурсам в масштабе корпоративного информационного пространства.

Таким образом, для организаций, которые реализуют в настоящее время проекты по развитию и совершенствованию архитектур корпоративных информационных систем, одной из актуальных задач является формирование системы управления доступом к информационным ресурсам автоматизированных систем, как на корпоративном, так и на межорганизационном уровнях, с учетом моделей, представленных в национальных стандартах.

Цель исследования – формирование наборов данных, необходимых для реализации процессов управления доступом к информационным ресурсам в автоматизированных системах, в соответствии с рекомендациями стандартов, и выделение групп рисков при управлении доступом.

Материалы и методы исследования

Концептуальная модель управления доступом к информационным ресурсам автоматизированных систем, разработанная на основе процессного подхода [6; 7, с. 26] и положений ГОСТ Р 59383-2021 [5], включает ряд последовательных процессов (рис. 1):

– аутентификация субъекта, который отправил запрос на предоставление доступа к ресурсу (как правило, аутентификация выполняется на уровне сеанса, а не на уровне каждого запроса на доступ, таким образом, аутентификационные данные сохраняются и применяются для множества пользовательских запросов);

– принятие решения по авторизации субъекта к запрашиваемому ресурсу, которое фиксируется в выпускаемом токене доступа (токен доступа содержит сведения о разрешении или отказе в доступе к ресурсу на основе политики управления доступом, учитывающей привилегии субъекта и факторы, влияющие на технологию доступа: время, местоположение, средства подключения и пр.);

– выполнение авторизации запрашиваемого ресурса в соответствии с принятым решением (получение прикладной системой токена доступа, содержащего идентификационные данные субъекта и ресурса, информацию о разрешении и уровне доступа) и предоставление субъекту доступа к информационному ресурсу с учетом определенных полномочий.

Рис. 1. Концептуальная модель управления доступом к информационным ресурсам автоматизированной системы в соответствии с ГОСТ Р 59383-2021

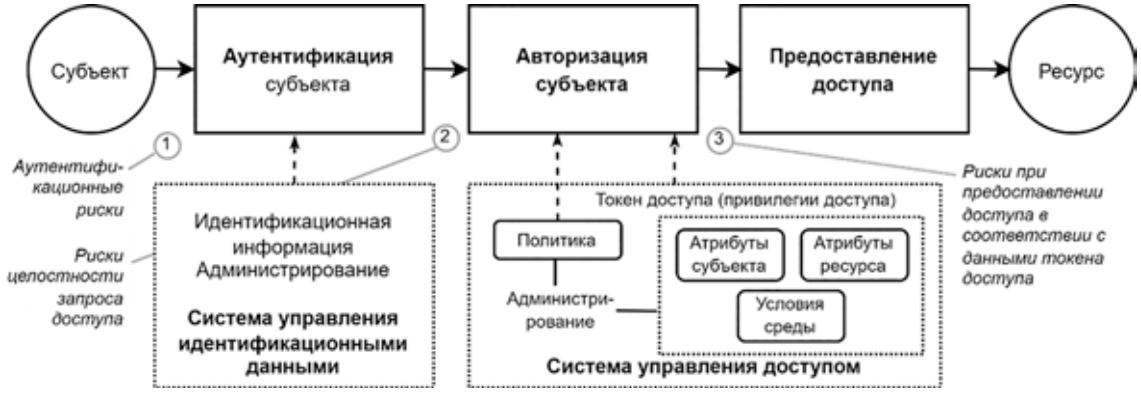

Рис. 2. Концептуальная модель управления доступом к информационным ресурсам с выделением обеспечивающих систем и групп рисков

Целью управления доступом является поддержание доступа субъекта к информационному ресурсу на минимальном уровне, необходимом для выполнения им своих функций, и минимизация рисков, связанных с несанкционированным доступом к информации.

Достижение цели обеспечивается решением ряда задач, в состав которых входят:

– стандартизация процессов управления доступом;

– стандартизация групп рисков при управлении доступом.

В соответствии с положениями ГОСТ Р 59383-2021 стандартизация процессов управления доступом включает:

1) формирование и утверждение политики управления доступом к корпоративным ИР;

2) определение систем, обеспечивающих выполнение политики управления доступом;

2) унификация процессов управления доступом;

3) унификация наборов данных, необходимых для реализации процессов.

