УДК 658 **DOI: 10.34670/AR.2026.28.98.076**

Применение технологии автоматизации процессов в системе управления предприятием

Туков Максим Сергеевич

Аспирант,
кафедра производственного менеджмента,
Луганский государственный университет им. Владимира Даля,
291034, Российская Федерация, Луганск, кв. Молодежный, 20А;
e-mail: makstuk6991@mail.ru

Родионов Александр Владимирович

Доктор экономических наук, профессор,
кафедра производственного менеджмента,
Луганский государственный университет им. Владимира Даля,
291034, Российская Федерация, Луганск, кв. Молодежный, 20А;
e-mail: makstuk6991@mail.ru

Аннотация

Данная статья рассматривает применение технологии Microsoft Active Directory как элемент управления предприятием. Обосновывается необходимость перехода к централизованной системе управления ИТ-инфраструктурой. Технология рассматривается как механизм, способный привнести прозрачность распределения прав доступа к информации и инструмент делегирования полномочий структурным подразделениям с сохранением централизованного контроля. Уделяется внимание ролевой модели доступа (RBAC). Разобраны важные этапы подготовки для внедрения данного решения.

Для цитирования в научных исследованиях

Туков М. С., Родионов А. В. Применение технологии автоматизации процессов в системе управления предприятием // Экономика: вчера, сегодня, завтра. 2026. Том 16. № 1А. С. 744-750. DOI: 10.34670/AR.2026.28.98.076

Ключевые слова

Active Directory, управление предприятием, ИТ-инфраструктура, групповая политика, ролевая модель доступа, централизованное управление, информационная безопасность.

Введение

В настоящее время предприятия представляют собой сложными организационными системами. Для решения задач комплексного управления применяются информационные технологии. В основу работы любой информационной технологии лежит информация. Так информация становится одним из ресурсов, который определяет качество управления предприятием.

Из-за возрастания значимости информации необходимо формирование на предприятии механизма обработки, структурирования и защиты информации.

Основная часть

В распределённой ИТ-инфраструктуре доступ к данным может осуществляться с различных рабочих станций включая удалённый доступ, когда сотрудники работают с информацией предприятия, не находясь при этом на рабочем месте. Задача комплексного централизованного управления предприятием должна подразумевать управление учетными записями пользователей корпоративной сети, правами доступа к данным, сетевыми ресурсами и политиками информационной безопасности.

Отсутствие единой централизованной системы управления ИТ-инфраструктурой приводит к её децентрализации, что приводит к негативным эффектам:

– **Дублирование функций**. Структурные подразделения вынуждены самостоятельно решать задачи администрирования, закупок и сопровождения ИТ-решений. Это приводит к параллельному созданию однотипных решений, чрезмерному увеличению штатной численности и росту фонда оплаты труда без сопоставимого увеличения качества управления.

– **Потеря прозрачности**. Руководство предприятия теряет возможность оперативного получения информации о состоянии информационных систем, структуре прав доступа сотрудников к информации, конфигурации оборудования и уровня защищённости коммерческой тайны. Это увеличивает управленческие риски и снижает внутренний контроль.

– **Временные затраты**. При децентрализированной системе управления любое изменение или внедрение новых регламентов, установка нового или обновление текущего программного обеспечения, изменение прав доступа может занимать значительное время.

Чтобы реализовать централизованное управление необходимо решение, которое смогло бы учесть вышеперечисленные проблемы и устранить их. Для таких задач весьма эффективным будет технология Microsoft Active Directory (AD).

Система Active Directory – это инструмент для сбора, хранения, обработки данных пользователей, и устройств. Благодаря этой технологии можно распределить пользователей и их устройства на роли, которые будут соответствовать их структурным подразделениям. Так администратор AD может назначить работникам бухгалтерии доступ к данным и инструментам, которые предназначены только для деятельности бухгалтерии, при этом ограничить доступ к документам других отделов. Если же возникнет необходимость изменить права доступа сотрудников бухгалтерии администратор AD может просто изменить роль, назначенную сотрудникам в каталоге Active Directory.