Политика управления доступом определяет, что формирование разрешения субъекту на доступ к информационному ресурсу в КИС должно быть регламентированным и включать процессы: аутентификации, авторизации субъекта, принятия решения и предоставление доступа к ИР, которые выполняются на основе присвоения субъектам привилегий доступа, учитывающим атрибуты ресурса, субъекта, среды, модели разграничения доступа.

Процессы управления доступом к ИР (рис. 2), обеспечиваются функционированием двух систем:

– системой управления идентификационными данными (аутентификация субъекта);

– системой управления доступом (аутентифицированный субъект через систему управления доступом запрашивает разрешение на доступ, а система формирует положительное или отрицательное решение по авторизации субъекта к ресурсу и определяет его полномочия).

Системой управления идентификационными данными реализуются следующие процессы:

– администрирование (назначение, введение идентификационных данных субъектов/пользователей; определение используемых методов аутентификации субъектов; применение различных уровней достоверности идентификации пользователей: упрощенный, стандартный, подтвержденный);

– идентификация субъекта (сопоставление субъекта с персональными учетными данными или учетными данными групп пользователей, т.е. распознавание субъекта на основе его идентификационных данных);

– аутентификация субъекта (подтверждение подлинности субъекта с заявленными идентификационными данными, принятие решения по результату аутентификации субъекта).

Система управления доступом отвечает за процессы:

– администрирование (назначение и поддержка атрибутов ресурсов, субъектов, условий среды доступа; формирование привилегий субъектов: ведение каталогов полномочий по доступу к ресурсам информационной системы зарегистрированным субъектам; ведение данных, необходимых для управления процессами в соответствии с принятой политикой);

– авторизация субъекта (прием запроса на доступ к ИР от аутентифицированного субъекта; идентификация запрашиваемого ИР; принятие решения о доступе субъекта к ресурсу и уровне прав, контроль процессов на соответствие политике, выпуск токена доступа);

– предоставление доступа к ресурсам (получение токена доступа: разрешение для субъекта доступа к ресурсу и возможных действий с ним в соответствии с политикой управления доступом).

Таким образом, с учетом положений ГОСТ Р 59383-2021 политика управления доступом требует унификации наборов данных, представляющих атрибуты участников информационного взаимодействия: субъектов и ресурсов.

Результаты исследования и их обсуждение

В соответствии с рекомендациями стандарта ГОСТ Р 59383-2021 были сформированы наборы данных, необходимые для реализации унифицированных процессов системы управления идентификационными данными и системы управления доступом к информационным ресурсам корпоративной информационной системы (табл. 1).

Для процессов управления доступом к ИР свойственны следующие группы рисков (рис. 2):

– аутентификационные риски (определяются минимально допустимым уровнем доверия к аутентификации субъекта в зависимости от уровня риска ресурса);

– риски целостности запроса доступа (связаны с безопасностью каналов связи, по которым поступает запрос на предоставление доступа к ресурсу: частные соединения внутри организации, передача через общедоступные сети или незащищенные каналы; включают меры по обеспечению целостности и конфиденциальности запросов доступа, установлению надежности каналов связи между субъектом и запрашиваемым ресурсом);

– риски авторизации (включают установление уровня риска несанкционированных действий субъекта с запрашиваемым ресурсом);

– риски при предоставлении доступа в соответствии с данными токена доступа (включают риски, связанные с целостностью и конфиденциальностью данных, участвующих в информационном обмене:

1) содержание запроса: аутентификационные данные субъекта, привилегии субъекта, запрашиваемый ресурс, запрашиваемая операция и др.;

2) данные, передаваемые ресурсу, и данные, запрашиваемые от ресурса).

Таблица 1

Наборы данных для реализации процессов управления доступом к информационным ресурсам в автоматизированных системах

Система управления	Процесс	Данные	Описание
Система управления идентификационными данными	Аутентификация субъекта	Идентификационные данные субъектов	Регистр физических лиц. Регистр юридических лиц
		Идентификационные данные информационных систем (ресурсов)	Регистр информационных систем (ИС) / информационных ресурсов
		Категория ИР с позиций информационной безопасности	Общие персональные данные. Специальные персональные данные. Биометрические персональные данные
		Технология аутентификации субъекта	Технология единого входа (SSO) для независимых программных приложений. Технология входа по идентификационным данным на уровне программных приложений
		Метод аутентификации субъекта	По паролю. По электронной подписи. Двухфакторная аутентификация (по постоянному паролю). Двухфакторная аутентификация (по одноразовому паролю)
		Уровень достоверности идентификации пользователя	Упрощенная учетная запись. Стандартная учетная запись. Подтвержденная учетная запись
		Данные для процесса аутентификации субъекта к ИС	Данные для процесса аутентификации идентифицированного субъекта: – идентификатор ИС; – категория ИР; – технология аутентификации; – метод аутентификации; – уровень достоверности идентификации

Система управления	Процесс	Данные	Описание
Система управления доступом	Авторизация субъекта: назначение и поддержка атрибутов участников информационного взаимодействия	Атрибуты ресурса	Идентификационные данные ресурсов: – идентификатор класса ресурсов; – идентификатор ресурса. Режим доступа: – свободный доступ; – ограниченный доступ (конфиденциальная, секретная информация). Категория ИР при ограниченном доступе: – содержит персональные данные (общие, специальные, биометрические). Допустимые профили доступа: – профили групп доступа; – роли доступа; – разрешенные действия (роли); – ограничения доступа
		Атрибуты субъекта	Идентификационные данные субъекта: – идентификатор субъекта; – маркер идентификации; – длительность сеанса идентификации (пользовательская, локальная сессия). Права доступа субъектов: – включение в группы доступа с определенной ролью; – ограничения доступа
		Атрибуты среды	Подключение через клиентское ПО: – специализированный клиент; – веб-клиент; – мобильный клиент. Сетевое подключение: – локальная сеть; – VPN-сеть; – выделенный IP
	Авторизация субъекта: формирование привилегий субъектов	Модель разграничения доступа	Разграничение доступа: – дискреционное; – мандатное; – на основе идентификационных данных; – на основе ролей; – на основе атрибутов; – на основе псевдонимов
		Привилегии субъекта на доступ к ресурсу	Полномочия по доступу к ресурсам ИС зарегистрированным субъектам на основе выбранной модели доступа. Перечень допустимых действий субъекта при обращении к ресурсу
		Токен доступа	Формирование токена доступа: сведения о привилегиях субъекта к ресурсам ИС в соответствующем формате
	Предоставление доступа	Разрешение на доступ субъекта к ИР с определенным набором действий	Получение токена доступа. Идентификация запрашиваемого ИР. Запрос на доступ к ИР от аутентифицированного субъекта с указанием его привилегий. Предоставление соответствующего контента и функций автоматизированной системы в соответствии с политикой управления доступом

В качестве примера формирования набора данных для реализации процессов управления доступом к информационным ресурсам на основе положений ГОСТ Р 59383-2021 рассмотрим описание прав пользователей информационной системы 1С:БИТ.ВУЗ на платформе 1С:Предприятие 8, которая используется в Российском государственном гуманитарном университете (ФГБОУ ВО «РГГУ») для автоматизации процессов управления в образовательной деятельности (табл. 2).

Таблица 2

Наборы данных для реализации процессов управления доступом к информационным ресурсам автоматизированной информационной системы управления учебным процессом