Внедрение такой технологии способствует созданию упрощённого управления групповыми политиками информационной среды предприятия. Групповой политикой в информационных технологиях, таких как Active Directory, принято называть набор правил и конфигураций для строгой настройки рабочей среды.

С точки зрения менеджмента любую организацию можно рассматривать как совокупность бизнес-процессов и персонала, взаимодействующих для достижения финансовых результатов. С такой точки зрения применение Active Directory следует рассматривать как создание «цифрового двойника» компании, где каждый элемент системы соответствует реальному сотруднику и подразделению. Также ценность такой системы в возможности перевода бумажных должностных инструкций в автоматизированное управление этими инструкциями.

В крупных территориально распределенных компаниях часто возникает конфликт между необходимостью централизованного контроля из «центра» и потребностью филиалов в административной самостоятельности. Грамотно отлаженная система Active Directory может поддерживать баланс между централизацией и делегированием полномочий и позволяет структурным подразделениям наделять своих работников теми или иными правами доступа, при этом данные действия будут отражены в общей структуре системы AD.

Active Directory предоставляет возможность: единства стандартов, делегирования возможностей и создания прозрачности для аудита. Рассмотрим данные перспективы.

Ключевым аспектом AD является единство корпоративных стандартов в сфере информационной безопасности и администрирования. Централизованное управление политиками (в частности, через механизмы групповых политик) позволяет устанавливать единые требования к аутентификации, конфиденциальности данных, управлению учётными записями и иным параметрам ИТ-среды для всей организации.

Иерархическая структура системы AD позволяет делегировать административные полномочия на уровне подразделения. Филиалы и структурные подразделения могут получить права управления своими ресурсами в пределах заданной зоны ответственности, что позволит перераспределить нагрузку, ускорить операционные процессы, не нарушая общих корпоративных стандартов.

Система аудита фиксирует факты доступа к критически важным данным, что служит сдерживающим фактором для неправомерных действий персонала. В случае инцидентов информационной безопасности система позволяет провести ретроспективный анализ, выявить причины и ответственных лиц, минимизируя последствия для бизнеса.

Централизованное хранение объектов и механизмов аутентификации обеспечивает прозрачность аудита ИТ-инфраструктуры. Несмотря на автономию отдельных подразделений, права доступа, изменение учётных записей и параметры безопасности остаются подконтрольными в рамках одного корпоративного пространства управления.

Таким образом, Active Directory занимает роль платформы, обеспечивающей целостность идентификационного и административного пространства предприятия, и позволяет избежать фрагментацию информационной среды, формируя устойчивое функционирование распределённой корпоративной сетью. Подход, когда права доступа и набор программных инструментов выдаются сотруднику персонально неэффективен, такой процесс трудоемкий, подвержен ошибкам и времязатратный.

Эффективным инструментов современного менеджмента в ИТ-среде является переход к ролевой модели управления доступом (RBAC), что как нельзя лучше позволяет организовать Active Directory.

Логика ролевой модели заключается в следующих принципах:

– **Создание «цифрового профиля» должности.** Система оперирует не конкретными физическими лицами, а должностями (ролями), закрепленными в организационной структуре предприятия, к примеру «главный специалист отдела кадров». В структуру каждой роли заранее включен набор прав доступа к данным и необходимый для работы на данной должности программный инструментарий.

– **Минимизация времени простоя.** В условиях децентрализованного управления процесс предоставления необходимых прав и набора программных инструментов может занимать продолжительное время. Ролевая модель призвана сжать такие сроки до минимума, что позволяет выдавать необходимые полномочия в момент выхода сотрудника на работу.

– **Снижение рисков ошибочного назначения прав**. Когда распределение полномочий осуществляется отдельно для каждого сотрудника, риски ошибочного назначения прав доступа возрастают. Применение ролей позволяе стандартизировать процедуры назначения прав и снижает риски ошибочных назначений полномочий.