Процесс	Данные	Описание
Авторизация субъекта: назначение и поддержка атрибутов участников информационного взаимодействия	Атрибуты ресурса	Идентификационные данные ресурсов: – идентификатор класса ресурсов: АИС «Управление учебным процессом» АИС-УУП: 001; – идентификатор ресурса: Функциональный модуль «Успеваемость»: 0001. ID ресурса: 001-0001 Режим доступа: – ограниченный доступ: конфиденциальная информация. Категория ИР при ограниченном доступе: – содержит персональные данные: общие. Допустимые профили доступа: – профиль доступа: Работа с успеваемостью (рис. 3); – разрешенные действия (роли): добавление, изменение документов; использование отчетов; чтение документов; чтение справочников и др. (рис. 3); – группы доступа: Работа с успеваемостью ФМОиЗР (рис. 4); – ограничения доступа: ИАИ ФМОиЗР, ИАИ ФМОПиЗР (рис. 5)
	Атрибуты субъекта	Идентификационные данные субъекта: – идентификатор субъекта: userid (Ivan I. Ivanov; Иванов ИИ); – маркер идентификации: разрешение от владельца ресурса на доступ включается в ID-данные; – длительность сеанса идентификации: пользовательская. Права доступа субъектов: – включение в группы доступа с определенной ролью: Работа с успеваемостью по подразделениям (рис. 5); – ограничения доступа: наименования подразделений, к документам которых разрешен доступ (рис. 5)
	Атрибуты среды	Подключение через клиентское ПО: – специализированный клиент. Сетевое подключение: – локальная сеть
Авторизация субъекта: формирование привилегий субъектов	Модель разграничения доступа	Разграничение доступа: – на основе групп и ролей
	Привилегии субъекта на доступ к ресурсу	Перечень полномочий по доступу субъектам к информационным ресурсам соответствующих подразделений при обращении к функциональному модулю «Успеваемость» (рис. 3, 5)

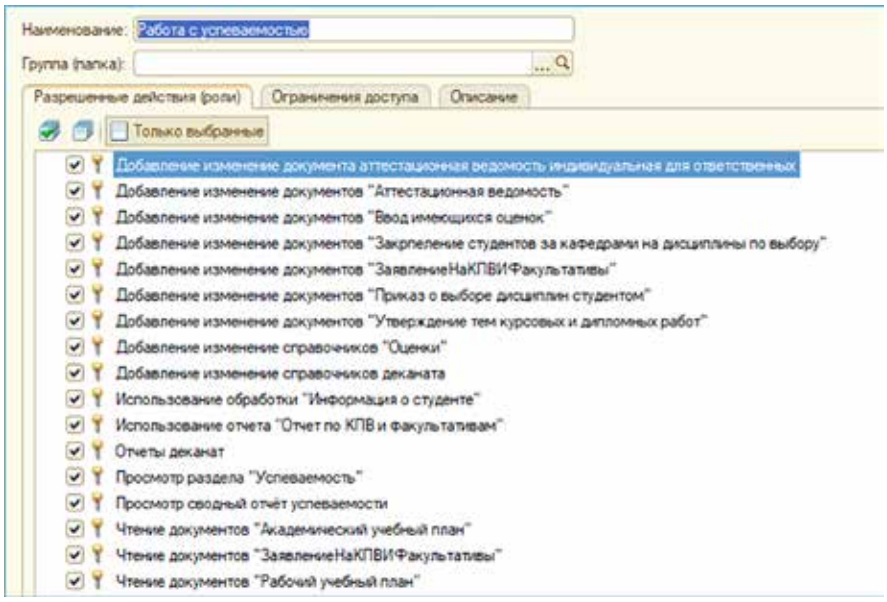

Рис. 3. Профиль доступа «Работа с успеваемостью» с разрешенными действиями (ролями)

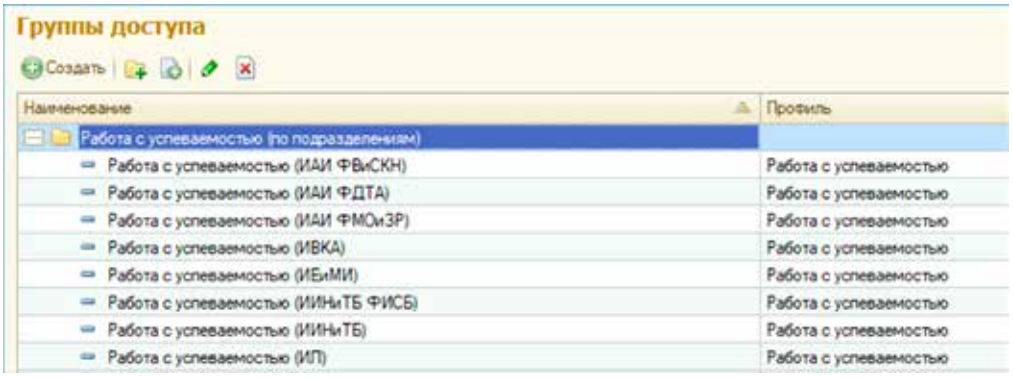

Рис. 4. Группы доступа по подразделениям, сформированные на основе профиля «Работа с успеваемостью»

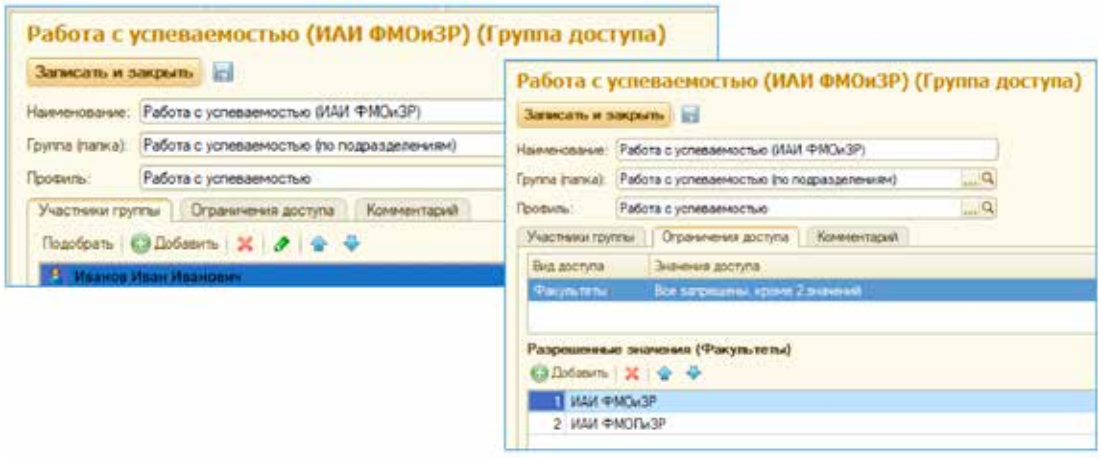

Рис. 5. Группа доступа по подразделениям с указанием участников и перечня подразделений, чьи информационные ресурсы разрешены им для доступа

На рис. 3–5 приведены примеры профиля доступа «Работа с успеваемостью» с разрешенными действиями (ролями) и групп доступа «Работа с успеваемостью (по подразделениям)», обеспечивающие работу пользователей с документами только тех подразделений, к которым им разрешен доступ.

Выводы

Создание и применение системы управления доступом к корпоративным информационным ресурсам, основанной на положениях ГОСТ Р 59383-2021, позволяет:

– снизить риски несанкционированного доступа к ИР;

– предоставлять доступ к ИР с учетом бизнес-требований и требований безопасности на основе единых политик доступа;

– формировать разрешение на доступ к ИР в соответствии с политикой доступа и привилегиями субъекта, учитывающими атрибуты ресурса, субъекта, среды, модели разграничения доступа.

Список литературы

1. Олейник П.П. Корпоративные информационные системы. СПб.: Питер, 2012. 174 с.

2. Лебедев А.С. Проблемы интеграции корпоративных информационных систем – методы и технологии // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2020. № 8. С. 73–78.

3. Рочев К.В. Информационные технологии. Анализ и проектирование информационных систем: учебное пособие для вузов. СПб.: Лань, 2022. 128 с.

4. Сысоева Л.А. Стандартизация требований к прикладным информационным системам организации для включения их в единую систему управления документами // Научное обозрение. Технические науки. 2021. № 3. С. 55–60.

5. ГОСТ Р 59383-2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом. Введ. 2021-05-20. М.: Стандартинформ, 2021. 30 с.

6. Дьяков С.А., Шер М.Л., Дудник Д.В., Миронов Л.В. Моделирование бизнес-процессов: методология, современные факторы в условиях цифровизации // Вестник Алтайской академии экономики и права. 2022. № 4–2. С. 181–190.

7. Громов А.И., Фляйшман А., Шмидт В. Управление бизнес-процессами: современные методы: монография / Под ред. А.И. Громова. М.: Юрайт, 2023. 367 с.