– **Контроль кадровых изменений.** При переводе сотрудника в другое подразделение его полномочия корректируются посредством изменения роли, так происходит аннулирования старых прав доступа и назначение новых. Такой подход повышает уровень информационной безопасности предприятия.

С точки зрения предприятия внедрение Active Directory является инвестиционным проектом стратегической важности, благодаря своим оптимизационным качествам. Эффективность внедрения данной системы оценивается через ее способность снижать операционные издержки и минимизировать управленческие риски.

В условиях децентрализованной информационной инфраструктуры затраты на обслуживание информационных систем возрастают пропорционально увеличению масштабов предприятия.

Стандартизация ИТ-инфраструктуры посредством Active Directory является действенным методом минимизации внеплановых расходов и правовых рисков. Централизованный контроль программного обеспечения исключает использование нелицензионных продуктов и позволяет сократить правовые и репутационные риски.

Дополнительно, ограничение прав пользователей на установку стороннего программного обеспечения снижает вероятность программных сбоев и простоев оборудования. Учитывая возможную высокую стоимость простоя на предприятиях, предварительное обеспечение стабильности через групповые политики становится важным элементом обеспечения непрерывности бизнес-процессов. Приведение рабочей среды к общему стандарту также ускоряет взаимодействие внутри организации и упрощает процедуры технической поддержки.

Развертывание Active Directory на предприятии представляет собой не узкоспециализированную техническую процедуру, а комплексный управленческий проект, направленный на трансформацию системы контроля и распределения ресурсов. Процесс внедрения целесообразно рассматривать как жизненный цикл инвестиционного проекта, где программно-аппаратная реализация является лишь инструментом достижения организационных целей.

На начальном этапе проводится глубокий анализ информационных потоков и прав собственности данных. Формируется «информационный портрет» предприятия, в рамках которого должны быть четко выверены владельцы конкретных данных. Например, финансовый

директор выступает распорядителем бюджетной информации, а директор по персоналу – персональных данных сотрудников.

Критически важным является изучение взаимодействия между подразделениями для выявления общих ресурсов, что позволяет избежать дублирования информации. Итогом данного этапа становится матрица доступа – документ, фиксирующий права сотрудников (чтение, изменение, удаление), пересечении ролей и информационные ресурсы. Данная матрица служит фундаментом для построения архитектуры безопасности.

Организационные подразделения в структуре Active Directory отражают реальную иерархию предприятия. Грамотное проектирование этих элементов позволяет делегировать административные полномочия руководителям среднего звена, ограничивая их влияние рамками вверенного подразделения.

Следующим этапом является проектирование логической структуры, главная цель которого создание модели управления, отражающей текущую иерархию предприятия. В данном контексте требуется сохранять гибкость, и соблюдать принцип приоритета бизнес–логики, согласно которому техническая реализация должна следовать за структурой бизнеса.

Технологические решения неэффективны без подкрепления нормативной базой. Внедрение AD без соответствующих регламентов может быть неэффективной. Необходима разработка корпоративных стандартов, таких как положение о парольной защите, ответственность за передачу учетных данных, и регламент предоставления доступа.

Переход на работу в новой среде должен быть закреплен приказом по предприятию с обязательным ознакомлением сотрудников под роспись. Это переводит вопросы информационной безопасности из плоскости личных договоренностей в плоскость трудового законодательства.

Критическим аспектом является обучение логике управления доступом. Руководители среднего звена должны осознать наличие инструментов контроля подчиненных и принять ответственность за санкционирование доступа к информации своего департамента.

Заключение

Внедрение Active Directory является не только важным шагом модернизации ИТ-инфраструктуры, но и решением внести прозрачность распределения прав доступа. Практической ценностью ввода на предприятия такой технологии будет упрощение администрирования информационной безопасности предприятия, путем централизации управления учётными записями и внедрением ролевой модели распределения полномочий.

Библиография

1. Корнеева Т. Ю., Никитин С. А. Цели и стратегии развития предприятий, их классификация и системный подход к их формированию // Известия Тульского государственного университета. Экономические и юридические науки. 2010. № 1-1. С. 195–204.
2. Крафт Р., Хилл Б. и др. Microsoft Windows Server 2016: полное руководство / пер. с англ. Москва: Диалектика, 2019. 1392 с.
3. Пасечко В. В. Место функциональных стратегий в стратегическом планировании деятельности организаций // Экономика, управление и финансы в цифровом обществе: материалы Междунар. науч.-практ. конф. (Курск, 26–27 апреля 2023 г.). Курск: Курский институт кооперации (филиал) Белгородского университета кооперации, экономики и права, 2023. С. 58–62.
4. Петров А. Н. Стратегический менеджмент: учебник для вузов. Санкт-Петербург: Питер, 2015. 400 с.

5. Риззо Т. Active Directory для Windows Server 2008: справочник администратора / пер. с англ. Москва: Русская редакция, 2010. 608 с.
6. Active Directory Administration with Windows PowerShell [Электронный ресурс]. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd378937(v=ws.10)?redirectedfrom=MSDN
7. TechNet: Windows Authentication [Электронный ресурс]. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755284(v=ws.10)?redirectedfrom=MSDN

Application of Process Automation Technology in the Enterprise Management System

Maksim S. Tukov

Postgraduate Student,
Department of Production Management,
Lugansk State University named after Vladimir Dal,
291034, 20A, Molodezhny Kvartal, Lugansk, Russian Federation;
e-mail: makstuk6991@mail.ru

Aleksandr V. Rodionov

Doctor of Economics, Professor,
Department of Production Management,
Lugansk State University named after Vladimir Dal,
291034, 20A, Molodezhny Kvartal, Lugansk, Russian Federation;
e-mail: makstuk6991@mail.ru

Abstract

This article examines the application of Microsoft Active Directory technology as an element of enterprise management. The necessity of transitioning to a centralized IT infrastructure management system is substantiated. The technology is considered as a mechanism capable of bringing transparency to the distribution of information access rights and as a tool for delegating authority to structural divisions while maintaining centralized control. Attention is paid to the role-based access control (RBAC) model. Important stages of preparation for the implementation of this solution are analyzed.

For citation

Tukov M.S., Rodionov A.V. (2026) Primeneniye tekhnologii avtomatizatsii protsessov v sisteme upravleniya predpriyatiyem [Application of Process Automation Technology in the Enterprise Management System]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 16 (1A), pp. 744-750. DOI: 10.34670/AR.2026.28.98.076

Keywords

Active Directory, enterprise management, IT infrastructure, group policy, role-based access model, centralized management, information security.

References

1. Active Directory Administration with Windows PowerShell. (n.d.). Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd378937(v=ws.10)?redirectedfrom=MSDN
2. Korneyeva, T. Yu., & Nikitin, S. A. (2010). Tseli i strategii razvitiya predpriyatiy, ikh klassifikatsiya i sistemnyy podkhod k ikh formirovaniyu [Goals and strategies of enterprise development, their classification and a systematic approach to their formation]. *Izvestiya Tulskogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki*, (1-1), 195-204.
3. Kraft, R., Hill, B., et al. (2019). *Microsoft Windows Server 2016: polnoe rukovodstvo* [Microsoft Windows Server 2016: The complete guide]. Dialektika.
4. Pasechko, V. V. (2023). Mesto funktsionalnykh strategiy v strategicheskom planirovanii deyatelnosti organizatsiy [The place of functional strategies in the strategic planning of organizations]. In *Ekonomika, upravlenie i finansy v tsifrovom obshchestve: materialy Mezhdunar. nauch.-prakt. konf.* (pp. 58-62). Kurskiy institut kooperatsii.
5. Petrov, A. N. (2015). *Strategicheskiy menedzhment: uchebnik dlya vuzov* [Strategic management: Textbook for universities]. Piter.
6. Rizzo, T. (2010). *Active Directory dlya Windows Server 2008: spravochnik administratora* [Active Directory for Windows Server 2008: Administrator's reference]. Russkaya redaktsiya.
7. TechNet: Windows Authentication. (n.d.). Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755284(v=ws.10)?redirectedfrom=MSDN